Citrix Virtual Apps and Desktops 7 1912 LTSR

Contents

Citrix Virtual Apps and Desktops 7 1912 LTSR (Long Term Service Release)

May 24, 2024

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

Citrix Virtual Apps and Desktops ist eine Virtualisierungslösung, die IT die Steuerung von virtuellen Maschinen, Anwendungen, der Lizenzierung und Sicherheit ermöglicht und gleichzeitig Benutzern von überall Zugriff mit jedem Gerät bietet.

Das Long Term Service Release (LTSR)-Programm für Citrix Virtual Apps and Desktops bietet Stabilität und langfristige Unterstützung für Citrix Virtual Apps and Desktops-Releases.

Das kumulative Update 9 (CU9) ist das neueste Update für 1912 LTSR. LTSRs stehen auch für die XenApp und XenDesktop-Version 7.15 zur Verfügung. Wenn Sie beim LTSR-Programm neu sind, ist die Installation des 1912 LTSR-Erstrelease nicht erforderlich. Wir empfehlen, dass Sie direkt 1912 LTSR CU9 installieren.

- Informationen zu Anwendungsfällen finden Sie unter https://www.citrix.com/products/citrix-virtual-apps-and-desktops/.
- Informationen zu Komponenten und Technologien in Citrix Virtual Apps and Desktops-Bereitstellungen finden Sie unter Technische Übersicht.

Frühere Releases

Die Dokumentation für andere derzeit verfügbare Versionen ist in Citrix Virtual Apps and Desktops.

Die Dokumentation zu älteren Versionen ist unter Legacy-Dokumentation archiviert.

Citrix Virtual Apps and Desktops in Citrix Cloud

Das Virtual Apps and Desktops-Angebot für Citrix Cloud heißt jetzt Citrix DaaS. Die Servicedokumentation finden Sie unter Citrix DaaS.

Downloads

Citrix Virtual Apps and Desktops 7 1912 LTSR CU9

Hilfreiche Links

- Citrix Supportability Pack
- Häufig gestellte Fragen zu LTSR (FAQs)
- Serviceoptionen für Citrix Virtual Apps and Desktops
- Produktlebenszyklusdaten
- LTSR-Programm für Receiver für Windows

Änderungen an Citrix-Produktnamen und -Versionsnummern

Informationen über seit 2018 geänderte Produktnamen und Versionsnummern finden Sie unter Neue Namen und Nummern.

Was ist neu

May 24, 2024

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)

Informationen zu 1912 LTSR (Erstrelease)

Cumulative Update 9 (CU9)

May 24, 2024

Veröffentlichungsdatum: 30. April 2024

Info zu diesem Release

Citrix Virtual Apps and Desktops 7 1912 LTSR Cumulative Update 9 (CU9) behebt mehr als 15 Probleme, die seit Veröffentlichung von 1912 LTSR CU8 gemeldet wurden.

1912 LTSR (Allgemeine Informationen)

1912 LTSR (Informationen zu Features und Upgrades)

Behobene Probleme seit Citrix Virtual Apps and Desktops 7 1912 LTSR CU8

Bekannte Probleme in diesem Release

Veraltete und entfernte Produkte und Features

Berechtigungsdaten des Citrix-Produkts für Subscription Advantage

Downloads

Citrix Virtual Apps and Desktops 7 1912 LTSR CU9

> **Wichtig:**
>
> Die Citrix License Administration Console hat das Ende des Lebenszyklus und das Ende der Unterstützung in Lizenzserver 11.17.2.0_BUILD_40000 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 Citrix Virtual Apps and Desktops-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 Citrix Virtual Apps and Desktops 7 1912 LTSR (Erstrealease) mit besonderem Augenmerk auf 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 1912 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 Citrix Virtual Apps and Desktops 7 1912 LTSR CU9

1912 LTSR-Basiskomponente	Version wie unter "Programme und Funktionen"angezeigt	Hinweise
Einzelsitzungs-VDA	1912.0.9000.9299	
Multisitzungs-VDA	1912.0.9000.9299	
Delivery Controller	1912.0.9000.9299	
Citrix Studio	1912.0.9000.85	
Citrix Director	1912.0.9000.14	
Citrix Gruppenrichtlinienverwaltung	7.24.9000.0	
Citrix Gruppenrichtlinie - clientseitige Erweiterung	7.24.9000.0	
Citrix StoreFront	1912.0.9000.17	
Citrix Provisioning	1912.80.iso	
Universeller Druckserver	1912.0.9000.15	
Sitzungsaufzeichnung	1912.0.9000	
Linux VDA	1912.0.9000	Informationen zu den unterstützten Plattformen finden Sie in der Linux VDA-Dokumentation
Profilverwaltung	1912.0.9000.3	
Citrix Verbundauthen-tifizierungsdienst	1912.0.9000.14	
Browserinhaltsumleitung	15.19.9000.16	

Kompatible Komponenten für Citrix Virtual Apps and Desktops 7 1912 LTSR CU9

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 1912 LTSR-Umgebung durchzuführen.

Kompatible Komponenten und Features	Version wie unter "Programme und Funktionen"angezeigt
App Layering	22.11
App-Schutzrichtlinien	1912 LTSR CU8
HDX RealTime Optimization Pack	2.9 LTSR CU7
Lizenzserver	11.17.2.0 Build 47000
Benutzerpersonalisierungslayer	23.12.4
Webplayer für die Sitzungsaufzeichnung	1912.0.9000
Self-Service-Kennwortzurücksetzung	1912.0.8000
Windows 10 32-Bit	Siehe Dokumentation zum Erstrelease.
Workspace Environment Management	2305
XenApp und XenDesktop 7.15 LTSR VDA (aktuelles Release)*	Nur aktuelles kumulatives Update

> **Hinweis:**
>
> Windows 10 32-Bit wird nur für 18 Monate ab der ersten Veröffentlichung von 1912 LTSR unterstützt. Windows 10 32-Bit wird nur unter Windows 10 Enterprise 2019 LTSC unterstützt.
>
> * Die XenApp und XenDesktop 7.15 LTSR VDA-Unterstützung gilt in diesem Fall nur für Windows 7 und Windows 2008 R2. Die Unterstützung für XenApp und XenDesktop 7.15 für LTSR endet am August 2022. Die Citrix Unterstützung für Windows 7 und Windows 2008 R2 endet, wenn Microsoft die Unterstützung für das Betriebssystem einstellt oder wenn die Unterstützung für XenApp und XenDesktop 7.15 LTSR endet, je nachdem, was zuerst eintritt. Weitere Informationen finden Sie in der Citrix Produktmatrix.

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.

Ausgeschlossene Elemente für Citrix Virtual Apps and Desktops 7 1912 LTSR CU9

Für die folgenden Features, Komponenten und Plattformen können die 1912-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 Komponenten und Features
AppDisks
AppDNA
Citrix SCOM Management Pack
Framehawk
Personal vDisk
StoreFront/Citrix Online-Integration

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.

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 1912 LTSR. 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 1912-LTSR-Kernkomponenten und dem Erstellen einer Site wird der Migrationsprozess in der folgenden Reihenfolge ausgeführt:

- Führen Sie das 1912-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 1912-LTSR-Site importieren.
- Führen Sie PowerShell-Import-Cmdlets auf dem neuen 1912-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

June 27, 2024

Die folgenden Probleme wurden seit Citrix Virtual Apps and Desktops 7 1912 LTSR CU8 behoben:

Citrix Provisioning

Die Dokumentation zu Citrix Provisioning 1912 CU9 enthält Informationen zu den Updates in diesem Release.

Delivery Controller

- Die Aufgabe “Maschinenkatalog erstellen/aktualisieren”schlägt in Verfügbarkeitszone B fehl, funktioniert aber für Verfügbarkeitszone A und C einwandfrei, da eine Volume Service-Instanz in Ihrer Cloud-Verbindung nicht gestartet werden konnte. Führen Sie den folgenden Befehl aus, um die Datenbanktabelle der Site so zu aktualisieren, dass sie das neue VolumeWorkerTemplate auf dem SQL-Server verwendet.


```
UPDATE HostingUnitServiceSchema.VolumeServiceConfigurationBaseTemplate
SET TemplateId = 'ami-09b42976632b27e9b'
WHERE RegionName = 'ap-southeast-2'
```

> **Hinweis:** Die Verfügbarkeitszone kann für verschiedene Kunden unterschiedlich sein.

[CVADHELP-24094]

- Aktualisierungen der `MonitorData.ResourceUtilization`-Tabelle in der Monitoring-Datenbank werden verzögert. [CVADHELP-22724]

Linux Virtual Delivery Agent

Die Dokumentation zu Linux Virtual Delivery Agent 1912 CU9 enthält keine behobenen Probleme.

Metainstaller

- 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.
  Wenn Sie sich mit einem Citrix-Konto oder 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. Zur Verwendung des Tokens das nächste Mal beim Ausführen von Sammeln oder Ablauf verfolgen und reproduzieren 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.
  [CVADHELP-24415]

Profilverwaltung

Die Dokumentation zur Profilverwaltung 1912 CU9 enthält Informationen zu den Updates in diesem Release.

Sitzungsaufzeichnung

Die Dokumentation zur Sitzungsaufzeichnung 1912 CU9 enthält Informationen zu den Updates in diesem Release.

StoreFront

Die Dokumentation zu StoreFront 1912 CU9 enthält Informationen zu den Updates in diesem Release.

Universeller Druckserver

Drucken

- Die Drucker, die mit dem universellen Druckserver verbunden sind, werden während des Druckens möglicherweise in Sitzungen nicht angezeigt. Das Problem tritt auf, wenn die Datei `httpd.conf` im Universal Print Server aktualisiert wird. [CVADHELP-21139]
- Wenn Sie VDA Version 1912 CU5 und OS Version 2012 R2 verwenden, schlagen verschiedene Druckaufträge vom Citrix UPS-Produktionsdruckserver mit der folgenden Fehlermeldung fehl:
  `CCgpStream::Open: WaitForMultipleObjects time out. InternalUpcRemoteOpenSt : Failed to Open Stream. Abort Job.`
  [CVADHELP-22354]

VDA für Einzelsitzungs-OS

Drucken

- Der Versuch, eine Datei über lokale Drucker mit der Citrix Workspace-App für Mac mit macOS Sonoma zu drucken, schlägt möglicherweise mit dieser Fehlermeldung fehl:

  ```
  Error: Printer not activated. Error code -41
  ```

  [CVADHELP-23839]
- Wenn Sie einen VDA neu starten und die Richtlinie “Universeller Druckserver”aktiviert ist, wird der Lastausgleich für universelle Druckserver möglicherweise nicht gestartet. [CVADHELP-23714]
- Lokale Drucker werden beim ersten Start möglicherweise nicht zur Sitzung umgeleitet. Die lokalen Drucker werden jedoch bei nachfolgenden Starts umgeleitet. [CVADHELP-23334]

Sitzung/Verbindung

- `CtxSvcHost` (`CtxSmartCardSvc`) wird möglicherweise unerwartet beendet, wenn Sie sich vom VDA abmelden. [CVADHELP-23172]
- Der Microsoft Teams-Umleitungsschlüssel MSTeamsRedirSupport in der Registrierung `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream` fehlt möglicherweise, wenn Sie sich über eine Benutzersitzung erneut mit einem Benutzergerät verbinden. Das Problem tritt auf, wenn nach wie vor eine RDP-Sitzung besteht. [CVADHELP-19993]
- Wenn Drucker oder Druckserver nicht erreichbar sind, kann die Reaktion auf die An- und Abmeldung einer Sitzung viel Zeit in Anspruch nehmen. [CVADHELP-23637]
- Der Prozess `WebSocketService.exe` kann nach einem VDA-Neustart am Schalttag nicht gestartet werden. [CVADHELP-24771]
- Microsoft Teams 2.1 ist auf dem VDA standardmäßig nicht optimiert. [CVADHELP-24767]

VDA für Multisitzungs-OS

Drucken

- Der Versuch, eine Datei über lokale Drucker mit der Citrix Workspace-App für Mac mit macOS Sonoma zu drucken, schlägt möglicherweise mit dieser Fehlermeldung fehl:

  ```
  Error: Printer not activated. Error code -41
  ```

  [CVADHELP-23839]
- Wenn Sie einen VDA neu starten und die Richtlinie "Universeller Druckserver"aktiviert ist, wird der Lastausgleich für universelle Druckserver möglicherweise nicht gestartet. [CVADHELP-23714]
- Lokale Drucker werden beim ersten Start möglicherweise nicht zur Sitzung umgeleitet. Die lokalen Drucker werden jedoch bei nachfolgenden Starts umgeleitet. [CVADHELP-23334]

Sitzung/Verbindung

- Wenn der Sitzungsaufzeichnungsagent nicht auf dem VDA installiert ist und Sie die PowerShell-Befehle `Get-BrokerSessionRecordingStatus`, `Start-BrokerSessionRecording` und `Stop-BrokerSessionRecording` ausführen, wird der VDA deregistriert und innerhalb weniger Sekunden erneut beim Delivery Controller registriert. Diese Aktion hat keine Auswirkungen auf die bestehenden Sitzungen. Wenn der Sitzungsaufzeichnungsagent auf dem VDA installiert ist, funktionieren die PowerShell-Befehle problemlos. [CVADHELP-23686]

- Der Prozess `WebSocketService.exe` verbraucht möglicherweise mehr Speicher auf den VDAs als erwartet. [CVADHELP-23870]
- `CtxSvcHost` (`CtxSmartCardSvc`) wird möglicherweise unerwartet beendet, wenn Sie sich vom VDA abmelden. [CVADHELP-23172]
- Der Prozess `WebSocketService.exe` kann nach einem VDA-Neustart am Schalttag nicht gestartet werden. [CVADHELP-24771]

Systemausnahmen

- Beim Update eines VDAs von 1912 LTSR CU5 auf CU6 tritt eine schwerwiegende Ausnahme in Wdica.sys mit Bluescreen und Bugcheckcode 0x000000CE auf. [CVADHELP-22365]

Cumulative Update 8 (CU8)

November 30, 2023

Veröffentlichungsdatum: 11. September 2023

Info zu diesem Release

Citrix Virtual Apps and Desktops 7 1912 LTSR Cumulative Update 8 (CU8) behebt mehr als 50 Probleme, die seit Veröffentlichung von 1912 LTSR CU7 gemeldet wurden.

1912 LTSR (Allgemeine Informationen)

1912 LTSR (Informationen zu Features und Upgrades)

Behobene Probleme seit Citrix Virtual Apps and Desktops 7 1912 LTSR CU7

Bekannte Probleme in diesem Release

Veraltete und entfernte Produkte und Features

Berechtigungsdaten des Citrix-Produkts für Subscription Advantage

Downloads

Citrix Virtual Apps and Desktops 7 1912 LTSR CU8

> **Wichtig:**
>
> Die Citrix License Administration Console hat das Ende des Lebenszyklus und das Ende der Unterstützung in Lizenzserver 11.17.2.0_BUILD_40000 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 Citrix Virtual Apps and Desktops-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 Citrix Virtual Apps and Desktops 7 1912 LTSR (Erstrealease) mit besonderem Augenmerk auf 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 1912 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 Citrix Virtual Apps and Desktops 7 1912 LTSR CU8

1912 LTSR-Basiskomponente	Version wie unter "Programme und Funktionen"angezeigt	Hinweise
Einzelsitzungs-VDA	1912.0.8000	
Multisitzungs-VDA	1912.0.8000	
Delivery Controller	1912.0.8000	
Citrix Studio	1912.0.8000	

1912 LTSR-Basiskomponente	Version wie unter “Programme und Funktionen”angezeigt	Hinweise
Citrix Director	1912.0.8000	
Citrix Gruppenrichtlinienverwaltung	7.24.8000	
Citrix Gruppenrichtlinie - clientseitige Erweiterung	7.24.8000	
Citrix StoreFront	1912.0.8000	
Citrix Provisioning	1912.80.iso	
Universeller Druckserver	1912.0.8000	
Sitzungsaufzeichnung	1912.0.8000	
Linux VDA	1912.0.8000	Informationen zu den unterstützten Plattformen finden Sie in der Linux VDA-Dokumentation.
Profilverwaltung	1912.0.8000	
Citrix Verbundauthen-tifizierungsdienst	1912.0.8000	
Browserinhaltsumleitung	15.19.8000	

Kompatible Komponenten für Citrix Virtual Apps and Desktops 7 1912 LTSR CU8

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 1912 LTSR-Umgebung durchzuführen.

Kompatible Komponenten und Features	Version wie unter “Programme und Funktionen”angezeigt
App Layering	22.11
App-Schutzrichtlinien	1912 LTSR CU8
HDX RealTime Optimization Pack	2.9 LTSR CU7
Lizenzserver	11.17.2.0 Build 44000

Kompatible Komponenten und Features	Version wie unter “Programme und Funktionen”angezeigt
Benutzerpersonalisierungslayer	23.6.2
Webplayer für die Sitzungsaufzeichnung	1912.0.8000
Self-Service-Kennwortzurücksetzung	1912.0.8000
Windows 10 32-Bit	Siehe Dokumentation zum Erstrelease.
Workspace Environment Management	2305
XenApp und XenDesktop 7.15 LTSR VDA (aktuelles Release)*	Nur aktuelles kumulatives Update

> **Hinweis:**
>
> Windows 10 32-Bit wird nur für 18 Monate ab der ersten Veröffentlichung von 1912 LTSR unterstützt. Windows 10 32-Bit wird nur unter Windows 10 Enterprise 2019 LTSC unterstützt.
>
> * Die XenApp und XenDesktop 7.15 LTSR VDA-Unterstützung gilt in diesem Fall nur für Windows 7 und Windows 2008 R2. Die Unterstützung für XenApp und XenDesktop 7.15 für LTSR endet am August 2022. Die Citrix Unterstützung für Windows 7 und Windows 2008 R2 endet, wenn Microsoft die Unterstützung für das Betriebssystem einstellt oder wenn die Unterstützung für XenApp und XenDesktop 7.15 LTSR endet, je nachdem, was zuerst eintritt. Weitere Informationen finden Sie in der Citrix Produktmatrix.

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.

Ausgeschlossene Elemente für Citrix Virtual Apps and Desktops 7 1912 LTSR CU8

Für die folgenden Features, Komponenten und Plattformen können die 1912-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 Komponenten und Features
AppDisks
AppDNA
Citrix SCOM Management Pack
Framehawk
Personal vDisk
StoreFront/Citrix Online-Integration

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.

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 1912 LTSR. 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 1912-LTSR-Kernkomponenten und dem Erstellen einer Site wird der Migrationsprozess in der folgenden Reihenfolge ausgeführt:

- Führen Sie das 1912-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 1912-LTSR-Site importieren.
- Führen Sie PowerShell-Import-Cmdlets auf dem neuen 1912-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 24, 2024

Die folgenden Probleme wurden seit Citrix Virtual Apps and Desktops 7 1912 LTSR CU7 behoben:

Citrix Director

- Sobald eine Sitzung eingerichtet wurde, wird der Anzeigename der Maschine auf der Seite “Maschinendetails”in Citrix Director auf den Namen der Bereitstellungsgruppe zurückgesetzt. [CVADHELP-18746]

Citrix Richtlinie

- Der Dienst CseEngine.exe verbraucht möglicherweise mehr Arbeitsspeicher auf den VDAs als erwartet. [CVADHELP-19226]
- Der Richtlinienwert für virtuelle Kanäle **VirtualChannelWhiteList** in der Einstellung HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\VCPolicies ist möglicherweise beschädigt und kann nach dem Neustart nicht auf den VDA angewendet werden. Das Problem tritt auf, wenn Sie Dateien aus dem Ordner C:\ProgramData\Citrix\GroupPolicy löschen oder den Ordnerinhalt ausschneiden und an einem anderen Ort einfügen. [CVADHELP-21420]
- Für die Gruppenrichtlinienmodellierung wird nicht der tatsächliche Wert, sondern der deaktivierte Wert angezeigt. Beispielsweise wird der Wert für **Anzeigespeicherlimit** als deaktiviert und nicht als 65536 KB (tatsächlicher Wert) angezeigt. [CVADHELP-22484]

- Das Anwenden von Citrix Benutzerrichtlinien auf verschiedene Domänen kann fehlschlagen, wenn Sie einen VDA auf Version LTSR CU7 aktualisieren. [CVADHELP-22992]

Citrix Provisioning

Die Dokumentation zu Citrix Provisioning 1912 CU8 enthält Informationen zu den Updates in diesem Release.

Citrix Studio

- Beim Versuch, einer Bereitstellungsgruppe weitere Maschinen hinzuzufügen, wird die Seite zur Maschinenzuteilung möglicherweise ausgeblendet. Benutzer werden daher auf der Seite "Maschinenzuteilung"nicht zugewiesen und die Maschinen werden als **Nicht zugewiesen** angezeigt. [CVADHELP-20000]
- Beim Hinzufügen einer App-V-Anwendung ist das Feld **Bereitgestellt als** möglicherweise leer. Das Problem tritt auf, wenn Sie die Anwendung hinzufügen und den Standardnamen der Anwendung ändern. [CVADHELP-21138]

Delivery Controller

- Wenn Siteaggregation oder Bereitstellungsgruppen mit bestimmten Brokerrichtlinien aktiviert sind, wird beim Starten einer Anwendung oder eines Desktops eine neue Sitzung erstellt, anstatt sich erneut mit der bestehenden Anwendung bzw. dem Desktop zu verbinden. [CVADHELP-19879]
- Wenn der reservierte Arbeitsspeicher kleiner ist als der konfigurierte Arbeitsspeicher, kann das Einschalten einer virtuellen Maschine fehlschlagen, wobei folgende Fehlermeldung angezeigt wird:

  Invalid memory setting: Memory reservation (sched.mem.min) should be equal to memsize (94208). The virtual machine failed to start. Failed to turn on the MemSched module. Error parsing scheduler-specific configuration parameters.

  [CVADHELP-21052]
- Das Erstellen einer neuen Hostverbindung auf dem XenServer-Poolmaster schlägt möglicherweise fehl und es wird diese Fehlermeldung angezeigt:

  Kontakt zum Hostserver kann nicht hergestellt werden. Prüfen Sie, ob die Verbindung eine gültige Hostadresse hat und ob der Hostserver eingeschaltet ist und ordnungsgemäß funktioniert.

Fehler beim Abrufen der XenServer-Hostliste.

[CVADHELP-21320]

- Der Citrix Brokerdienst (Brokerservice.exe) wird möglicherweise unerwartet beendet, nachdem die Verbindung zum Lizenzserver getrennt wurde. [CVADHELP-21615]
- Die Anzahl der in Citrix Studio und Citrix Director angezeigten Sitzungen stimmt möglicherweise nicht überein. Citrix Studio zeigt weniger aktive Sitzungen als Citrix Director. [CVADHELP-21727]
- Bestimmte Citrix XML-Leistungsindikatoren werden möglicherweise nicht im Diagramm zur Leistungsüberwachung angezeigt. [CVADHELP-21785]
- Das Importieren des lokalen Hostcache schlägt möglicherweise fehl und es wird die Ereignis-ID 505 angezeigt. Das Problem tritt auf, wenn Sie den Registrierungswert **XmlStaTicketLifetimeInSeconds** zum Befehl **Set-BrokerServiceConfigurationData** hinzugefügt haben. [CVADHELP-22967]
- Mit diesem Fix wird vSAN 8 durch die Maschinenerstellungsdienste (MCS) unterstützt. [CVADHELP-23415]

Linux Virtual Delivery Agent

Die Dokumentation zu Linux Virtual Delivery Agent 1912 CU8 enthält spezifische Informationen zu den Updates in diesem Release.

Metainstaller

- Wenn Sie VDA für Multisitzungs-OS mit aktivierter Option **Verbindungen mit einer Servermaschine aktivieren** installieren und den VDA dann aktualisieren, wird im Upgradeassistenten nicht der Text **Zusätzliche Komponenten zum Aktivieren vermittelter Verbindungen zu einem Server** angezeigt, sondern **Zusätzliche Komponenten für MCS-Masterimage**.

  > **Hinweis:**
  >
  > Dieser Fix gilt für Citrix Virtual Apps and Desktops 1912 LTSR CU8 und für Upgrades von 1912 LTSR CUs auf 1912 LTSR CU8 und höher. Der Fix gilt jedoch nicht für XenApp und XenDesktop 7.15 LTSR CUs und Upgrades von XenApp und XenDesktop 7.15 LTSR auf Citrix Virtual Apps and Desktops 1912 LTSR CUs.

  [CVADHELP-21557]

Optimierung für Microsoft Teams

- Der Citrix HDX HTML5-Videoumleitungsdienst (WebSocketService.exe) wird bei der Verwendung von Microsoft Teams möglicherweise unerwartet beendet. [CVADHELP-22561]

Profilverwaltung

Die Dokumentation zur Profilverwaltung 1912 CU8 enthält Informationen zu den Updates in diesem Release.

Sitzungsaufzeichnung

Die Dokumentation zur Sitzungsaufzeichnung 1912 CU8 enthält keine behobenen Probleme.

StoreFront

Die Dokumentation zu StoreFront 1912 CU8 enthält Informationen zu den Updates in diesem Release.

VDA für Einzelsitzungs-OS

Installation, Deinstallation, Upgrade

- Nach dem Upgrade eines VDA auf 1912 LTSR CUx oder 2203 LTSR CUx wird der Wert für **ApplicationLaunchWaitTimeoutMS** unter dem Registrierungsschlüssel HKEY_LOCAL_MACHINE\SYSTEM\CurrentC möglicherweise nicht wiederhergestellt. [CVADHELP-22758]

Tastatur

- Auf VDA-Version 1912 CU5, die unter Microsoft Windows 10 Version 21H1 oder 21H2 ausgeführt wird, wird die Tastatur in der HDX-Sitzung möglicherweise nicht korrekt mit dem Endpunkt synchronisiert. [CVADHELP-21534]

Sitzung/Verbindung

- Das Aktivieren von SSL auf VDAs kann fehlschlagen, wenn die Zertifikatsvorlage mit **Key Storage Provider** als **Kryptografieanbieter** erstellt wurde. [CVADHELP-21485]

- Interne Websites bestimmter Drittanbieteranwendungen mit installiertem VDA ermöglichen möglicherweise keinen Zugriff ohne Aufforderung. [CVADHELP-22081]
- Wenn das Protokoll Enlightened Data Transport (EDT) aktiviert ist, bleiben Citrix Sitzungen möglicherweise hängen, wenn Sie den VDA von Version 1912 LTSR CU6 auf Version 1912 LTSR CU7 aktualisieren. [CVADHELP-23370]
- Wenn der Sitzungsaufzeichnungsagent nicht auf dem VDA installiert ist und Sie die PowerShell-Befehle **Get-BrokerSessionRecordingStatus**, **Start-BrokerSessionRecording** und **Stop-BrokerSessionRecording** ausführen, wird die Registrierung des VDA beim Delivery Controller aufgehoben und innerhalb weniger Sekunden wiederhergestellt. Diese Aktion hat keine Auswirkungen auf die bestehenden Sitzungen. Wenn der Sitzungsaufzeichnungsagent auf dem VDA installiert ist, funktionieren die PowerShell-Befehle problemlos. [CVADHELP-23491]

Smartcards

- Wenn Sie eine Sitzung mit einer Smartcard starten und versuchen, eine gesperrte Sitzung zu entsperren, werden Sie möglicherweise aufgefordert, statt einer Smartcard-PIN ein Kennwort einzugeben. Das Problem tritt auf, wenn Sie den Microsoft-Patch KB5018410 installiert haben. [CVADHELP-21665]

Systemausnahmen

- Beim schnellen Anschließen und Entfernen eines USB-Geräts wird auf VDAs möglicherweise der Fehlerprüfcode 000000CA angezeigt. [CVADHELP-21459]
- Während des Sitzungsstarts kann es bei VDAs zu einer schwerwiegenden Ausnahme bei der Initialisierung des benutzerdefinierten virtuellen Kanals für ControlUp kommen und es wird ein blauer Bildschirm angezeigt. [CVADHELP-21885]
- Der HTML5-Videoumleitungsdienst (CtxHdxWebSocketService) wird möglicherweise unerwartet beendet. [CVADHELP-22012]
- Der universelle Citrix PDF-Druckertreiber wird möglicherweise aufgrund eines Fehlers in Modul acfpdfuamd64.dll unerwartet beendet. [CVADHELP-22085]
- Auf VDAs kann es bei Wdica.sys zu einer schwerwiegenden Ausnahme mit Bluescreen kommen. [CVADHELP-22482]
- Der Grafikstatusanzeigeprozess GfxStatusIndicator.exe wird möglicherweise wiederholt beendet. [CVADHELP-23142]

VDA für Multisitzungs-OS

Tastatur

- Wenn Sie zwei Instanzen einer Anwendung öffnen und die Einstellung **DisableToggler** auf fünf Sekunden setzen, müssen Sie möglicherweise etwa 30 Sekunden warten, bevor Sie die zweite Anwendung eingeben. [CVADHELP-22491]

Sitzung/Verbindung

- Der Aufzeichnungsstatus im Sitzungsaufzeichnungsplayer ändert sich nach Abschluss der Aufzeichnung und selbst nach dem Abmelden möglicherweise nicht von **Live** in **Abgeschlossen**. Das Problem tritt unter Microsoft Windows 10 oder in einer veröffentlichten Anwendung auf. [CVADHELP-17556]
- Das Aktivieren von SSL auf VDAs kann fehlschlagen, wenn die Zertifikatsvorlage mit Key Storage Provider als Kryptografieanbieter erstellt wurde. [CVADHELP-21485]
- Das Öffnen von PDF-Dateien mit Adobe Reader DC auf Citrix Servern kann unter Anzeige der folgenden Fehlermeldung fehlschlagen:

  Werfault.exe - Anwendungsfehler

  Die Anwendung konnte nicht korrekt gestartet werden (0xc0000142). Klicken Sie auf OK, um die Anwendung zu schließen.

  [CVADHELP-21779]
- Die Sitzungsaufzeichnung wird möglicherweise fortgesetzt, wenn Sie sich von der Sitzung abgemeldet haben oder wenn die Sitzung unterbrochen wird. [CVADHELP-22097]
- Die Benutzersitzung wird möglicherweise kontinuierlich aktualisiert, wenn Sie eine Linux-Sitzung starten, auf der Ubuntu über "Windows Subsystem for Linux GUI"(WSLg) ausgeführt wird. [CVADHELP-22198]
- Wenn Sie zwei Instanzen einer Anwendung öffnen und die Einstellung **DisableToggler** auf fünf Sekunden setzen, müssen Sie möglicherweise etwa 30 Sekunden warten, bevor Sie die zweite Anwendung eingeben. [CVADHELP-22679]
- Nach dem Upgrade eines VDA von 1912 LTSR CU5 auf CU6 oder CU7 werden die Werte **LogoffCheckerStartupDelayInSeconds** und **SeamlessFlags** unter dem Registrierungsschlüssel HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI möglicherweise nicht wiederhergestellt. [CVADHELP-22783]
- Wenn Sie den DPI-Wert des Clients ändern und sich danach mit einer Sitzung wieder verbinden, wird der neue Wert möglicherweise nicht auf die Sitzung angewendet. [CVADHELP-23007]

- Bei aktiviertem EDT-Protokoll (Enlightened Data Transport) bleiben Citrix Sitzungen möglicherweise hängen, wenn Sie einen VDA von Version 1912 LTSR CU6 auf Version 1912 LTSR CU7 aktualisieren. [CVADHELP-23370]

Smartcards

- Wenn Sie eine Sitzung mit einer Smartcard starten und versuchen, eine gesperrte Sitzung zu entsperren, werden Sie möglicherweise aufgefordert, statt einer Smartcard-PIN ein Kennwort einzugeben. Das Problem tritt auf, wenn Sie den Microsoft-Patch KB5018410 installiert haben. [CVADHELP-21665]

Systemausnahmen

- Der Terminaldienste-Prozess könnte aufgrund eines Fehlers im Modul RPM.dll unerwartet beendet werden. [CVADHELP-21108]
- Der Diensthost-Prozess (svchost.exe) verbraucht auf einem VDA für Multisitzungs-OS möglicherweise mehr Arbeitsspeicher als erwartet, wenn die UiPath Remote Runtime-Komponente installiert ist. [CVADHELP-21678]
- Während des Sitzungsstarts kann es bei VDAs zu einer schwerwiegenden Ausnahme bei der Initialisierung des benutzerdefinierten virtuellen Kanals für ControlUp kommen und es wird ein blauer Bildschirm angezeigt. [CVADHELP-21885]
- Der HTML5-Videoumleitungsdienst (CtxHdxWebSocketService) wird möglicherweise unerwartet beendet. [CVADHELP-22012]
- Der universelle Citrix PDF-Druckertreiber wird möglicherweise aufgrund eines Fehlers in Modul acfpdfuamd64.dll unerwartet beendet. [CVADHELP-22085]
- Beim Update eines VDAs von 1912 LTSR CU5 auf CU6 tritt eine schwerwiegende Ausnahme in Wdica.sys mit Bluescreen und Bugcheckcode 0x000000CE auf. [CVADHELP-22365]
- Auf VDAs kann es bei Wdica.sys zu einer schwerwiegenden Ausnahme mit Bluescreen kommen. [CVADHELP-22482]

Cumulative Update 7 (CU7)

May 10, 2023

Releasedatum: 15. März 2023

Info zu diesem Release

Citrix Virtual Apps and Desktops 7 1912 LTSR Cumulative Update 7 (CU7) behebt mehr als 55 Probleme, die seit Veröffentlichung von 1912 LTSR CU6 gemeldet wurden.

1912 LTSR (Allgemeine Informationen)

1912 LTSR (Informationen zu Features und Upgrades)

Behobene Probleme seit Citrix Virtual Apps and Desktops 7 1912 LTSR CU6

Bekannte Probleme in diesem Release

Veraltete und entfernte Produkte und Features

Berechtigungsdaten des Citrix-Produkts für Subscription Advantage

Downloads

Citrix Virtual Apps and Desktops 7 1912 LTSR CU7

> **Wichtig:**
>
> Die Citrix License Administration Console hat das Ende des Lebenszyklus und das Ende der Unterstützung in Lizenzserver 11.17.2.0_BUILD_40000 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 Citrix Virtual Apps and Desktops-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 Citrix Virtual Apps and Desktops 7 1912 LTSR (Erstrealease) mit besonderem Augenmerk auf 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 1912 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 Citrix Virtual Apps and Desktops 7 1912 LTSR CU7

1912 LTSR-Basiskomponente	Version wie unter "Programme und Funktionen"angezeigt	Hinweise
Einzelsitzungs-VDA	1912.0.7000	
Multisitzungs-VDA	1912.0.7000	
Delivery Controller	1912.0.7000	
Citrix Studio	1912.0.7000	
Citrix Director	1912.0.7000	
Citrix Gruppenrichtlinienverwaltung	7.24.7000	
Citrix Gruppenrichtlinie - clientseitige Erweiterung	7.24.7000	
Citrix StoreFront	1912.0.7000	
Citrix Provisioning	1912.37.iso	
Universeller Druckserver	1912.0.7000	
Sitzungsaufzeichnung	1912.0.7000	
Linux VDA	1912.0.7000	Informationen zu den unterstützten Plattformen finden Sie in der Linux VDA-Dokumentation.
Profilverwaltung	1912.0.7000	
Citrix Verbundauthen-tifizierungsdienst	1912.0.7000	
Browserinhaltsumleitung	15.19.7000	

Kompatible Komponenten für Citrix Virtual Apps and Desktops 7 1912 LTSR CU7

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 1912 LTSR-Umgebung durchzuführen.

Kompatible Komponenten und Features	Version wie unter "Programme und Funktionen"angezeigt
App Layering	22.11
App-Schutzrichtlinien	1912 LTSR CU7
HDX RealTime Optimization Pack	2.9 LTSR CU6
Lizenzserver	11.17.2.0 Build 40000
Benutzerpersonalisierungslayer	22.11.3
Webplayer für die Sitzungsaufzeichnung	1912.0.7000
Teams-Optimierung	1912.12.0
Self-Service-Kennwortzurücksetzung	1912.0.7000
Windows 10 32-Bit	Siehe Dokumentation zum Erstrelease.
Workspace Environment Management	2212
XenApp und XenDesktop 7.15 LTSR VDA (aktuelles Release)*	Nur aktuelles kumulatives Update

> **Hinweis:**
>
> Windows 10 32-Bit wird nur für 18 Monate ab der ersten Veröffentlichung von 1912 LTSR unterstützt. Windows 10 32-Bit wird nur unter Windows 10 Enterprise 2019 LTSC unterstützt.
>
> * Die XenApp und XenDesktop 7.15 LTSR VDA-Unterstützung gilt in diesem Fall nur für Windows 7 und Windows 2008 R2. Die Unterstützung für XenApp und XenDesktop 7.15 für LTSR endet am August 2022. Die Citrix Unterstützung für Windows 7 und Windows 2008 R2 endet, wenn Microsoft die Unterstützung für das Betriebssystem einstellt oder wenn die Unterstützung für XenApp und XenDesktop 7.15 LTSR endet, je nachdem, was zuerst eintritt. Weitere Informationen finden Sie in der Citrix Produktmatrix.

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.

Ausgeschlossene Elemente für Citrix Virtual Apps and Desktops 7 1912 LTSR CU7

Für die folgenden Features, Komponenten und Plattformen können die 1912-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 Komponenten und Features
AppDisks
AppDNA
Citrix SCOM Management Pack
Framehawk
Personal vDisk
StoreFront/Citrix Online-Integration

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.

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 1912 LTSR. 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 1912-LTSR-Kernkomponenten und dem Erstellen einer Site wird der Migrationsprozess in der folgenden Reihenfolge ausgeführt:

- Führen Sie das 1912-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 1912-LTSR-Site importieren.
- Führen Sie PowerShell-Import-Cmdlets auf dem neuen 1912-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

June 26, 2023

Die folgenden Probleme wurden seit Citrix Virtual Apps and Desktops 7 1912 LTSR CU6 behoben:

Citrix Director

- Wenn ein VDA und ein Delivery Controller auf derselben Maschine installiert sind, wird der VDA in der Ansicht **Filter > Maschinen > Alle Maschinen** von Citrix Director möglicherweise nicht angezeigt. [CVADHELP-20271]

Citrix Richtlinie

- Mit diesem Fix wurden mehrere Speicherprobleme behoben. [CVADHELP-19916, CVADHELP-20908, CVADHELP-20909]
- Der Wert der Richtlinieneinstellung wird möglicherweise als **Kpbs** statt als **Kbps**angezeigt. [CVADHELP-21527]

Citrix Provisioning

Die Dokumentation zu Citrix Provisioning 1912 CU7 enthält Informationen zu den Updates in diesem Release.

Citrix Studio

- Versuche, eine neue Citrix Virtual Apps and Desktops-Site mit den Berechtigungen DBCreator, Securityadmin und Public von der Citrix Studio-Konsole aus zu erstellen, schlagen möglicherweise fehl. [CVADHELP-20594]

Delivery Controller

- Citrix Studio zeigt möglicherweise Sicherheits-IDs (SID) der Maschinen anstelle von Kontonamen an, wenn einige Domänencontroller heruntergefahren werden. [CVADHELP-19312]

Linux Virtual Delivery Agent

Die Dokumentation zu Linux Virtual Delivery Agent 1912 CU7 enthält spezifische Informationen zu den Updates in diesem Release.

Lizenzierung

- Das Citrix Studio PowerShell Snap-In “Licensing Administration”kann möglicherweise nicht mit Lizenzservern kommunizieren, wenn starke Verschlüsselungssammlungen zulässig sind. [CVADHELP-20056]

Optimierung für Microsoft Teams

- Microsoft Teams-Anrufe werden möglicherweise kurz nach der ersten Verbindung getrennt. [CVADHELP-20042]

- Der HTML5-Videoumleitungsdienst (CtxHdxWebSocketService) wird möglicherweise unerwartet beendet. [CVADHELP-21074]

Profilverwaltung

Die Dokumentation zur Profilverwaltung 1912 CU7 enthält Informationen zu den Updates in diesem Release.

Sicherheitsprobleme

- Dieser Fix behebt ein Sicherheitsproblem. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX559370.

Sitzungsaufzeichnung

Die Dokumentation zur Sitzungsaufzeichnung 1912 CU7 enthält keine behobenen Probleme.

StoreFront

Die Dokumentation zu StoreFront 1912 CU7 enthält Informationen zu den Updates in diesem Release.

Universeller Druckserver

Server

- Ein Dokument auf dem Citrix Universellen Druckserver kann möglicherweise nicht auf freigegebenen Sitzungsdruckern gedruckt werden. Das Problem tritt nach dem Upgrade von Citrix Virtual Apps and Desktops 1912 LTSR auf CU4 auf. [CVADHELP-19431]

VDA für Einzelsitzungs-OS

Tastatur

- Die virtuelle Tastatur wird in einer veröffentlichten Anwendung möglicherweise nicht automatisch angezeigt, wenn Sie den Cursor in ein bearbeitbares Feld setzen. [CVADHELP-21419]

Sitzung/Verbindung

- Ist die virtualisierungsbasierter Sicherheit aktiviert, wenn Sie mit einem Benutzergerät über Remote-PC-Zugriff auf eine Workstation zugreifen und dann die Verbindung trennen, wird möglicherweise ein schwarzer Bildschirm angezeigt, wenn Sie die Workstation physisch erreichen und sich am System anmelden. [CVADHELP-20342]
- Das Wiederherstellen der Verbindung zu einer Sitzung kann fehlschlagen. [CVADHELP-20439]
- Der Citrix Softwaregrafikprozess (Ctxgfx.exe) wird möglicherweise unerwartet beendet, wenn die Richtlinie **Sitzungswasserzeichen** auf dem VDA aktiviert wird. [CVADHELP-20607]
- Wenn Sie Ihre aktuell verbundene Benutzersitzung von der lokalen Konsole eines physischen VDA aus übernehmen, verbleiben möglicherweise alle oder einige Displays, die an den physischen VDA angeschlossen sind, im Energiesparmodus. [CVADHELP-20619]
- Während der Wiederverbindung der Sitzung verschwindet möglicherweise die Batteriestatusanzeige, wenn das Netzkabel eingesteckt ist. [CVADHELP-20768]
- Wenn Sie einen Monitor anschließen, verschwindet das Seamlessfenster möglicherweise. [CVADHELP-21084]
- In der neuesten Version von Chrome schlägt die Erweiterung für die Browserinhaltsumleitung möglicherweise fehl. Das führt dazu, dass der optimierte Microsoft Teams-Anruf unterbrochen wird. [CVADHELP-21336]

Systemausnahmen

- Bei VDAs kommt es möglicherweise zu einer schwerwiegenden Ausnahme mit angezeigtem Bluescreen, wenn eine Sitzung, die das EDT-Protokoll (Enlightened Data Transport) verwendet, die Verbindung trennt oder wiederherstellt. [CVADHELP-20293]
- Der Prozess wfshell.exe wird möglicherweise aufgrund des fehlerhaften Moduls CtxUiMon.dll unerwartet beendet. [CVADHELP-20312]
- Wenn Microsoft Azure Information Protection (AIP) installiert und Citrix Hook aktiviert ist, werden Microsoft 365-Anwendungen möglicherweise unerwartet beendet. [CVADHELP-20642]
- Der Dienst CseEngine.exe verbraucht möglicherweise mehr Arbeitsspeicher auf den VDAs als erwartet. [CVADHELP-20909]
- Wenn Sie einen veröffentlichten Desktop starten, den **Datei-Explorer** öffnen und unter **Netzwerk >\Client** auf das umgeleitete lokale Laufwerk C klicken, wird der **Datei-Explorer** möglicherweise unerwartet beendet. [CVADHELP-21089]

- Auf VDAs kann es bei tdica.sys zu einer schwerwiegenden Ausnahme mit Bluescreen kommen. Das Problem tritt auf, wenn Sie versuchen, die Verbindung zu einer Sitzung wiederherzustellen. [CVADHELP-21318]

Benutzererfahrung

- Wenn Sie sich über Citrix Gateway anmelden und **LDAP SSO Name Attribute** auf **UserPrincipalName** eingestellt ist, zeigt das Citrix-Wasserzeichen den Anmeldenamen möglicherweise falsch an. [CVADHELP-21815]

VDA für Multisitzungs-OS

Tastatur

- Die virtuelle Tastatur wird in einer veröffentlichten Anwendung möglicherweise nicht automatisch angezeigt, wenn Sie den Cursor in ein bearbeitbares Feld setzen. [CVADHELP-21419]

Drucken

- Auf Mac-Clients wird das Standardpapierformat des Druckers möglicherweise nicht beibehalten, nachdem Sie sich ab- und wieder angemeldet haben. [CVADHELP-21161]

Sitzung/Verbindung

- Wenn Sie als anonymer Benutzer eine Anwendung von einem VDA aus starten, wird möglicherweise die folgende Fehlermeldung angezeigt:

  Incorrect username and password.

  [CVADHELP-19802]

- Der Bildschirmschoner wird möglicherweise in einer wiederverbundenen Sitzung von einer im Seamlessmodus veröffentlichten App angezeigt, die über einen VDA hergestellt wurde, für den der Bildschirmschoner aktiviert ist. [CVADHELP-20431]
- Mit diesem Fix können Sie Platzhalter im Prozesspfad verwenden, wenn Sie virtuelle Kanäle zur Positivliste hinzufügen. Weitere Informationen finden Sie in der Dokumentation zur Sicherheit virtueller Kanäle. [CVADHELP-20478]
- Während der Wiederverbindung der Sitzung verschwindet möglicherweise die Batteriestatusanzeige, wenn das Netzkabel eingesteckt ist. [CVADHELP-20768]

- VDAs reagieren möglicherweise nicht mehr, wenn das RPM einen Abmeldevorgang verzögert, indem es eine Sperre nicht wie erwartet aufhebt. [CVADHELP-20892]
- Das Feature "Positivliste für virtuelle Kanäle"funktioniert möglicherweise nicht in Microsoft Teams. [CVADHELP-21287]
- In der neuesten Version von Chrome schlägt die Erweiterung für die Browserinhaltsumleitung möglicherweise fehl. Das führt dazu, dass der optimierte Microsoft Teams-Anruf unterbrochen wird. [CVADHELP-21336]

Systemausnahmen

- Der Prozess wfshell.exe wird möglicherweise aufgrund des fehlerhaften Moduls CtxUiMon.dll unerwartet beendet. [CVADHELP-20312]
- Der Dienst CseEngine.exe verbraucht möglicherweise mehr Arbeitsspeicher auf den VDAs als erwartet. [CVADHELP-20909]
- Wenn Sie einen veröffentlichten Desktop starten, den **Datei-Explorer** öffnen und unter **Netzwerk >\Client** auf das umgeleitete lokale Laufwerk C klicken, wird der **Datei-Explorer** möglicherweise unerwartet beendet. [CVADHELP-21089]

Benutzererfahrung

- Wenn Sie sich über Citrix Gateway anmelden und **LDAP SSO Name Attribute** auf **UserPrincipalName** eingestellt ist, zeigt das Citrix-Wasserzeichen den Anmeldenamen möglicherweise falsch an. [CVADHELP-21815]

Cumulative Update 6 (CU6)

December 14, 2022

Releasedatum: 31. Oktober 2022

Info zu diesem Release

Citrix Virtual Apps and Desktops 7 1912 LTSR Cumulative Update 6 (CU6) behebt mehr als 35 Probleme, die seit Veröffentlichung von 1912 LTSR CU5 gemeldet wurden.

1912 LTSR (Allgemeine Informationen)

1912 LTSR (Informationen zu Features und Upgrades)

Behobene Probleme seit Citrix Virtual Apps and Desktops 7 1912 LTSR CU5

Bekannte Probleme in diesem Release

Veraltete und entfernte Produkte und Features

Berechtigungsdaten des Citrix-Produkts für Subscription Advantage

Downloads

Citrix Virtual Apps and Desktops 7 1912 LTSR CU6

> **Wichtig:**
>
> Die Citrix License Administration Console hat das Ende des Lebenszyklus und das Ende der Unterstützung in Lizenzserver 11.17.2.0_BUILD_37000 erreicht. Verwenden Sie Citrix Licensing Manager.

Neue Bereitstellungen

Wie stelle ich das CU6 von Grund auf bereit

Mit dem CU6-Metainstaller können Sie eine neue Citrix Virtual Apps and Desktops-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 Citrix Virtual Apps and Desktops 7 1912 LTSR (Erstrealease) mit besonderem Augenmerk auf 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 1912 LTSR. Citrix empfiehlt die Aktualisierung aller LTSR-Komponenten Ihrer Bereitstellung auf CU6. Beispiel: Wenn Citrix Provisioning zur LTSR-Bereitstellung gehört, aktualisieren Sie die Citrix Provisioning-Komponenten auf die CU6-Version. Wenn Citrix Provisioning nicht zu Ihrer Bereitstellung gehört, brauchen Sie es nicht zu installieren oder zu aktualisieren.

Basiskomponenten von Citrix Virtual Apps and Desktops 7 1912 LTSR CU6

1912 LTSR-Basiskomponente	Version wie unter “Programme und Funktionen”angezeigt	Hinweise
Einzelsitzungs-VDA	1912.0.6000	
Multisitzungs-VDA	1912.0.6000	
Delivery Controller	1912.0.6000	
Citrix Studio	1912.0.6000	
Citrix Director	1912.0.6000	
Citrix Gruppenrichtlinienverwaltung	7.24.6000	
Citrix Gruppenrichtlinie - clientseitige Erweiterung	7.24.6000	
Citrix StoreFront	1912.0.6000	
Citrix Provisioning	1912.31.iso	
Universeller Druckserver	1912.0.6000	
Sitzungsaufzeichnung	1912.0.6000	
Linux VDA	1912.0.6000	Informationen zu den unterstützten Plattformen finden Sie in der Linux VDA-Dokumentation.
Profilverwaltung	1912.0.6000	
Citrix Verbundauthen-tifizierungsdienst	1912.0.6000	
Browserinhaltsumleitung	15.19.6000	
Citrix Probe Agent	2009	Herunterladen

Kompatible Komponenten für Citrix Virtual Apps and Desktops 7 1912 LTSR CU6

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 1912 LTSR-Umgebung durchzuführen.

Kompatible Komponenten und Features	Version wie unter “Programme und Funktionen”angezeigt
App Layering	22.08
App-Schutzrichtlinien	1912 LTSR CU6
HDX RealTime Optimization Pack	2.9 LTSR CU5
Lizenzserver	11.17.2.0 Build 40000
Benutzerpersonalisierungslayer	22.6.1
Webplayer für die Sitzungsaufzeichnung	1912.0.6000
Teams-Optimierung	1912.0.0
Self-Service-Kennwortzurücksetzung	1912.0.6000
Windows 10 32-Bit	Siehe Dokumentation zum Erstrelease.
Workspace Environment Management	2206
XenApp und XenDesktop 7.15 LTSR VDA (aktuelles Release)*	Nur aktuelles kumulatives Update

> **Hinweis:**
>
> Windows 10 32-Bit wird nur für 18 Monate ab der ersten Veröffentlichung von 1912 LTSR unterstützt. Windows 10 32-Bit wird nur unter Windows 10 Enterprise 2019 LTSC unterstützt.
>
> * Die XenApp und XenDesktop 7.15 LTSR VDA-Unterstützung gilt in diesem Fall nur für Windows 7 und Windows 2008 R2. Die Unterstützung für XenApp und XenDesktop 7.15 für LTSR endet am August 2022. Die Citrix Unterstützung für Windows 7 und Windows 2008 R2 endet, wenn Microsoft die Unterstützung für das Betriebssystem einstellt oder wenn die Unterstützung für XenApp und XenDesktop 7.15 LTSR endet, je nachdem, was zuerst eintritt. Weitere Informationen finden Sie in der Citrix Produktmatrix.

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.

Ausgeschlossene Elemente für Citrix Virtual Apps and Desktops 7 1912 LTSR CU6

Für die folgenden Features, Komponenten und Plattformen können die 1912-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 Komponenten und Features
AppDisks
AppDNA
Citrix SCOM Management Pack
Framehawk
Personal vDisk
StoreFront/Citrix Online-Integration

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.

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 1912 LTSR. 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 1912-LTSR-Kernkomponenten und dem Erstellen einer Site wird der Migrationsprozess in der folgenden Reihenfolge ausgeführt:

- Führen Sie das 1912-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 1912-LTSR-Site importieren.
- Führen Sie PowerShell-Import-Cmdlets auf dem neuen 1912-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

March 27, 2023

Die folgenden Probleme wurden seit Citrix Virtual Apps and Desktops 7 1912 LTSR CU5 behoben:

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 Richtlinie

- Nach dem Upgrade von Citrix Virtual Apps and Desktops von Version 1912 LTSR CU3 auf CU4 oder CU5 werden VDAs möglicherweise nicht beim Delivery Controller registriert und bleiben nicht registriert. [CVADHELP-19834]
- Eine falsche DNS-Abfrage wird möglicherweise generiert, wenn CseEngine.exe das Gruppenrichtlinienobjekt (GPO) abruft. [CVADHELP-20361]

Citrix Provisioning

Die Dokumentation zu Citrix Provisioning 1912 CU6 enthält Informationen zu den Updates in diesem Release.

Citrix Studio

- Versuche, in Citrix Studio eine Hostingverbindung zu Azure herzustellen, schlagen möglicherweise mit einer Ausnahme fehl. [CVADHELP-18741]
- Vorgänge, bei denen Maschinenkataloge in Citrix Studio zum Einsatz kommen, z. B. das Zugreifen, Erstellen, Entfernen oder Aufzählen von Katalogen, sind möglicherweise langsam. Dieses Problem tritt auf, wenn ein Nutanix-Hypervisor als Host der Verbindung verwendet wird. [CVADHELP-19652]

Delivery Controller

- Der Citrix Broker-Dienst (Brokerservice.exe) reagiert möglicherweise nicht mehr und geht offline. [CVADHELP-16352]
- 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]
- Wenn Sie beim Aktualisieren eines MCS-Katalogs die virtuelle Maschine und anschließend den entsprechenden Snapshot auswählen, wird möglicherweise folgende Fehlermeldung angezeigt:

  Ein unerwarteter Fehler ist aufgetreten. Wenden Sie sich an den technischen Support von Citrix.

  [CVADHELP-17794]
- Das Einschalten einer Maschine kann fehlschlagen, nachdem die Verbindung mit System Center Virtual Machine Manager (SCVMM) wiederhergestellt wurde. [CVADHELP-18400]
- Der Citrix Brokerdienst (Brokerservice.exe) wird möglicherweise aufgrund eines Modulfehlers in LicPolEng.dll unerwartet beendet. [CVADHELP-19674]
- Wenn Sie eine statische IP-Adresse verwenden, um eine Maschine mit VDA-Version 2203 LTSR aus einem Masterimage zu erstellen, wird bei der Image-Vorbereitung möglicherweise DHCP von MCS (Maschinenerstellungsdienste) nicht aktiviert. [CVADHELP-19892]

- Beim Upgrade virtueller Maschinen von Version 1912 LTSR auf Version 1912 LTSR CU2 schlägt die Anmeldung an der Maschine mit den Domänenanmeldeinformationen nach dem ersten Neustart fehl. Die Anmeldung ist jedoch nach einem weiteren Neustart erfolgreich. [CVADHELP-19900]
- Durch diesen Fix werden Basisdatenträgern eindeutige Namen zugewiesen. [CVADHELP-19938]
- Auf dem Delivery Controller kann eine hohe CPU-Auslastung auftreten. Der Energiestatus von VDAs wird daraufhin als unbekannt angezeigt. [CVADHELP-20061]
- Nach dem Upgrade des Delivery Controller auf Version 1912 CU5 kann beim geplanten Neustart von nicht energieverwalteten VDAs ein Fehler auftreten. [CVADHELP-20138]

Linux Virtual Delivery Agent

Die Dokumentation zu Linux Virtual Delivery Agent 1912 CU6 enthält keine behobenen Probleme.

Profilverwaltung

Die Dokumentation zur Profilverwaltung 1912 CU6 enthält Informationen zu den Updates in diesem Release.

Sitzungsaufzeichnung

Die Dokumentation zur Sitzungsaufzeichnung 1912 CU6 enthält keine behobenen Probleme.

StoreFront

Die Dokumentation zu StoreFront 1912 CU6 enthält Informationen zu den Updates in diesem Release.

VDA für Einzelsitzungs-OS

Tastatur

- Die Tastenkombination Strg+Pause funktioniert möglicherweise nicht in Sitzungen, die mit der Citrix Workspace-App für Linux geöffnet wurden. [CVADHELP-19043]
- Eine Linkshändermaus, bei der die primäre Taste auf dem Benutzergerät und dem VDA auf **Links** eingestellt ist, funktioniert möglicherweise nicht wie erwartet. [CVADHELP-19444]

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-17876]
- Die Registrierung von Maschinen wird möglicherweise aufgrund eines Deadlocks im Broker Agent aufgehoben und sie bleiben nicht registriert. [CVADHELP-18952]
- Wenn Sie einen Monitor anschließen oder trennen, ist das Seamlessfenster möglicherweise falsch positioniert. [CVADHELP-19168]
- Zwei VDAs statt einem können einem einzelnen Benutzer zugewiesen werden. [CVADHELP-19700]
- HDX Insights-Daten werden für Benutzersitzungen auf Remote-PC-Zugriff-VDAs nach einer Wiederverbindung möglicherweise nicht aktualisiert. Citrix ADM meldet dann weniger Verbindungen als tatsächlich vorliegen. [CVADHELP-19762]
- Das Starten einer Sitzung schlägt möglicherweise fehl, wenn die Verschlüsselungssammlung **TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384** verwendet wird. [CVADHELP-19796]
- Wenn Sie eine Sitzung beenden, reagiert der Server möglicherweise nicht mehr. Das Problem tritt aufgrund einer Endlosschleife in icausbb.sys auf. [CVADHELP-19814]
- Der Windows-Audiodienst wird möglicherweise nicht automatisch gestartet, wenn Sie Virtual Delivery Agent mit dem Befehlszeilenparameter `servervdi`installieren. Infobereich enthält die Fehlermeldung:

  Der Audiodienst wird nicht ausgeführt.

  [CVADHELP-19823]
- Der Citrix HDX HTML5-Videoumleitungsdienst (WebSocketService.exe) kann bei Verwendung von Microsoft Teams, das für Citrix HDX optimiert ist, ein Sitzungsleck verursachen. [CVADHELP-20058]
- Beim Wiederverbinden mit einer veröffentlichten Anwendung werden möglicherweise zwei veröffentlichte Anwendungen gestartet und der Delivery Controller zeigt als Anwendungsstatus "Anwendung wird nicht ausgeführt"an. [CVADHELP-20476]

Systemausnahmen

- Ein Fehler in CTXCDF kann dazu führen, dass der Windows Management Instrumentation Provider Service (WMIPRVSE.exe) beendet wird und die Ereignis-ID 5612 im Ereignisprotokoll generiert. [CVADHELP-17425]

- Der Prozess WebSocketService.exe wird möglicherweise unerwartet beendet, sodass Microsoft Teams-Anrufe fehlschlagen und folgende Fehlermeldung angezeigt wird:

  Es wird immer noch eine Verbindung mit Remotegeräten hergestellt. Der Anruf ist noch nicht verfügbar.

  [CVADHELP-17758]

- Im Prozess PicaVcHost.exe kann eine Zugriffsverletzung auftreten, worauf der Prozess unerwartet beendet wird. [CVADHELP-18387]
- Sitzungsstarts schlagen möglicherweise fehl und ein grauer Bildschirm wird angezeigt. [CVADHELP-19232]

VDA für Multisitzungs-OS

Tastatur

- Eine Linkshändermaus, bei der die primäre Taste auf dem Benutzergerät und dem VDA auf **Links** eingestellt ist, funktioniert möglicherweise nicht wie erwartet. [CVADHELP-19444]

Sitzung/Verbindung

- Die Registrierung von Maschinen wird möglicherweise aufgrund eines Deadlocks im Broker Agent aufgehoben und sie bleiben nicht registriert. [CVADHELP-18952]
- Bei der Wiedergabe eines Videos mit Windows Media Player werden die Ereignisprotokolle für benutzerdefinierte virtuelle Kanäle möglicherweise nicht in der Ereignisanzeige angezeigt. Dies kann passieren, wenn die Richtlinie "Positivliste für virtuelle Kanäle"aktiviert und der Wert leer ist. [CVADHELP-19525]
- Die TermService-Berechtigung im Registrierungsschlüssel HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Ica\Se wird möglicherweise während der Installation eines VDA unter Citrix Virtual Apps and Desktops 1912 CU nicht wiederhergestellt, was zu Sitzungsfehlern führt. [CVADHELP-19546]
- **HDX Insights**-Daten werden für Benutzersitzungen auf Remote-PC-Zugriff-VDAs nach einer Wiederverbindung möglicherweise nicht aktualisiert. Citrix ADM meldet dann weniger Verbindungen als tatsächlich vorliegen. [CVADHELP-19762]
- Wenn Sie eine Sitzung beenden, reagiert der Server möglicherweise nicht mehr. Das Problem tritt aufgrund einer Endlosschleife in icausbb.sys auf. [CVADHELP-19814]
- Beim Wiederverbinden mit einer veröffentlichten Anwendung werden möglicherweise zwei veröffentlichte Anwendungen gestartet und der Delivery Controller zeigt als Anwendungsstatus "Anwendung wird nicht ausgeführt"an. [CVADHELP-20476]

Systemausnahmen

- Ein Fehler in CTXCDF kann dazu führen, dass der Windows Management Instrumentation Provider Service (WMIPRVSE.exe) beendet wird und die Ereignis-ID 5612 im Ereignisprotokoll generiert. [CVADHELP-17425]
- Sitzungsstarts schlagen möglicherweise fehl und ein grauer Bildschirm wird angezeigt. [CVADHELP-19232]
- Bei der automatischen Wiederverbindung von Clients (ACR) auf Multisitzungs-OS-VDAs wird der Citrix Audioumleitungsdienst möglicherweise unerwartet beendet. [CVADHELP-19694]
- Auf VDAs kann es bei picavc.sys oder picadm.sys zu einer schwerwiegenden Ausnahme mit Bluescreen kommen. [CVADHELP-19897]

Virtual Desktop-Komponenten–Sonstiges

- Der Start von App-V-Anwendungen schlägt möglicherweise auf nicht persistenten Maschinen fehl, wenn der App-V-Cache auf das persistente Laufwerk umgeleitet wird. [CVADHELP-19125]
- Erstellen von App-V-Anwendungen per Einzelverwaltung in Citrix Studio führt zu doppelten Anwendungen in App-V-Paketen. Dies verlangsamt die Anwendungsenumerierung. Das Problem tritt nach dem Upgrade von Citrix Virtual Apps and Desktops 1912 LTSR von Version CU2 zu CU4 auf. Erstellen von App-V-Anwendungen per Einzelverwaltung in Citrix Studio führt zu doppelten Anwendungen in App-V-Paketen. Dies verlangsamt die Anwendungsenumerierung. Das Problem tritt nach dem Upgrade von Citrix Virtual Apps and Desktops 1912 LTSR von Version CU2 zu CU4 auf. [CVADHELP-19603]

Cumulative Update 5 (CU5)

March 15, 2022

Releasedatum: 09. März 2022

Info zu diesem Release

Citrix Virtual Apps and Desktops 7 1912 LTSR Cumulative Update 5 (CU5) behebt mehr als 60 Probleme, die seit Veröffentlichung von 1912 LTSR CU4 gemeldet wurden.

1912 LTSR (Allgemeine Informationen)

1912 LTSR (Informationen zu Features und Upgrades)

Downloads

Citrix Virtual Apps and Desktops 7 1912 LTSR CU5

> **Wichtig:**
>
> Die Citrix License Administration Console hat das Ende des Lebenszyklus und das Ende der Unterstützung in Lizenzserver 11.17.2.0_BUILD_37000 erreicht. Verwenden Sie den Citrix Licensing Manager.

Neue Bereitstellungen

Wie stelle ich das CU5 von Grund auf bereit?

Mit dem CU5-Metainstaller können Sie eine neue Citrix Virtual Apps and Desktops-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 Citrix Virtual Apps and Desktops 7 1912 LTSR (Erstrealease) mit besonderem Augenmerk auf 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 1912 LTSR. Nicht vergessen: Citrix empfiehlt, alle LTSR-Komponenten in Ihrer Bereitstellung auf CU5 zu aktualisieren. Beispiel: Wenn Citrix Provisioning zur LTSR-Bereitstellung gehört, aktualisieren Sie die Citrix Provisioning-Komponenten auf die CU5-Version. Wenn Citrix Provisioning nicht zu Ihrer Bereitstellung gehört, brauchen Sie es nicht zu installieren oder zu aktualisieren.

Basiskomponenten von Citrix Virtual Apps and Desktops 7 1912 LTSR CU5

1912 LTSR-Basiskomponente	Version wie unter “Programme und Funktionen”angezeigt	Hinweise
Einzelsitzungs-VDA	1912.0.5000	
Multisitzungs-VDA	1912.0.5000	
Delivery Controller	1912.0.5000	
Citrix Studio	1912.0.5000	
Citrix Director	1912.0.5000	
Citrix Gruppenrichtlinienverwaltung	7.24.5000	
Citrix Gruppenrichtlinie - clientseitige Erweiterung	7.24.5000	
Citrix StoreFront	1912.0.5000	
Citrix Provisioning	1912.0.25	
Universeller Druckserver	1912.0.5000	
Sitzungsaufzeichnung	1912.0.5000	
Linux VDA	1912.0.5000	Informationen zu den unterstützten Plattformen finden Sie in der Linux VDA-Dokumentation.
Profilverwaltung	1912.0.5000	
Citrix Verbundauthen-tifizierungsdienst	1912.0.5000	
Umleitung des Browserinhalts	15.19.5000	
Citrix Probe Agent	2006	Download

Kompatible Komponenten für Citrix Virtual Apps and Desktops 7 1912 LTSR CU5

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 1912 LTSR-Umgebung durchzuführen.

Kompatible Komponenten und Features	Version wie unter “Programme und Funktionen”angezeigt
App Layering	21.07.0
App-Schutzrichtlinien	1912.0.0
HDX RealTime Optimization Pack	2.9 LTSR CU4
Lizenzserver	11.17.2.0 Build 37000
Benutzerpersonalisierungslayer	21.12.2
Webplayer für die Sitzungsaufzeichnung	1912.0.0
Teams-Optimierung	1912.0.0
Self-Service-Kennwortzurücksetzung	1.1
Windows 10 32-Bit	Siehe Dokumentation zum Erstrelease.
Workspace Environment Management	2112
XenApp und XenDesktop 7.15 LTSR VDA (aktuelles Release)*	Nur aktuelles kumulatives Update

> **Hinweis:**
>
> Windows 10 32-Bit wird nur für 18 Monate ab der ersten Veröffentlichung von 1912 LTSR unterstützt. Windows 10 32-Bit wird nur unter Windows 10 Enterprise 2019 LTSC unterstützt.
>
> * Die XenApp und XenDesktop 7.15 LTSR VDA-Unterstützung gilt in diesem Fall nur für Windows 7 und Windows 2008 R2. Die Unterstützung für XenApp und XenDesktop 7.15 für LTSR endet am August 2022. Die Citrix Unterstützung für Windows 7 und Windows 2008 R2 endet, wenn Microsoft die Unterstützung für das Betriebssystem einstellt oder wenn die Unterstützung für XenApp und XenDesktop 7.15 LTSR endet, je nachdem, was zuerst eintritt. Weitere Informationen finden Sie in der Citrix Produktmatrix.

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.

Ausgeschlossene Elemente für Citrix Virtual Apps and Desktops 7 1912 LTSR CU5

Für die folgenden Features, Komponenten und Plattformen können die 1912-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 Komponenten und Features
AppDisks
AppDNA
Citrix SCOM Management Pack
Framehawk
Personal vDisk
StoreFront/Citrix Online-Integration

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.

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 1912 LTSR. 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 1912-LTSR-Kernkomponenten und dem Erstellen einer Site wird der Migrationsprozess in der folgenden Reihenfolge ausgeführt:

- Führen Sie das 1912-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 1912-LTSR-Site importieren.
- Führen Sie PowerShell-Import-Cmdlets auf dem neuen 1912-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 3, 2022

Die folgenden Probleme wurden seit Citrix Virtual Apps and Desktops 7 1912 LTSR CU4 behoben:

Citrix Provisioning

Die Dokumentation zu Citrix Provisioning 1912 CU5 enthält Informationen zu den Updates in diesem Release.

Citrix Director

- Sobald eine Sitzung eingerichtet wurde, wird der Anzeigename der Maschine auf der Seite “Maschinendetails”in Citrix Director auf den Namen der Bereitstellungsgruppe zurückgesetzt. [CVADHELP-18746]
- Beim Zugriff von einem VDA, bei dem die Systemsprache auf Spanisch eingestellt ist, zeigt Citrix Director möglicherweise falschen Text an. [CVADHELP-18864]

Citrix Studio

- Wenn Sie die StoreFront-Serveradresse über Citrix Studio hinzufügen und sie einer Bereitstellungsgruppe zuweisen, ist der Store standardmäßig auf **OFF** eingestellt. Daher kann nicht auf den Store zugegriffen werden. [CVADHELP-17980]
- 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

- In Umgebungen mit Energieverwaltung werden Verbindungen möglicherweise weiterhin an VDAs vermittelt, die nicht eingeschaltet wurden. [CVADHELP-18374]
- Versuche, neue Administratoren mit PowerShell-Befehlen in Citrix Studio hinzuzufügen, schlagen möglicherweise fehl. [CVADHELP-18573]
- Versuche, Sitzungen in Citrix Studio zu enumerieren oder zu starten, schlagen möglicherweise fehl, wenn SQLs eine hohe CPU-Nutzung hat. Die folgende Fehlermeldung wird angezeigt:

  Ereignis 1201: Die Verbindung zwischen dem Citrix Brokerdienst und der Datenbank wurde unterbrochen.

  [CVADHELP-18875]

Linux Virtual Delivery Agent

Die Dokumentation zu Linux Virtual Delivery Agent 1912 CU5 enthält spezifische Informationen zu den Updates in diesem Release.

Profilverwaltung

Die Dokumentation zur Profilverwaltung 1912 CU5 enthält Informationen zu den Updates in diesem Release.

Sitzungsaufzeichnung

Die Dokumentation zur Sitzungsaufzeichnung 1912 CU5 enthält keine behobenen Probleme.

StoreFront

Die Dokumentation zu StoreFront 1912 CU5 enthält Informationen zu den Updates in diesem Release.

VDA für Einzelsitzungs-OS

Tastatur

- Wenn Sie ein russisches Tastaturlayout auf einem macOS-Gerät verwenden, das an einen VDA unter Windows angeschlossen ist, funktionieren die Tastenkombinationen möglicherweise nicht. [CVADHELP-17788]
- Auf einem Android-Gerät, das an einen VDA mit Version 1912 LTSR CU3 angeschlossen ist, wird die Bildschirmtastatur möglicherweise nicht automatisch angezeigt, wenn Sie ein Texteingabefeld aktivieren. [CVADHELP-18613]
- Wenn Sie Benutzersitzungen starten, wird der generische Input Method Editor (IME) des Clients möglicherweise nicht automatisch eingestellt. Daher synchronisiert sich die Tastatur nicht automatisch mit dem Endpunkt. [CVADHELP-18776]

Drucken

- Wenn Sie dem generischen universellen Drucker eine Richtlinie hinzufügen, wird möglicherweise der generische Citrix Universelle Drucker zum Standarddrucker anstelle des Client-Hauptdruckers. [CVADHELP-18157]
- Die Sitzungsdrucker verschwinden möglicherweise während der Wiederverbindung der Sitzung, sodass auf die VDAs nicht von einem Remotedesktop (RDP) aus zugegriffen werden kann. [CVADHELP-19062]

Sitzung/Verbindung

- Die Audioausgabequalität eines Mikrofons ist bei Verbindungen über Citrix Gateway möglicherweise schlecht. [CVADHELP-16863]
- Wenn Sie eine von einem veröffentlichten Desktop gestartete Sitzung schließen und die VDAs werden auf Google Cloud Platform gehostet, bleibt die Sitzung möglicherweise auf dem VDA aktiv und wird nicht als getrennt angezeigt. [CVADHELP-17923]
- Die folgenden Schritte können dazu führen, dass eine zufällige Zeichenfolge in das E-Mail-Fenster eingegeben wird, wenn sie in einer veröffentlichten Microsoft Outlook-App mit aktiviertem lokalen IME ausgeführt werden:

  - Öffnen Sie das E-Mail-Fenster.
  - Drücken Sie die **Esc**-Taste, um das Dialogfeld **Möchten Sie Ihre Änderungen speichern?** anzuzeigen und geben Sie beliebigen Text ein.
  - Drücken Sie die **Esc**-Taste, um das Dialogfeld zu schließen.

  [CVADHELP-18379]

- Wenn Citrix IME aktiviert ist, reagieren bestimmte Anwendungen von Drittanbietern möglicherweise nicht und Anwendungsstarts in einer Benutzersitzung schlagen möglicherweise fehl. Das Problem tritt aufgrund eines Fehlers im CtxIme-Modul. [CVADHELP-18511]
- Wenn Sie Ihren VDA von XenApp und XenDesktop Version 7.15 CU3 auf CU4 oder auf Citrix Virtual Apps and Desktops Version 1912 LTSR aktualisieren, wird der Registrierungswert **LogoffCheckSysModules** unter dem Registrierungsschlüssel HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet auf den Standardwert zurückgesetzt. [CVADHELP-19214]

Benutzererfahrung

- Eine Linkshändermaus, bei der die primäre Taste auf dem Benutzergerät und dem VDA auf **Links** eingestellt ist, funktioniert möglicherweise nicht wie erwartet. [CVADHELP-17908]

Benutzeroberfläche

- Wenn Sie in einer Umgebung mit mehreren Monitoren den Hauptmonitor auf Hochformat einstellen, werden SAS-Benachrichtigungen möglicherweise um 90 Grad gedreht angezeigt. [CVADHELP-17779]

VDA für Multisitzungs-OS

Tastatur

- Wenn der japanische Eingabemethodeneditor (IME) auf **IME-Modus für beste Erfahrung** eingestellt ist, werden Eingabezeichenfolgen möglicherweise dupliziert. [CVADHELP-18259]
- Auf einem Android-Gerät, das an einen VDA mit Version 1912 LTSR CU3 angeschlossen ist, wird die Bildschirmtastatur möglicherweise nicht automatisch angezeigt, wenn Sie ein Texteingabefeld aktivieren. [CVADHELP-18613]

Drucken

- Wenn Sie dem generischen universellen Drucker eine Richtlinie hinzufügen, wird möglicherweise der generische Citrix Universelle Drucker zum Standarddrucker anstelle des Client-Hauptdruckers. [CVADHELP-18157]
- Die Sitzungsdrucker verschwinden möglicherweise während der Wiederverbindung der Sitzung, sodass auf die VDAs nicht von einem Remotedesktop (RDP) aus zugegriffen werden kann. [CVADHELP-19062]

Sitzung/Verbindung

- In einer veröffentlichten Instanz von Microsoft Edge oder Internet Explorer ist eine mit dem Signaturfeature digital im Webbrowser angewendete Signatur möglicherweise nicht klar zu sehen, wenn bestimmte Drittanbieteranwendungen gestartet werden.

  Zum Aktivieren der Option legen Sie folgenden Registrierungsschlüssel fest:

  HKEY_LOCAL_MACHINE\Software\Citrix\MultiTouch

  Name: PressureValue

  Typ: REG_DWARD

  Wert: 32000 (Dezimal)

  [CVADHELP-18325]
- Wenn Citrix IME aktiviert ist, reagieren bestimmte Anwendungen von Drittanbietern möglicherweise nicht und Anwendungsstarts in einer Benutzersitzung schlagen möglicherweise fehl. Das Problem tritt aufgrund eines Fehlers im CtxIme-Modul. [CVADHELP-18511]
- Wenn die Lizenzen auf dem Lizenzserver erschöpft sind und der **Zusatzkulanzzeitraum** deaktiviert ist, wird möglicherweise ein eingefrorener, schwarzer Bildschirm mit der Fehlermeldung **Zugriff verweigert** angezeigt. [CVADHELP-18712]
- Wenn Sie mit der automatischen Wiederverbindung von Clients die Verbindung zu einer Sitzung wiederherstellen, die auf VDA Version 2109 oder höher ausgeführt wird, werden Audiogeräte möglicherweise nicht der Sitzung zugeordnet. [CVADHELP-18888]
- Wenn Sie eine virtuelle Citrix-Sitzung verlassen, können eines oder mehrere der folgenden Probleme auftreten:
  - Der VDA listet weiterhin die abgebrochene Sitzung und den Prozess logonui.exe auf. Der Prozess logonui.exe kann zwangsweise beendet werden.
  - Die Sitzung wird mit einem leeren Benutzernamen in Citrix Studio angezeigt.
  - Möglicherweise können Sie keine weiteren Sitzungen starten.

[CVADHELP-19182]

Systemausnahmen

- Wenn Sie den BCR-Proxy mit einer PAC-Datei konfigurieren, kann die Browserinhaltsumleitung fehlschlagen. Der Prozess HdxBrowserCef.exe wird dann unerwartet beendet. [CVADHELP-16463]
- Wenn Sie die Remotedesktopverbindung (mstsc.exe) als veröffentlichte Anwendung starten, wird der Prozess CredentialUIBroker.exe möglicherweise unerwartet beendet. [CVADHELP-18694]
- Der Citrix Stack Control Service (SCService64.exe) wird möglicherweise unerwartet beendet. [CVADHELP-18707]
- Microsoft sendet möglicherweise fälschlicherweise die **WTS_REMOTE_CONNECT**-Nachricht, bevor die Verbindungsbenachrichtigung **ConnectNotify**gesendet wird. Infolgedessen können eines oder mehrere der folgenden Funktionsprobleme auftreten:
  - Sitzungen werden möglicherweise unerwartet beendet.
  - Wiederverbindungen von Sitzungen schlagen möglicherweise fehl.
  - RPM Package Manager stürzt möglicherweise ab.

  [CVADHELP-18980]
- Wenn die automatische Wiederverbindung von Clients ausgewählt ist, wird die Sitzung möglicherweise unerwartet geschlossen. [CVADHELP-19268]

Benutzeroberfläche

- In einer Benutzersitzung, die über die Citrix Workspace-App gestartet wurde, können Sie die Sprachleiste möglicherweise nicht ausblenden, selbst wenn Sie die Option **Nein, Sprachleiste ausblenden** festgelegt haben. [CVADHELP-18239]
- Statusmeldungen werden möglicherweise nicht angezeigt, wenn veröffentlichte Ressourcen gestartet werden. [CVADHELP-19070]

Cumulative Update 4 (CU4)

March 15, 2022

Datum der Veröffentlichung: 3. November 2021

Info zu diesem Release

Citrix Virtual Apps and Desktops 7 1912 LTSR Kumulatives Update 4 (CU4) behebt mehr als 70 Probleme, die seit dem Release von 1912 LTSR CU3 gemeldet wurden.

1912 LTSR (Allgemeine Informationen)

1912 LTSR (Informationen zu Features und Upgrades)

Behobene Probleme seit Citrix Virtual Apps and Desktops 7 1912 LTSR CU3

Bekannte Probleme in diesem Release

Veraltete und entfernte Produkte und Features

Berechtigungsdaten des Citrix-Produkts für Subscription Advantage

Downloads

Citrix Virtual Apps and Desktops 7 1912 LTSR CU4

> **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 CU4 von Grund auf bereit?

Mit dem CU4-Metainstaller können Sie eine neue Citrix Virtual Apps and Desktops-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 Citrix Virtual Apps and Desktops 7 1912 LTSR (Erstrealease) mit besonderem Augenmerk auf 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 1912 LTSR. Nicht vergessen: Citrix empfiehlt, alle LTSR-Komponenten in Ihrer Bereitstellung auf CU4 zu aktualisieren. Beispiel: Wenn Citrix Provisioning zur LTSR-Bereitstellung gehört, aktualisieren Sie die Citrix Provisioning-Komponenten auf die CU4-Version. Wenn Citrix Provisioning nicht zu Ihrer Bereitstellung gehört, brauchen Sie es nicht zu installieren oder zu aktualisieren.

Basiskomponenten von Citrix Virtual Apps and Desktops 7 1912 LTSR CU4

1912 LTSR-Basiskomponente	Version wie unter "Programme und Funktionen"angezeigt	Hinweise
Einzelsitzungs-VDA	1912.0.4000	
Multisitzungs-VDA	1912.0.4000	
Delivery Controller	1912.0.4000	
Citrix Studio	1912.0.4000	
Citrix Director	1912.0.4000	
Citrix Gruppenrichtlinienverwaltung	7.24.4000	
Citrix Gruppenrichtlinie - clientseitige Erweiterung	7.24.4000	
Citrix StoreFront	1912.0.4000	
Citrix Provisioning	1912.0.19	
Universeller Druckserver	1912.0.4000	
Sitzungsaufzeichnung	1912.0.4000	
Linux VDA	1912.0.3000	Informationen zu den unterstützten Plattformen finden Sie in der Linux VDA-Dokumentation.
Profilverwaltung	1912.0.4000	
Citrix Verbundauthentifizierungsdienst	1912.0.4000	
Umleitung des Browserinhalts	15.19.4000	
Citrix Probe Agent	2006	Download

Kompatible Komponenten für Citrix Virtual Apps and Desktops 7 1912 LTSR CU4

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 1912 LTSR-Umgebung durchzuführen.

Kompatible Komponenten und Features	Version wie unter “Programme und Funktionen”angezeigt
App Layering	21.07.0
App-Schutzrichtlinien	1912.0.0
HDX RealTime Optimization Pack	2.9 LTSR CU4
Lizenzserver	11.17.2.0 Build 36000
Benutzerpersonalisierungslayer	21.02.0
Webplayer für die Sitzungsaufzeichnung	1912.0.0
Teams-Optimierung	1912.0.0
Self-Service-Kennwortzurücksetzung	1.1
Windows 10 32-Bit	Siehe Dokumentation zum Erstrelease.
Workspace Environment Management	2109
XenApp und XenDesktop 7.15 LTSR VDA (aktuelles Release)*	Nur aktuelles kumulatives Update

> **Hinweis:**
>
> Windows 10 32-Bit wird nur für 18 Monate ab der ersten Veröffentlichung von 1912 LTSR unterstützt. Windows 10 32-Bit wird nur unter Windows 10 Enterprise 2019 LTSC unterstützt.
>
> * Die XenApp und XenDesktop 7.15 LTSR VDA-Unterstützung gilt in diesem Fall nur für Windows 7 und Windows 2008 R2. Die Unterstützung für XenApp und XenDesktop 7.15 für LTSR endet am August 2022. Die Citrix Unterstützung für Windows 7 und Windows 2008 R2 endet, wenn Microsoft die Unterstützung für das Betriebssystem einstellt oder wenn die Unterstützung für XenApp und XenDesktop 7.15 LTSR endet, je nachdem, was zuerst eintritt. Weitere Informationen finden Sie in der Citrix Produktmatrix.

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.

Ausgeschlossene Elemente für Citrix Virtual Apps and Desktops 7 1912 LTSR CU4

Für die folgenden Features, Komponenten und Plattformen können die 1912-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 Komponenten und Features
AppDisks
AppDNA
Citrix SCOM Management Pack
Framehawk
Personal vDisk
StoreFront/Citrix Online-Integration

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.

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 1912 LTSR. 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 1912-LTSR-Kernkomponenten und dem Erstellen einer Site wird der Migrationsprozess in der folgenden Reihenfolge ausgeführt:

- Führen Sie das 1912-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 1912-LTSR-Site importieren.
- Führen Sie PowerShell-Import-Cmdlets auf dem neuen 1912-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

July 8, 2022

Die folgenden Probleme wurden seit Citrix Virtual Apps and Desktops 7 1912 LTSR CU3 behoben:

Citrix Richtlinie

- 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 Provisioning

Die Dokumentation zu Citrix Provisioning 1912 CU4 enthält Informationen zu den Updates in diesem Release.

Citrix Director

- In der On-Premises-Version von Citrix Director und auf der Registerkarte **Überwachung** von Citrix Virtual Apps and Desktops Service wird möglicherweise die folgende Meldung angezeigt, selbst wenn die RDS-Lizenz einwandfrei funktioniert:

  RDS-Lizenzierung hat den Kulanzzeitraum überschritten.

  [CVADHELP-17469]

- Die VDA-Zuweisung zu einer Bereitstellungsgruppe und das Aktivieren der Einstellung **VdaDataCollection** auf dem Delivery Controller können zu sporadischen Neustarts der VDA-Datensammlungs-Engine führen. Das Problem tritt auf, wenn eine der Gruppenrichtlinieneinstellungen aktualisiert wurde. [CVADHELP-18361]
- Die Suche eines Benutzers unter Auswählen eines zugewiesenen oder statischen Desktops ohne aktive Sitzung kann mit der folgenden Fehlermeldung in Citrix Director fehlschlagen:

  Maschinen können nicht abgerufen werden.

  [CVADHELP-18327]

Citrix Studio

- Wenn Sie in einer in Citrix Studio angezeigten Fehlermeldung auf den Link **Lösung suchen** klicken, wird möglicherweise ein falscher Link geöffnet. [CVADHELP-17800]

Delivery Controller

- Wenn die Lizenzierung unterbrochen wird, läuft die Sitzung ggf. für einen Kulanzzeitraum von 30 Tagen weiter. Nach 30 Tagen endet der Kulanzzeitraum und die Verbindung schlägt fehl. [CVADHELP-16487]
- Beim Update von Citrix Virtual Apps and Desktops auf Version 1912 LTSR wird die Konfigurationsdatei Citrix.AzureRmPlugin.dll.config möglicherweise nicht aktualisiert und die Verbindung zu Microsoft Azure Resource Manager schlägt fehl. [CVADHELP-16839]
- Der Delivery Controller kann möglicherweise keine Verbindung zur Datenbank herstellen. Es wird folgende Fehlermeldung angezeigt. Der Fehler führt zu Leistungsproblemen.

Ereignis 1201: Die Verbindung zwischen dem Citrix Brokerdienst und der Datenbank wurde unterbrochen.

Der Fehler tritt auf, wenn eine Mehrzeilentabellenfunktion in SQL, etwa **DAGetSessionUidsInCatalogScope** oder **DesktopGroupScope** in einer Umgebung aufgerufen wird, in der eine große Anzahl von Sitzungen ausführt werden. Wenn beispielsweise 100.000 Sitzungen ausgeführt werden und 100.000 Uid-Einträge in einer Einzeltabelle vorliegen, wird die Leistung beeinträchtigt und die Verbindung schlägt fehl.

[CVADHELP-17021]

- Die Tabelle **MonitorData.[Machine]** in der Überwachungsdatenbank enthält möglicherweise doppelte Einträge. [CVADHELP-17025]
- Das Deaktivieren von Warnungen zum Hypervisorzustand in Citrix Director kann fehlschlagen.

  Zum Implementieren dieses Fixes legen Sie folgenden Registrierungsschlüssel fest:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Monitor\Service\Toggles

  Name: HypervisorMonitoring

  Typ: DWORD

  Wert: 00000000

  [CVADHELP-17218]
- Der Sitetest schlägt möglicherweise fehl, wenn die Netzwerkverbindung zwischen Delivery Controllern in verschiedenen Satellitenzonen blockiert ist. [CVADHELP-17273]
- Ein Bereitstellungsgruppenadministrator, dem ein benutzerdefinierter Bereich zugewiesen ist, kann möglicherweise die Liste der Neustartzeitpläne nicht abrufen oder verwalten. [CVADHELP-17683]
- 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]
- Wenn Sie Citrix Virtual Apps and Desktops auf Version 1912 LTSR aktualisieren und XenServer neu starten, bleiben die virtuellen Maschinen möglicherweise in einem unbekannten Energiestatus hängen und werden in Citrix Studio nicht aktualisiert. [CVADHELP-17750]
- Das Hinzufügen einer Hostingeinheit auf dem Delivery Controller unter Angabe des FQDN in Großbuchstaben als HTTPS-URL oder HTTP-URL kann fehlschlagen. [CVADHELP-17862]

- Das Aktualisieren des Hostingverbindungskennworts für einen Microsoft System Center Virtual Machine Manager (SCVMM)-Hypervisor kann zu einem Timeout führen. [CVADHELP-17909]
- Das Starten oder Neustarten des Citrix Überwachungsdiensts während eines Upgrades kann zu einem Datenbankverbindungsfehler und zum Verlust alter Daten führen. Zur Vermeidung legen Sie die Standardaufbewahrung gemäß Platinum Edition (PLT) fest. [CVADHELP-18069]

Linux Virtual Delivery Agent

Die Dokumentation zu Linux Virtual Delivery Agent 1912 CU4 enthält spezifische Informationen zu den Updates in diesem Release.

Metainstaller

- Bei der Installation oder dem Upgrade eines VDAs wird der Wert SetDisplayRequiredMode des Registrierungsschlüssels HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics möglicherweise gelöscht. [CVADHELP-17031]
- Der Benutzerpersonalisierungslayer wird nicht installiert. [CVADHELP-17672]

Optimierung für Microsoft Teams

- Für Microsoft Teams optimierte Anrufe können fehlschlagen, weil der Prozess ctxsvchost.exe aufgrund eines Fehlers im Modul CtxTeamsSvc.dll unerwartet beendet wird. [CVADHELP-16918]
- Der HTML5-Videoumleitungsdienst (txHdxWebSocketService) wird möglicherweise unerwartet beendet. [CVADHELP-17146]
- Wenn Sie Microsoft Teams im optimierten HDX-Modus in einem veröffentlichten Desktop verwenden, wird die Verbindung bei Audioanrufen möglicherweise getrennt. [CVADHELP-17341]
- Bei dem Versuch, an einem Anruf teilzunehmen, wird der Citrix HDX HTML5-Videoumleitungsdienst (WebSocketService.exe) möglicherweise unerwartet beendet und der Aufruf schlägt fehl. [CVADHELP-17424]

Profilverwaltung

Die Dokumentation zur Profilverwaltung 1912 CU4 enthält Informationen zu den Updates in diesem Release.

Sitzungsaufzeichnung

Die Dokumentation zur Sitzungsaufzeichnung 1912 CU4 enthält Informationen zu den Updates in diesem Release.

StoreFront

Die Dokumentation zu StoreFront 1912 CU4 enthält Informationen zu den Updates in diesem Release.

VDA für Einzelsitzungs-OS

Inhaltsumleitung

- 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. [CVADHELP-17057]
- Bei Verwendung einiger Anwendungen von Drittanbietern verbraucht der Websocketagent.exe möglicherweise einen hohen Prozentsatz der CPU. Das Problem tritt auf, wenn die Richtlinie **Browserinhaltsumleitung** oder **HTML5-Videoumleitung** aktiviert ist. [CVADHELP-17067]
- Dieser Fix ist eine Erweiterung von HdxWebProxy zur Zusammenarbeit mit dessen Blue Coat-Webproxys. [CVADHELP-18078]

Tastatur

- Von EDT MTU Discovery wird möglicherweise eine falsche maximale Übertragungseinheit berechnet, wenn Pfade zwischen VDA und Client asymmetrisch sind. Die Sitzung kann gestartet werden. Die Tastatur und die Maus reagieren jedoch nicht. [CVADHELP-16654]

Sitzung/Verbindung

- Die Registrierung von VDAs wird möglicherweise zeitweise aufgehoben, wenn IPv6 aktiviert ist. [CVADHELP-14847]
- Die Registrierung der VDAs kann bleibend aufgehoben werden. [CVADHELP-16445]
- Nach dem Start einer Sitzung ist in der Audiowiedergabe unter Microsoft Windows möglicherweise ein rotes X zu sehen, das nicht entfernt werden kann. [CVADHELP-16815]

- Die Zwischenablagenzuordnung kann bei der Erstverbindung zwischen virtueller Desktopsitzung und Client blockiert werden. Nach dem Trennen und Wiederherstellen der Verbindung funktioniert die Zwischenablagenzuordnung nur von der virtuellen Desktopsitzung zum Client. [CVADHELP-17039]
- Um benutzerdefinierten Text in einem Wasserzeichen zu aktualisieren, melden Sie sich ab und verbinden Sie sich dann erneut mit der Sitzung. [CVADHELP-17056]
- Wenn Sie für **DPI** einen anderen Wert als 100 % in einem VDA festlegen, wird der **DPI-Wert** möglicherweise auf 100% zurückgesetzt. Das Problem tritt auf, wenn versucht wird, einen Desktop zu sperren. [CVADHELP-17276]
- Wenn die Multistream-Richtlinie aktiviert ist, werden auf Linux-Endpunkten gestartete Sitzungen möglicherweise getrennt. Das Problem tritt bei VDA-Version 1912 LTSR auf. [CVADHELP-17301]
- Wenn Sie Microsoft Teams im optimierten HDX-Modus in einem veröffentlichten Desktop verwenden, wird die Verbindung bei Audioanrufen möglicherweise getrennt. [CVADHELP-17341]
- Die Wiederverbindung mit einer Sitzung bei aktivierter Benutzerpersonalisierungslayer-Richtlinie schlägt möglicherweise fehl. [CVADHELP-17369]
- Die Verwendung einer AMD-Grafikkarte auf einem Einzelsitzungs-VDI-Desktop schlägt möglicherweise fehl. [CVADHELP-17757]
- Citrix Verbindungslizenzen werden verbraucht, wenn Sie Benutzersitzungen trennen, die über einen physischen VDA verbunden waren. [CVADHELP-17802]
- Bei Verwendung einer NVIDIA-GPU übersteigt die Framerate im Vollbildmodus evtl. nicht 60 F/s, selbst wenn die maximale Framerate für den Bildschirm konfiguriert wurde. [CVADHELP-17904]
- Die Option zum Kopieren von Tabellen ist in manchen Anwendungen von Drittanbietern möglicherweise deaktiviert oder nicht verfügbar. Zum Aktivieren der Option legen Sie folgenden Registrierungsschlüssel fest:

  HKEY_LOCAL_MACHINE\CurrentControlSet\Control\Citrix\wfshell\virtual Clipboard

  Name: DisableFileSupport

  Typ: DWORD

  Wert: 00000001

  [CVADHELP-17986]
- Dieser Fix ermöglicht die Protokollierung der Positivliste für virtuelle Kanäle. Weitere Informationen finden Sie unter Sicherheit virtueller Kanäle. [CVADHELP-18129]

Smartcards

- Beim Zugriff auf Smartcards per Microsoft Edge-Browser mit aktiviertem **SFRhook** kann der Prozess msedge.exe unerwartet beendet werden. [CVADHELP-17956]

Systemausnahmen

- 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]
- Microsoft Teams wird möglicherweise nicht optimiert, wenn ein CtxSvcHost.exe-Prozess unerwartet beendet wird. Ursache ist ein Fehler im Citrix HDX-Teams-Umleitungsdienst. [CVADHELP-16946]
- Im Citrix Desktop-Dienst (BrokerAgent.exe) kann eine Zugriffsverletzung auftreten, worauf der Dienst unerwartet beendet wird. [CVADHELP-17055]
- Der HTML5-Videoumleitungsdienst (CtxHdxWebSocketService) wird möglicherweise unerwartet beendet. [CVADHELP-17146]
- Der Prozess wfshell.exe wird möglicherweise unerwartet beendet, sodass Starts veröffentlichter Anwendungen fehlschlagen. [CVADHELP-17310]
- Auf VDAs kann es in icausbb.sys zu einer schwerwiegenden Ausnahme mit Bluescreen und Bugcheckcode 0x3B kommen. [CVADHELP-17339]
- Bei dem Versuch, an einem Anruf teilzunehmen, wird der Citrix HDX HTML5-Videoumleitungsdienst (WebSocketService.exe) möglicherweise unerwartet beendet und der Aufruf schlägt fehl. [CVADHELP-17424]
- Der Prozess winlogon.exe wird möglicherweise unerwartet beendet. Das Problem tritt aufgrund des fehlerhaften Moduls PicaWinlogonHook64.dll auf. [CVADHELP-17651]
- Die Audio- und Videoverbindung in einer für Microsoft Teams optimierten Videokonferenz kann getrennt und der HdxRtcEngine.exe beendet werden. [CVADHELP-17741]

VDA für Multisitzungs-OS

Inhaltsumleitung

- 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. [CVADHELP-17057]

- Dieser Fix ist eine Erweiterung von HdxWebProxy zur Zusammenarbeit mit dessen Blue Coat-Webproxys. [CVADHELP-18078]

Tastatur

- Von EDT MTU Discovery wird möglicherweise eine falsche maximale Übertragungseinheit berechnet, wenn Pfade zwischen VDA und Client asymmetrisch sind. Die Sitzung kann gestartet werden. Die Tastatur und die Maus reagieren jedoch nicht. [CVADHELP-16654]

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]

Sitzung/Verbindung

- Die Registrierung von VDAs wird möglicherweise zeitweise aufgehoben, wenn IPv6 aktiviert ist. [CVADHELP-14847]
- Die Registrierung der VDAs kann bleibend aufgehoben werden. [CVADHELP-16445]
- Bei Verwendung bestimmter Anwendungen von Drittanbietern wird möglicherweise ein schwarzer Bildschirm angezeigt, wenn die Anwendung ein anderes Fenster öffnet. [CVADHELP-16956]
- Die Zwischenablagenzuordnung kann bei der Erstverbindung zwischen virtueller Desktopsitzung und Client blockiert werden. Nach dem Trennen und Wiederherstellen der Verbindung funktioniert die Zwischenablagenzuordnung nur von der virtuellen Desktopsitzung zum Client. [CVADHELP-17039]
- Das Festlegen des Werts von **HideStatusMessages** auf **1**, um die Leiste "Wird gestartet" auszublenden, kann zu einer Fehlfunktion des Registrierungsschlüssels HKEY_LOCAL_MACHINE\Software\M führen. [CVADHELP-17138]
- Wenn die Multistream-Richtlinie aktiviert ist, werden auf Linux-Endpunkten gestartete Sitzungen möglicherweise getrennt. Das Problem tritt bei VDA-Version 1912 LTSR auf. [CVADHELP-17301]
- Wenn Sie Microsoft Teams im optimierten HDX-Modus in einem veröffentlichten Desktop verwenden, wird die Verbindung bei Audioanrufen möglicherweise getrennt. [CVADHELP-17341]
- Manche Anwendungen von Drittanbietern hören in einer Seamlesssitzung möglicherweise auf zu reagieren. [CVADHELP-17309]

- Der Start von SSL-Sitzungen unter Citrix Virtual Apps and Desktops LTSR CU1, CU2 oder CU3 kann mit der folgenden Fehlermeldung fehlschlagen:

  Ihre Sitzung 'Bereitstellungsgruppenname'wurde wegen des Fehlers 3500 nicht erfolgreich gestartet. Wenden Sie sich an Ihren Administrator, um weitere Informationen zu dem Fehler zu erhalten.

  [CVADHELP-17421]

- Der Hooking-Treiber CtxUvi kann bei Verwendung von Docker-Containern entladen werden. [CVADHELP-17614]
- Dieser Fix enthält Verbesserungen an der Positivliste für virtuelle Kanäle. Daher können Sie nur virtuelle Citrix Kanäle in virtuellen App- und Desktop-Sitzungen öffnen. Sie können auch benutzerdefinierte virtuelle Kanäle zur Positivliste über die Richtlinieneinstellungen **Positivliste für virtuelle Kanäle** hinzufügen. [CVADHELP-17918]
- Nach dem Upgrade der Citrix Workspace-App auf Version 1909 oder höher können Sie die Sprachleiste in Seamlesssitzungen möglicherweise nicht ruckelfrei verschieben. [CVADHELP-18118]
- Die Option zum Kopieren von Tabellen ist in manchen Anwendungen von Drittanbietern möglicherweise deaktiviert oder nicht verfügbar. Zum Aktivieren der Option legen Sie folgenden Registrierungsschlüssel fest:

  HKEY_LOCAL_MACHINE\CurrentControlSet\Control\Citrix\wfshell\virtual Clipboard

  Name: DisableFileSupport

  Typ: DWORD

  Wert: 00000001

  [CVADHELP-17986]

- Dieser Fix ermöglicht die Protokollierung der Positivliste für virtuelle Kanäle. Weitere Informationen finden Sie unter Sicherheit virtueller Kanäle. [CVADHELP-18129]

Smartcards

- Beim Zugriff auf Smartcards per Microsoft Edge-Browser mit aktiviertem **SFRhook** kann der Prozess msedge.exe unerwartet beendet werden. [CVADHELP-17956]

Systemausnahmen

- 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]

- Microsoft Teams wird möglicherweise nicht optimiert, wenn ein CtxSvcHost.exe-Prozess unerwartet beendet wird. Ursache ist ein Fehler im Citrix HDX-Teams-Umleitungsdienst. [CVADHELP-16946]
- Im Citrix Desktop-Dienst (BrokerAgent.exe) kann eine Zugriffsverletzung auftreten, worauf der Dienst unerwartet beendet wird. [CVADHELP-17055]
- Der HTML5-Videoumleitungsdienst (CtxHdxWebSocketService) wird möglicherweise unerwartet beendet. [CVADHELP-17146]
- Der Prozess wfshell.exe wird möglicherweise unerwartet beendet, sodass Starts veröffentlichter Anwendungen fehlschlagen. [CVADHELP-17310]
- Bei dem Versuch, an einem Anruf teilzunehmen, wird der Citrix HDX HTML5-Videoumleitungsdienst (WebSocketService.exe) möglicherweise unerwartet beendet und der Aufruf schlägt fehl. [CVADHELP-17424]
- Wenn Sie eine veröffentlichte Anwendung starten, wird winlogon.exe möglicherweise unerwartet beendet und die Benutzersitzung getrennt. [CVADHELP-17602]
- Veröffentlichte universelle Windows-Anwendungen (UWA) werden möglicherweise nicht gestartet. Es wird folgende Ausnahme angezeigt:

  System.Runtime.InteropServices.COMException (0x80270134)

  [CVADHELP-18116]

Cumulative Update 3 (CU3)

March 15, 2022

Veröffentlichungsdatum: 12. Mai 2021

Info zu diesem Release

Citrix Virtual Apps and Desktops 7 1912 LTSR Cumulative Update 3 (CU3) behebt mehr als 80 Probleme, die seit Veröffentlichung von 1912 LTSR CU2 gemeldet wurden.

1912 LTSR (Allgemeine Informationen)

1912 LTSR (Informationen zu Features und Upgrades)

Behobene Probleme seit Citrix Virtual Apps and Desktops 7 1912 LTSR CU2

Bekannte Probleme in diesem Release

Veraltete und entfernte Produkte und Features

Berechtigungsdaten des Citrix-Produkts für Subscription Advantage

Downloads

Citrix Virtual Apps and Desktops 7 1912 LTSR CU3

> **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 CU3 von Grund auf bereit?

Mit dem CU3-Metainstaller können Sie eine neue Citrix Virtual Apps and Desktops-Umgebung basierend auf dem 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 Citrix Virtual Apps and Desktops 7 1912 LTSR (Erstrealease) mit besonderem Augenmerk auf 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 1912 LTSR. Nicht vergessen: Citrix empfiehlt, alle LTSR-Komponenten in Ihrer Bereitstellung auf CU3 zu aktualisieren. Beispiel: Wenn Citrix Provisioning zur LTSR-Bereitstellung gehört, aktualisieren Sie die Citrix Provisioning-Komponenten auf die CU3-Version. Wenn Citrix Provisioning nicht zu Ihrer Bereitstellung gehört, brauchen Sie es nicht zu installieren oder zu aktualisieren.

Basiskomponenten von Citrix Virtual Apps and Desktops 7 1912 LTSR CU3

1912 LTSR-Basiskomponente	Version wie unter "Programme und Funktionen"angezeigt	Hinweise
Einzelsitzungs-VDA	1912.0.3000	
Multisitzungs-VDA	1912.0.3000	
Delivery Controller	1912.0.3000	
Citrix Studio	1912.0.3000	
Citrix Director	1912.0.3000	
Citrix Gruppenrichtlinienverwaltung	7.24.3000	
Citrix Gruppenrichtlinie - clientseitige Erweiterung	7.24.3000	
Citrix StoreFront	1912.0.3000	
Citrix Provisioning	1912.0.13	
Universeller Druckserver	1912.0.3000	
Sitzungsaufzeichnung	1912.0.3000	
Linux VDA	1912.0.3000	Informationen zu den unterstützten Plattformen finden Sie in der Linux VDA-Dokumentation.
Profilverwaltung	1912.0.3000	
Citrix Verbundauthen-tifizierungsdienst	1912.0.3000	
Umleitung des Browserinhalts	15.19.3000	
Citrix Probe Agent	2006	Download

Kompatible Komponenten für Citrix Virtual Apps and Desktops 7 1912 LTSR CU3

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 1912 LTSR-Umgebung durchzuführen.

Kompatible Komponenten und Features	Version wie unter “Programme und Funktionen”angezeigt
App Layering	19.11.0
App-Schutzrichtlinien	1912.0.0
HDX RealTime Optimization Pack	2.9 LTSR
Lizenzserver	11.16.6.0 Build 34000
Benutzerpersonalisierungslayer	19.11.0
Webplayer für die Sitzungsaufzeichnung	1912.0.0
Teams-Optimierung	1912.0.0
Self-Service-Kennwortzurücksetzung	1.1
Windows 10 32-Bit	
Workspace Environment Management	2003.0.0 und höher
XenApp und XenDesktop 7.15 LTSR VDA (aktuelles Release)*	Nur aktuelles kumulatives Update

> **Hinweis:**
>
> Windows 10 32-Bit wird nur für 18 Monate ab der ersten Veröffentlichung von 1912 LTSR unterstützt. Windows 10 32-Bit wird nur unter Windows 10 Enterprise 2019 LTSC unterstützt.
>
> * Die XenApp und XenDesktop 7.15 LTSR VDA-Unterstützung gilt in diesem Fall nur für Windows 7 und Windows 2008 R2. Die Unterstützung für XenApp und XenDesktop 7.15 für LTSR endet am August 2022. Die Citrix Unterstützung für Windows 7 und Windows 2008 R2 endet, wenn Microsoft die Unterstützung für das Betriebssystem einstellt oder wenn die Unterstützung für XenApp und XenDesktop 7.15 LTSR endet, je nachdem, was zuerst eintritt. Weitere Informationen finden Sie in der Citrix Produktmatrix.

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.

Ausgeschlossene Elemente für Citrix Virtual Apps and Desktops 7 1912 LTSR CU3

Für die folgenden Features, Komponenten und Plattformen können die 1912-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 Komponenten und Features
AppDisks
AppDNA
Citrix SCOM Management Pack
Framehawk
Personal vDisk
StoreFront/Citrix Online-Integration

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.

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 1912 LTSR. 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 1912-LTSR-Kernkomponenten und dem Erstellen einer Site wird der Migrationsprozess in der folgenden Reihenfolge ausgeführt:

- Führen Sie das 1912-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 1912-LTSR-Site importieren.
- Führen Sie PowerShell-Import-Cmdlets auf dem neuen 1912-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

March 15, 2022

Die folgenden Probleme wurden seit Citrix Virtual Apps and Desktops 7 1912 LTSR CU2 behoben:

Citrix Director

- Nach der Deinstallation eines VDA bleiben die Namespaces für Citrix Windows Management Instrumentation (WMI) möglicherweise erhalten. [CVADHELP-14965]
- Citrix Director zeigt gelegentlich die folgende Warnung auf dem Delivery Controller an:

  Die `System.ServiceModel.ChannelFactory1 communication object _[<object name>_]` kann nicht geändert werden, solange der Status "Opening"ist.

  [CVADHELP-15801]

- 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]
- Wenn Sie auf der Seite **Director > Filter > Alle Maschinen** eine Maschine auswählen und dann Wartungsvorgänge ausführen, werden die Häkchen für die ausgewählten Maschinen möglicherweise nicht beibehalten. [CVADHELP-16469]
- Beim Extrahieren von Prozessdaten aus der Überwachungs-API werden möglicherweise ungültige Daten angezeigt. Die Prozesserstellungszeit (**ProcessCreationDate**) wird nach der Prozesserfassungszeit (**CollectionDate**) angezeigt, statt davor. [CVADHELP-17092]

Citrix Richtlinie

- Wenn Sie die Citrix Gruppenrichtlinienengine von Version 1.7 auf Version 1912 LTSR aktualisieren, wird die Richtlinie **Druckerzuweisungen** unter **Citrix Benutzerrichtlinien** möglicherweise nicht angezeigt. [CVADHELP-15608]

Citrix Provisioning

Die Dokumentation zu Citrix Provisioning 1912 CU3 enthält Informationen zu den Updates in diesem Release.

Delivery Controller

- Beim Versuch, einen Delivery Controller neu zu starten, wird möglicherweise die Registrierung aller verbundenen VDAs in mehreren Domänen aufgehoben. [CVADHELP-12840]
- 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]

- Der Fix bewirkt, dass die Vorbereitungsmaschine nicht die standardmäßige Cacheablaufzeit (fünf Minuten) verwendet. Der Fix bewirkt Folgendes:
  - Senkt die Ablaufzeit für Maschinen mit unbekanntem Energiezustand (eine Minute).
  - Senkt die Ablaufzeit für Vorbereitungsmaschinen im Übergang zwischen Energiezuständen (fünf Sekunden)
  - Senkt die Ablaufzeit für Vorbereitungsmaschinen, die nicht im Übergang zwischen Energiezuständen sind (eine Minute)
  - Senkt die Ablaufzeit für andere Maschinen (nicht Vorbereitungsmaschinen) im Übergang zwischen Energiezuständen (30 Sekunden)

  [CVADHELP-15678]
- Wenn Sie eine Energieaktion mit PowerShell ausführen, wird die Aktion möglicherweise erfolgreich ausgeführt aber in **Citrix Studio > Protokollierung** als fehlgeschlagen protokolliert. [CVADHELP-15807]
- 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]
- In einer Umgebung mit mehreren Zonen und hoher Latenz kann das Upgrade von XenApp und XenDesktop Version 7.15 LTSR CU5 auf Citrix Virtual Apps and Desktops Version 1912 CU1 mit der folgenden Ausnahme fehlschlagen:

  NullReferenceException

  [CVADHELP-16236]
- Auf einem Delivery Controller wird möglicherweise folgende Fehlermeldung häufig in **Ereignisanzeige > Windows-Protokolle > Anwendung** angezeigt:

  Fehler-ID 505: Fehler bei einem Import in den Citrix Config Sync-Dienst.

  [CVADHELP-16322]
- Die Anmeldung bei einer nicht vermittelten RDP-Sitzung mit UPN-Anmeldeinformationen kann zu einer nicht abgefangenen Ausnahme führen. In 1912 LTSR CU2 wurde eine Namensübersetzung für UPN-Benutzernamen eingeführt. Die Kürzung des Benutzernamens aufgrund des in RDS-Datenstrukturen festgelegten Limits führt zu einem falschen Benutzernamen. Dies führt zu der nicht abgefangenen Ausnahme. [CVADHELP-16510]
- Wenn Sie eine VM-gehostete App starten und dann versuchen, eine zweite VM-gehostete App vom selben VDA aus zu starten, schlägt der Start möglicherweise fehl. Das Problem tritt auf,

wenn der Maschinenkatalog die statische Zuordnung verwendet. [CVADHELP-16829]

Linux Virtual Delivery Agent

Die Dokumentation zu Linux Virtual Delivery Agent 1912 CU3 enthält spezifische Informationen zu den Updates in diesem Release.

Metainstaller

- Bei der Installation oder dem Upgrade eines VDAs wird der Wert SetDisplayRequiredMode des Registrierungsschlüssels HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics möglicherweise gelöscht. [CVADHELP-17031]

Profilverwaltung

Die Dokumentation zur Profilverwaltung 1912 CU3 enthält Informationen zu den Updates in diesem Release.

Sitzungsaufzeichnung

Die Dokumentation zur Sitzungsaufzeichnung 1912 CU3 enthält Informationen zu den Updates in diesem Release.

StoreFront

Die Dokumentation zu StoreFront 1912 CU3 enthält Informationen zu den Updates in diesem Release.

VDA für Einzelsitzungs-OS

Tastatur

- Wenn die Richtlinie zur Zwischenablageumleitung aktiviert ist, kann das Kopieren von Inhalten zwischen einer veröffentlichten Anwendung und einem Endpunkt über die **Kopieren**-Option aus dem Kontextmenü fehlschlagen. Das Problem tritt bei Internet Explorer auf. [CVADHELP-15647]

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]
- Änderungen an der **Lokale Einstellungen** unter **Druckervoreinstellungen** geht möglicherweise verloren, wenn Sie die Änderungen nicht innerhalb von 54 Sekunden speichern. [CVADHELP-15725]
- 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]
- Clientdrucker können bei Herstellung einer Verbindung mit einer gehosteten HDX-Sitzung möglicherweise nicht umgeleitet werden. [[CVADHELP-16279]
- Wird versucht, eine PDF-Datei aus einer über die Citrix Workspace-App für HTML5 gestarteten Sitzung auszudrucken, wird die Datei möglicherweise nicht einwandfrei gedruckt. [CVADHELP-16809]

Sitzung/Verbindung

- Nach dem Upgrade eines VDAs von Version 7.15.2000 auf Version 1912.2000 können die Datenwerte für **EnableReadImageFileExecOptionsExclusionList** aus folgenden Registrierungsschlüsseln verschwinden: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\ und HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook. [CVADHELP-15090]
- Selbst wenn die VDA-Zeitzonenrichtlinie zur Verwendung der serverseitigen Zeitzone konfiguriert ist, wird möglicherweise weiterhin die clientseitige Zeitzone verwendet. [CVADHELP-15395]
- Bei integrierten Surface Pro-Webcams kann ein Fehler auftreten. [CVADHELP-15567]
- Der Citrix HDX HTML5-Videoumleitungsdienst (WebSocketAgent.exe) wird möglicherweise zeitweise angehalten. Eingehende Anrufe werden dann nicht unter Microsoft Teams angezeigt. Der Anrufempfänger erhält außerdem keine Benachrichtigungen. [CVADHELP-15611]
- Nach der Installation eines VDA wird beim Versuch, die Registerkarte **Privater Schlüssel** unter **Zertifikateigenschaften** anzuzeigen, möglicherweise folgende Fehlermeldung angezeigt:

  One or more of the objects properties are missing or invalid.

  [CVADHELP-15703]

- Wenn Sie einen physischen Monitor über einen DisplayPort an einen RemotePC mit physischer NVIDIA-GPU anschließen, wird auf dem Monitor möglicherweise nichts angezeigt. [CVADHELP-16022]
- Wenn Sie eine Verbindung zwischen einem Endpunkt mit Touchscreen und einem VDA-Version 1912 herstellen, funktioniert die Bildschirmtastatur möglicherweise nicht. Das Problem tritt bei nicht als Administrator angemeldeten Benutzern auf, bei denen die UAC auf einem VDA aktiviert ist. [CVADHELP-16045]
- Die Registrierung von VDAs wird möglicherweise aufgehoben, wenn die Konsolensitzung nach dem Trennen der Benutzersitzung sofort neu verbunden wird. [CVADHELP-16152]
- Beim Starten einer VDA-Sitzung auf einem Laptop mit Intel UHD-Grafikkarte wird möglicherweise der Bildschirm grau angezeigt. [CVADHELP-16519]
- Auf Server-VDI-VDAs bietet die Schaltfläche Ein/Aus im **Startmenü** möglicherweise nicht die Option **Trennen**. [CVADHELP-16595]
- Bei Verwendung des generischen IME für Microsoft Windows 10 20H2 mit dem Update KB4586853 wird die Anwendung möglicherweise unerwartet beendet. [CVADHELP-16664]
- Wenn Sie einen Screenshot mit dem Snipping-Tool erstellen oder komplexe Berechnungen (Pivot-Tabelle o. ä.) durchführen, können Leistungsprobleme auftreten. Das Problem tritt auf, wenn Sie den Wert von **CursorShapeChangeMinInterval** des Registrierungsschlüssels HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics auf 50 setzen. [CVADHELP-16718]
- Mit diesem Fix können Sie jetzt in den erweiterten Tastatureinstellungen verschiedene Eingabemethoden für jedes Anwendungsfenster festlegen. [CVADHELP-16731]
- Wenn Sie Remote-PC-Zugriff unter Windows 10 mit dem NVIDIA-Grafikkartenadapter in einer Headless-Konfiguration verwenden, können Wiederverbindungsprobleme auftreten. [CVADHELP-16848]
- Wenn ein nicht-englischer VDA im Leerlauf ist, wird möglicherweise eine Timeoutnachricht mit bedeutungslosem Code angezeigt. [CVADHELP-16880]
- Dieser Fix ist eine Verbesserung von **HdxWebProxy**. Eine Komponente der Browserinhaltsumleitung kann, soweit HTTP-Datenverkehr aus dem Overlay stammt, über Webproxys geleitet werden, die auf Zulassung des HTTP-Datenverkehrs konfiguriert sind. [CVADHELP-17044]

Systemausnahmen

- 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]

- Auf VDAs kann es bei wdica.sys zu einer schwerwiegenden Ausnahme mit Bluescreen kommen. [CVADHELP-16055]
- Das unerwartete Beenden der Terminaldienste kann dazu führen, dass die Registrierung von VDAs aufgehoben wird. Das Problem tritt aufgrund des fehlerhaften Moduls RPM.dll auf. [CVADHELP-16110]
- Auf VDAs kann es beim Remotezugriff zu einer schwerwiegenden Ausnahme mit Bluescreen kommen. Das Problem tritt auf, wenn Sie einen VDA auf einer neuen Maschine installieren und ihn dann neu starten. [CVADHELP-16284]
- Auf VDAs kann es zu einer schwerwiegenden Ausnahme mit Bluescreen und Bugcheckcode 0x0000010D (WDF_VIOLATION) kommen. [CVADHELP-16773]

VDA für Multisitzungs-OS

Tastatur

- Die japanische Tastaturzuordnung funktioniert möglicherweise nicht, wenn sie mit einem Endpunkt mit einem anderen Betriebssystem als Windows verbunden ist. [CVADHELP-15273]
- Wenn die Richtlinie zur Zwischenablageumleitung aktiviert ist, kann das Kopieren von Inhalten zwischen einer veröffentlichten Anwendung und einem Endpunkt über die **Kopieren**-Option aus dem Kontextmenü fehlschlagen. Das Problem tritt bei Internet Explorer auf. [CVADHELP-15647]

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]
- Änderungen an der **Lokale Einstellungen** unter **Druckervoreinstellungen** geht möglicherweise verloren, wenn Sie die Änderungen nicht innerhalb von 54 Sekunden speichern. [CVADHELP-15725]
- 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]
- Das Drucken einer großen Microsoft Excel-Datei über den universellen Citrix-Druckertreiber (UPD) kann während des **Spoolingvorgangs** fehlschlagen. [CVADHELP-16153]

- Wird versucht, eine PDF-Datei aus einer über die Citrix Workspace-App für HTML5 gestarteten Sitzung auszudrucken, wird die Datei möglicherweise nicht einwandfrei gedruckt. [CVADHELP-16809]

Sitzung/Verbindung

- In bestimmten Szenarien stimmt die in Citrix Studio angezeigte Citrix-Produktlizenznutzung nicht mit der im Citrix License Manager angezeigten Lizenznutzung überein. [CVADHELP-14950]
- Nach dem Upgrade eines VDAs von Version 7.15.2000 auf Version 1912.2000 können die Datenwerte für **EnableReadImageFileExecOptionsExclusionList** aus folgenden Registrierungsschlüsseln verschwinden: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\ und HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook. [CVADHELP-15090]
- Selbst wenn die VDA-Zeitzonenrichtlinie zur Verwendung der serverseitigen Zeitzone konfiguriert ist, wird möglicherweise weiterhin die clientseitige Zeitzone verwendet. [CVADHELP-15395]
- Nach der Installation eines VDA wird beim Versuch, die Registerkarte **Privater Schlüssel** unter **Zertifikateigenschaften** anzuzeigen, möglicherweise folgende Fehlermeldung angezeigt:

  One or more of the objects properties are missing or invalid.

  [CVADHELP-15703]
- Beim Wiederverbinden mit einer Sitzung kann der Citrix Audioumleitungsdienst (CtxAudioSvc) fehlschlagen. Das Problem tritt auf, wenn ein Multisitzungs-OS-VDA unter Microsoft Windows 10 Version 2004 oder höher ausgeführt wird. [CVADHELP-15804]
- Wenn Sie eine Verbindung zwischen einem Endpunkt mit Touchscreen und einem VDA-Version 1912 herstellen, funktioniert die Bildschirmtastatur möglicherweise nicht. Das Problem tritt bei nicht als Administrator angemeldeten Benutzern auf, bei denen die UAC auf einem VDA aktiviert ist. [CVADHELP-16045]
- 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]
- Änderungen der Richtlinie "Wasserzeichen"wie **VDA-Hostname einschließen** oder **VDA-IP-Adresse einschließen** sind möglicherweise in der nächsten Sitzung nicht wirksam.

  Legen Sie als Behebung den folgenden Registrierungsschlüssel fest:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\Watermark

  Name: PolicyInterval

  Typ: DWORD

Wert: Gewünschter Wert in Sekunden (z. B. 2 Sekunden)

[CVADHELP-16485]

- Wenn Sie erst ein Fix CVADHELP-12886 anwenden und dann ein Snippingtool einsetzen, kann sich der Speicherverbrauch auf 4 GB erhöhen, wodurch Sitzungen schließlich nicht mehr reagieren. [CVADHELP-16542]
- Wenn Sie einen Screenshot mit dem Snipping-Tool erstellen oder komplexe Berechnungen (Pivot-Tabelle o. ä.) durchführen, können Leistungsprobleme auftreten. Das Problem tritt auf, wenn Sie den Wert von **CursorShapeChangeMinInterva** des Registrierungsschlüssels HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics auf 50 setzen. [CVADHELP-16718]
- Mit diesem Fix können Sie jetzt in den erweiterten Tastatureinstellungen verschiedene Eingabemethoden für jedes Anwendungsfenster festlegen. [CVADHELP-16731]
- Wenn Sie die erste von einem Desktop Viewer auf einem Gerät gestartete Sitzung trennen, wird das Feature zur schnellen Wiederverbindung möglicherweise umgangen, was die Sitzung verlangsamt. [CVADHELP-16953]

Systemausnahmen

- Wenn die Richtlinie **Adaptiver HDX-Transport** aktiviert ist, endet der Terminaldienst möglicherweise nicht, wenn er manuell beendet wird. [CVADHELP-15524]
- 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]
- Auf VDAs kann es bei wdica.sys zu einer schwerwiegenden Ausnahme mit Bluescreen kommen. [CVADHELP-16055]
- Das unerwartete Beenden der Terminaldienste kann dazu führen, dass die Registrierung von VDAs aufgehoben wird. Das Problem tritt aufgrund des fehlerhaften Moduls RPM.dll auf. [CVADHELP-16110]

Virtual Desktop-Komponenten –Sonstiges

- Der Start einer ausführbaren Datei mit einfachem Anführungszeichen im Dateinamen schlägt möglicherweise fehl. [CVADHELP-16104]

Cumulative Update 2 (CU2)

March 15, 2022

Veröffentlichungsdatum: November 2020

Info zu diesem Release

Citrix Virtual Apps and Desktops 7 1912 LTSR Kumulatives Update 2 (CU2) behebt mehr als 100 Probleme, die seit dem Release von 1912 LTSR CU1 gemeldet wurden.

1912 LTSR (Allgemeine Informationen)

1912 LTSR (Informationen zu Features und Upgrades)

Behobene Probleme seit Citrix Virtual Apps and Desktops 7 1912 LTSR CU1

Bekannte Probleme in diesem Release

Veraltete und entfernte Produkte und Features

Berechtigungsdaten des Citrix-Produkts für Subscription Advantage

Downloads

Citrix Virtual Apps and Desktops 7 1912 LTSR CU2

> **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 CU2 von Grund auf bereit?

Mit dem CU2-Metainstaller können Sie eine neue Citrix Virtual Apps and Desktops-Umgebung basierend auf dem 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 Citrix Virtual Apps and Desktops 7 1912 LTSR (Erstrealease) mit besonderem Augenmerk auf 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 1912 LTSR. Citrix empfiehlt die Aktualisierung aller LTSR-Komponenten Ihrer Bereitstellung auf CU2. Beispiel: Wenn Citrix Provisioning zur LTSR-Bereitstellung gehört, aktualisieren Sie die Citrix Provisioning-Komponenten auf die CU2-Version. Wenn Citrix Provisioning nicht zu Ihrer Bereitstellung gehört, brauchen Sie es nicht zu installieren oder zu aktualisieren.

Basiskomponenten von Citrix Virtual Apps and Desktops 7 1912 LTSR CU2

1912 LTSR-Basiskomponente	Version wie unter "Programme und Funktionen"angezeigt	Hinweise
Einzelsitzungs-VDA	1912.0.2000	
Multisitzungs-VDA	1912.0.2000	
Delivery Controller	1912.0.2000	
Citrix Studio	1912.0.2000	
Citrix Director	1912.0.2000	
Citrix Gruppenrichtlinienverwaltung	7.24.2000	
Citrix Gruppenrichtlinie - clientseitige Erweiterung	7.24.2000	
Citrix StoreFront	1912.0.2000	
Citrix Provisioning	1912.0.7	
Universeller Druckserver	1912.0.2000	
Sitzungsaufzeichnung	1912.0.2000	
Linux VDA	1912.0.2000	Informationen zu den unterstützten Plattformen finden Sie in der Linux VDA-Dokumentation.
Profilverwaltung	1912.0.2000	
Citrix Verbundauthen-tifizierungsdienst	1912.0.2000	
Umleitung des Browserinhalts	15.19.2000	

1912 LTSR-Basiskomponente	Version wie unter “Programme und Funktionen”angezeigt	Hinweise
Citrix Probe Agent	2006	Download

Kompatible Komponenten für Citrix Virtual Apps and Desktops 7 1912 LTSR CU2

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 1912 LTSR-Umgebung durchzuführen.

Kompatible Komponenten und Features	Version wie unter “Programme und Funktionen”angezeigt
App Layering	19.11.0
App-Schutzrichtlinien	1912.0.0
HDX RealTime Optimization Pack	2.9 LTSR
Lizenzserver	11.16.6.0 Build 32000
Benutzerpersonalisierungslayer	19.11.0
Webplayer für die Sitzungsaufzeichnung	1912.0.0
Teams-Optimierung	1912.0.0
Self-Service-Kennwortzurücksetzung	1.1
Windows 10 32-Bit	
Workspace Environment Management	2003.0.0 und höher
XenApp und XenDesktop 7.15 LTSR VDA (aktuelles Release)*	Nur aktuelles kumulatives Update

> **Hinweis:**
>
> Windows 10 32-Bit wird nur für 18 Monate ab der ersten Veröffentlichung von 1912 LTSR unterstützt. Windows 10 32-Bit wird nur unter Windows 10 Enterprise 2019 LTSC unterstützt.
>
> * Die XenApp und XenDesktop 7.15 LTSR VDA-Unterstützung gilt in diesem Fall nur für Windows 7 und Windows 2008 R2. Die Unterstützung für XenApp und XenDesktop 7.15 für LTSR endet am August 2022. Die Citrix Unterstützung für Windows 7 und Windows 2008 R2 endet, wenn Microsoft

> die Unterstützung für das Betriebssystem einstellt oder wenn die Unterstützung für XenApp und XenDesktop 7.15 LTSR endet, je nachdem, was zuerst eintritt. Weitere Informationen finden Sie in der Citrix Produktmatrix.

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.

Ausgeschlossene Elemente für Citrix Virtual Apps and Desktops 7 1912 LTSR CU2

Für die folgenden Features, Komponenten und Plattformen können die 1912-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 Komponenten und Features
AppDisks
AppDNA
Citrix SCOM Management Pack
Framehawk
Personal vDisk
StoreFront/Citrix Online-Integration

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.

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 1912 LTSR. 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 1912-LTSR-Kernkomponenten und dem Erstellen einer Site wird der Migrationsprozess in der folgenden Reihenfolge ausgeführt:

- Führen Sie das 1912-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 1912-LTSR-Site importieren.
- Führen Sie PowerShell-Import-Cmdlets auf dem neuen 1912-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 Fixes in 7.15 LTSR CU7, die nicht in 1912 LTSR CU2 sind

Wenn Sie ein Upgrade von 7.15 LTSR CU7 auf 1912 LTSR CU2 in Betracht ziehen, beachten Sie, dass eine kleine Teilmenge von Fixes, die in 7.15 LTSR CU7 enthalten sind, in 1912 LTSR CU2 nicht vorhanden sind. Wenn Ihre Bereitstellung von bestimmten Fixes in 7.15 LTSR CU7 abhängig ist, empfiehlt Citrix, dass Sie diese Liste vor dem Upgrade überprüfen.

- CVADHELP-13287
- CVADHELP-13993

- CVADHELP-14249
- CVADHELP-14428
- CVADHELP-14515
- CVADHELP-14640
- CVADHELP-14740
- CVADHELP-14847
- CVADHELP-14865
- CVADHELP-14870
- CVADHELP-14905
- CVADHELP-14935
- CVADHELP-14950
- CVADHELP-14959
- CVADHELP-14965
- CVADHELP-15248
- CVADHELP-15298
- CVADHELP-15326
- CVADHELP-15536
- CVADHELP-15568
- CVADHELP-15572
- CVADHELP-15598
- CVADHELP-15608
- CVADHELP-15628
- CVADHELP-15724
- CVADHELP-15749
- CVADHELP-15792
- CVADHELP-15893
- CVADHELP-16036
- CVADHELP-16096
- CVADHELP-16097
- CVADHELP-16410
- CVADHELP-16453

Behobene Probleme

Die folgenden Probleme wurden seit Citrix Virtual Apps and Desktops 7 1912 LTSR CU1 behoben:

Citrix Director

- Wenn Sie in Citrix Director den Bericht für eine Bereitstellungsgruppe ohne fehlgeschlagene Verbindung auf der Registerkarte **Fehler** unter **Trends** abrufen, werden die Details korrekt ausgefüllt. Beim Exportieren des Berichts werden allerdings alle Bereitstellungsgruppen, einschließlich derer ohne fehlgeschlagene Verbindungen, möglicherweise als solche mit fehlgeschlagener Verbindung angezeigt. [CVADHELP-14392]
- 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 Director zeigt möglicherweise nicht alle Datensätze an. Nur die obersten 50 Einträge werden in die CSV-Datei exportiert, obwohl auf der Filterseite **Anwendungsinstanzen** mehrere Anwendungsinstanzen aufgeführt werden. [CVADHELP-14783]
- Wenn Sie in Citrix Director den Bericht für eine Bereitstellungsgruppe auf der Registerkarte **Lastauswertungsprogrammindex** abrufen, werden die Details möglicherweise falsch angezeigt. Der Bericht zeigt nicht die Details der ausgewählten Bereitstellungsgruppe, sondern aller Bereitstellungsgruppen an. [CVADHELP-14869]
- Wenn Sie in Citrix Director über **Director-Konsole > Trends > Maschinennutzung** die Maschinennutzung für eine ausgewählte Bereitstellungsgruppe überprüfen, wird der Wert als 0 (Null) angezeigt. Das Problem tritt auf, wenn Sie eine Bereitstellungsgruppe unter **Maschinen mit Multisitzungs-OS** auswählen. Das Problem tritt nur bei der Spalte Verwendet auf. [CVADHELP-15136]
- Die Integration von NetScaler Management and Analytics System (MAS) in Citrix Director schlägt möglicherweise fehl. Der Befehl C:\inetpub\wwwroot\Director\bin..\DisplayConfig\HdxInsightPlugin\HdxIn schlägt daraufhin fehl, und es wird die folgende Meldung angezeigt:

  Could not perform the logon operation and inner exception: The remote server returned an error: (400) Bad Request.

  [CVADHELP-15219]
- Wenn Sie eine Sitzung auf Version 1912 LTSR oder 1912 LTSR CU1 des VDA im Schatten spiegeln, wird der Prozess der Microsoft-Remoteunterstützung (msra.exe) möglicherweise unerwartet beendet. [CVADHELP-15230]
- Bei der Konsolidierungsaufgabe für die Sitzungsaktivität kann ein Timeout auftreten, was sich auf die Benutzererfahrung auswirkt. [CVADHELP-15305]

- Die Tabelle der anwendungsbasierten Nutzung für eine Bereitstellungsgruppe pro Zeitraum auf der Registerkarte **Kapazitätsverwaltung> Nutzung gehosteter Anwendungen** enthält möglicherweise falsche Nutzungsdaten. [CVADHELP-15368]

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]
- Nach einem VDA-Upgrade von CU 2005 auf Version 2006 wird die Gruppenrichtlinienengine (CseEngine.exe) möglicherweise unerwartet beendet und der Ausnahmecode 0xc0000409 wird angezeigt. [CVADHELP-15363]
- Wenn Sie in Citrix Studio versuchen, eine Citrix Richtlinie zu erstellen oder zu ändern, wird folgende Fehlermeldung auf der Registerkarte “Protokollierung”angezeigt:

  Fehler beim Versuch, Details zur Richtlinienänderung zu ermitteln.

  Die Richtlinie wird korrekt angewendet, doch Sie können nicht ermitteln, wer die Einstellungen geändert hat. Das Problem tritt auf, wenn Sie Citrix Virtual Apps and Desktops von Version 1912 LTSR CU1 auf Version 1912 LTSR aktualisieren. [CVADHELP-15726]

Citrix Provisioning

Die Dokumentation zu Citrix Provisioning 1912 CU2 enthält Informationen zu den Updates in diesem Release.

Citrix Studio

- 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-10932]
- Wenn Sie Studio als veröffentlichte App ausführen, hört es möglicherweise auf zu reagieren. [CVADHELP-14207]

- Auf der Seite **Maschinenzuteilung** fehlen möglicherweise einige Kontrollkästchen. Das Problem tritt auf, wenn Sie versuchen, Maschinen zu einer Bereitstellungsgruppe oder einem Maschinenkatalog hinzuzufügen, der eine oder mehrere vom Benutzer zugewiesene Maschinen enthält. [CVADHELP-15684]
- Dieser Fix ersetzt die folgenden Registrierungseinstellungen durch eine Studio-Richtlinie:
  - **Client-Tastaturlayoutsynchronisierung und Verbesserung des IME:** Aktiviert oder deaktiviert die dynamische Tastaturlayoutsynchronisierung und IME.
  - **Unicode-Tastaturlayoutzuordnung aktivieren:** Aktiviert oder deaktiviert die Unicode-Tastaturzuordnung.
  - **Meldungsfeld für Tastaturlayoutwechsel ausblenden:** Blendet das Meldungsfeld für Tastaturlayoutwechsel aus oder ein.

  [CVADHELP-15706]
- Beim Erstellen einer Hostingverbindung mit Azure schlagen Versuche, einen Dienstprinzipal zu erstellen, möglicherweise mit dem Fehler **ADSTS700016** fehl. [CVADHELP-16219]

Delivery Controller

- 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]
- Wenn Sie Maschinenkataloge mithilfe der Maschinenerstellungsdienste aktualisieren, wird der vorherige Basisdatenträgerordner möglicherweise nicht aus dem **VMware-Speicher** gelöscht. [CVADHELP-14264]
- Die Tabelle **MonitorData.[Benutzer]** in der Überwachungsdatenbank kann Daten möglicherweise nicht mit Active Directory synchronisieren. Außerdem sind der Benutzername, der Anzeigename und die UPN-Informationen in der Tabelle veraltet. [CVADHELP-14700]
- Versuche, Anwendungen zu starten, schlagen möglicherweise fehl. Viele Zugriffsanforderungen für die Tabelle **Chb_State.Sessions** werden blockiert. [CVADHELP-14876]
- 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]
- Mit diesem Fix unterstützt Azure Maschinen des Typs NV4as_v4. [CVADHELP-15317]
- Mit diesem Fix werden die v1-Schlüsselverweise auf den Director- und Überwachungsdienst entfernt. [CVADHELP-15327]
- Nach dem Upgrade eines VDA auf Version 1912 LTSR CU1 wird der Benutzername eines nicht vertrauenswürdigen Benutzers, der sich an einer Maschine anmeldet, als **Domain\UPN** statt **Domain\Username** angezeigt. [CVADHELP-15440]
- Wenn Citrix Analytics zu Leistungszwecken in Citrix Director aktiviert ist, kann es zu einem Arbeitsspeicherverlust im Überwachungsdienst kommen. [CVADHELP-15607]
- Wenn ein Tabellenspeicherkonto fehlt, können Sie weiterhin 15 Minuten lang die einzelnen Datensätze für jede Maschine alle 20 Sekunden lesen. Danach reagiert der Energiezustand nicht mehr. [CVADHELP-15677]
- Der Download von Snapshots kann bei Verwendung von Microsoft Azure fehlschlagen. [CVADHELP-15679]
- Dieser Fix sorgt dafür, dass MCS von Microsoft System Center Virtual Machine Manager (SCVMM) 2019 unterstützt wird.

  [CVADHELP-15779]
- Änderungen am Parameter `DefaultInstall` ermöglichen, dass Sie Microsoft System Center Configuration Manager (SCCM) verwenden, um die Machine Creation Services I/O (MCSIO) unter einem Systemkonto zu installieren. [CVADHELP-15593]
- Der Versuch, einen Desktop zu starten, kann fehlschlagen, wenn die Energieaktion vom Delivery Controller gesendet wird. Die Energieaktion schlägt mit der folgenden Ausnahme fehl:

  System.Runtime.Remoting.RemotingException

  [CVADHELP-15835]
- Dieser Fix bietet die folgenden Vorteile:
  - **Unterstützung für Azure Standard SSD-Datenträger**. Beim Erstellen eines Katalogs können Citrix Virtual Apps and Desktops-Administratoren "Standard-SSD"als Datenträgertyp für gepoolte und persistente Kataloge auswählen.
  - **Gestattet Azure-Unterstützung für die sichere Übertragung in Azure-Speicher** Die Option "Sichere Übertragung erforderlich"erhöht die Sicherheit von Speicherkonten, indem nur von sicheren Verbindungen auf die Konten zugegriffen werden kann.
  - **Behebung eines Problem beim Caching des Energiezustands**. Die Synchronisierung des Energiezustands dauert nur noch 5 anstelle von 20 Minuten.

  - **Unterstützt das Entfernen von Beschränkungen bei der Energieverwaltung**. Sie können 1000 VMs in 12 Minuten einschalten. Zuvor dauerte das 1 Stunde.
  - Durch diesen Fix begrenzt Azure Resource Manager Anforderungen von Abonnements und Mandanten durch das Routing von Datenverkehr gemäß Grenzwerten, die auf die spezifischen Anforderungen des Anbieters zugeschnitten sind.

  [CVADHELP-15392]

- Der Energiezustand virtueller Maschinen, den der Citrix Brokerdienst empfängt, ist möglicherweise falsch und führt zu Fehlern beim Sitzungsstart. Das Problem tritt auf, wenn der Controller die virtuellen Maschinen nicht ordnungsgemäß aus- und wieder einschalten kann. [CVADHELP-15864]
- Wenn Sie viele Maschinen mit einem Microsoft Azure-Plug-In verwalten oder aus- und wieder einschalten, können Remotingausnahmen auftreten. [CVADHELP-16103]

Linux VDA

Die Dokumentation zum Linux VDA 1912 CU2 enthält Informationen zu den Updates in diesem Release.

Metainstaller

- Beim Ausführen des Installationsprogramms VDAServerSetup_1912.exe kann eine Ausnahme auftreten. [CVADHELP-14457]
- 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

Die Dokumentation zur Profilverwaltung 1912 CU2 enthält Informationen zu den Updates in diesem Release.

Sitzungsaufzeichnung

Die Dokumentation zur Sitzungsaufzeichnung 1912 CU2 enthält Informationen zu den Updates in diesem Release.

StoreFront

Die Dokumentation zu StoreFront 1912 CU2 enthält Informationen zu den Updates in diesem Release.

Probleme mit Drittanbieterprodukten

- Ein Problem in Microsoft Windows 10 Version 1809 kann bei Verwendung des Surface Pro mit Surface Book-Stift zu leicht unberechenbarem Verhalten führen. [HDX-17649]

VDA für Einzelsitzungs-OS

Installation, Deinstallation, Upgrade

- Beim Upgrade eines VDAs wird der Registrierungsschlüssel **MaxVideoMemoryBytes** möglicherweise auf den Standardwert zurückgesetzt. [CVADHELP-13629]

Tastatur

- Wenn Sie die **Windows-Taste + P** drücken, um die Projekt-Randleiste anzuzeigen, zeigen alle verbundenen Bildschirme möglicherweise einen schwarzen Hintergrund an, bis Sie die Esc-Taste drücken. Das Problem tritt auf, wenn **Transparentes Schlüsselpassthrough** in einer Seamlesssitzung aktiviert ist. [CVADHELP-14949]
- Bei Remote-PC-Zugriff-Bereitstellungen funktionieren Tastatureingaben möglicherweise nicht in Sitzungen, die unter einem anderen Betriebssystem als Windows ausgeführt werden. [CVADHELP-15291]
- Wenn die F5-Taste als Tastaturküzel für die Funktion **Activate Terminal Node** in CATIA V5 Digital Mockup (DMU) konfiguriert ist, kann das Wiederverbinden mit einer Sitzung die entsprechende Funktion auslösen. [CVADHELP-15402]

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 mehrere USB-Geräte an eine Sitzung umgeleitet werden, funktioniert eines von ihnen möglicherweise nicht ordnungsgemäß. [CVADHELP-12516]

- 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]

- Wenn Sie die Einstellung **Hoher DPI-Wert** so konfigurieren, dass die native Auflösung anstelle eines hohen DPI-Werts verwendet wird, stimmt die DPI-Skalierung zwischen VDA und Benutzergerät möglicherweise nicht überein. Das Problem tritt während der ersten Verbindung auf. [CVADHELP-13205]
- 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]
- Nach dem Neustart eines VDAs funktioniert die USB-Umleitung mit Hardwareverschlüsselung möglicherweise nicht. [CVADHELP-13336]
- 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]
- Wenn Sie die HDX RealTime-Webcamvideokomprimierung verwenden, zeigt eine Webcam möglicherweise statt eines Live-Bildes einen schwarzen Bildschirm an. [CVADHELP-13877]
- 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]
- 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]

- Beim ersten Start einer VDI-Sitzung auf einem 4K-Monitor wird die Sitzung möglicherweise mit einer niedrigeren Auflösung angezeigt. Unter Umständen wird auch ein grauer Rand um das Sitzungsfenster angezeigt. Das Problem tritt bei Geräten mit Grafikkarten bestimmter Drittanbieter auf. [CVADHELP-14401]
- Der Citrix Softwaregrafikprozess (Ctxgfx.exe) verbraucht möglicherweise kontinuierlich Speicher in einer Sitzung. [CVADHELP-14509]

- Wenn Sie VDA Version 1912 oder Version 7.15 CU5 auf einer physischen Maschine installieren, erfasst Windows Management Instrumentation (WMI) diese nicht als virtuelle physische Maschine, sondern als virtuelle Maschine. Microsoft System Center Configuration Manager (SCCM) erfasst die Maschine als virtuelle Maschine und nicht als physische Maschine. Das Problem tritt auf, wenn die Microsoft-Richtlinie **Virtualisierungsbasierte Sicherheit aktivieren** auf **EIN** festgelegt ist.

  Zum Implementieren dieses Fixes legen Sie folgenden Registrierungsschlüssel fest:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\XdMonitor

  Name: IsVDARunningOnVM

  Typ: DWORD

  Wert: 00000000

  [CVADHELP-14597]

- Wenn Sie auf einem VDA von einem Multimonitor-Thin Client erneut eine Verbindung mit einem Einzelmonitor-Thin Client herstellen, wird das Monitorlayout möglicherweise nicht aktualisiert. [CVADHELP-14646]
- Einige 32-Bit-Scananwendungen von Drittanbietern funktionieren möglicherweise nicht auf einem VDA, wenn sie mithilfe der generischen USB-Umleitung an den VDA umgeleitet werden. Das Problem tritt auf, wenn die Scananwendungen auf dem VDA den TWAIN DSM verwenden. Das Problem kann auch auf einem VDA mit Remote-PC-Zugriff auftreten. [CVADHELP-14698]
- Wenn ein Benutzer per Remote-PC-Zugriff auf einen Büro-PC zugreift, wird die Remotesitzung möglicherweise auch auf dem Büro-PC angezeigt. Dadurch werden Sitzungsaktivitäten sichtbar. [CVADHELP-14893]
- Die Optimierung für Microsoft Teams funktioniert möglicherweise nicht in Microsoft Teams. Das Problem tritt auf, wenn Citrix HDX nicht verbunden ist. [CVADHELP-14967]
- Dieser Fix bietet einen Timer zum Senden eines kleinen Datagramms über eine UDP-Verbindung, um die Verbindung zwischen Host und Client aufrechtzuerhalten.

  Um den Fix zu aktivieren, erstellen Sie die Registrierungseinstellung wie folgt:

  - *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]

- Eine Sitzung wird möglicherweise getrennt, wenn Sie den Desktop maximieren, minimieren oder die Größe ändern. Das Problem tritt auf einem VDA für Einzelsitzungs-OS Version 1912 CU1 mit Microsoft Windows 10 Version 1809 auf. [CVADHELP-15200]
- Wenn der CtxUvi Hooking-Treiber deaktiviert ist, werden möglicherweise keine Ereignisprotokolle generiert. Das Problem tritt auf, wenn nur wenige Systemressourcen verfügbar sind. [CVADHELP-15241]
- Wenn Sie versuchen, sich erneut mit einer neuen virtuellen Maschine zu verbinden, wird möglicherweise die folgende Microsoft .NET Framework-Fehlermeldung angezeigt:

  Error Unhandled exception has occurred in your application

  [CVADHELP-15267]
- Die neuesten virtuellen Kanäle werden möglicherweise nicht zur internen hartcodierten Positivliste hinzugefügt. Wenn Sie die Positivliste aktivieren, funktionieren solche neuen virtuellen Kanäle nicht mehr, es sei denn, sie werden der benutzerdefinierten Positivliste hinzugefügt. [CVADHELP-15296]
- Mit diesem Fix wird eine Warnmeldung für Arbeitsstations-VDAs angezeigt, bevor eine Sitzung aufgrund eines Leerlauftimeouts getrennt wird. [CVADHELP-15319]
- 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 Legacygrafikmodus-Richtlinie aktiviert ist, wird bei Sitzungsstart möglicherweise ein grauer Bildschirm angezeigt. Dieses Problem tritt bei VDA-Version 7.15.6000 auf. [CVADHELP-15841]
- Mit diesem Fix ist der WTS-Hook standardmäßig aktiviert, wenn Sie das Flag auf 0x80000000 setzen. [CVADHELP-15929]
- Folgende Probleme können bei Microsoft Teams auftreten:
  - Wenn Sie eine Sitzung wieder verbinden, wird der Prozess HdxTeams.exe möglicherweise nicht gestartet. Das Problem tritt auf VDAs unter Microsoft Windows Server auf.
  - Der Citrix HDX-Teams-Umleitungsdienst (TeamsSvcs) erhält möglicherweise keine Benutzersitzungs-ID. Dadurch bleibt die Aktualisierung des Registrierungsschlüssel für die Microsoft Teams-Umleitung aus.
  - Wenn Sie eine Sitzung wieder verbinden, wird der Citrix HDX-Teams-Umleitungsdienst (TeamsSvcs) möglicherweise unerwartet beendet.

  [CVADHELP-16213]

Smartcards

- Mit diesem Fix können Sie unter Verwendung der Funktion **SCardGetStatusChange** verfolgen, wie oft eine Smartcard in einem Lesegerät eingesteckt oder entfernt wurde. [CVADHELP-15463]

Systemausnahmen

- 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]
- Der Prozess PicaShell.exe wird möglicherweise unerwartet beendet, wenn eine Heap-Beschädigung in der DLL des virtuellen Kanals für die Zwischenablage vorliegt. [CVADHELP-14945]

- Das für die Browser-Inhaltsumleitung erforderliche Browser-Add-On für Internet Explorer (Citrix HDXJsInjector) kann beim Verwenden der Entwicklertools einen Webseitenfehler verursachen. Bei InjectorScript.js tritt gelegentlich eine Laufzeitausnahme auf, wenn in einem HTML-Dokument auf das head-Element (document.head) zugegriffen wird. Die folgende Fehlermeldung wird angezeigt:

  Error: Unable to get property 'appendChild'of undefined or null reference

  [CVADHELP-14960]

- 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]

Benutzererfahrung

- Wenn bestimmte Drittanbieteranwendungen in einer Benutzersitzung ausgeführt werden, wird der Mauszeiger möglicherweise zu einem drehenden Kreis. Das Problem tritt auf, wenn Sie ein Objekt in der Sitzung ziehen oder einen Zoomvorgang durchführen. [CVADHELP-14247]

VDA für Multisitzungs-OS

Tastatur

- Wenn Sie die **Windows-Taste + P** drücken, um die Projekt-Randleiste anzuzeigen, zeigen alle verbundenen Bildschirme möglicherweise einen schwarzen Hintergrund an, bis Sie die Esc-Taste drücken. Das Problem tritt auf, wenn **Transparentes Schlüsselpassthrough** in einer Seamlesssitzung aktiviert ist. [CVADHELP-14949]

Sitzung/Verbindung

- Wenn mehrere USB-Geräte an eine Sitzung umgeleitet werden, funktioniert eines von ihnen möglicherweise nicht ordnungsgemäß. [CVADHELP-12516]
- 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.

  Zum Implementieren dieses Fixes legen Sie folgenden Registrierungsschlüssel fest:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics

  Name: CursorShapeChangeMinInterval

Typ: DWORD

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

[CVADHELP-12886]

- Nach dem Neustart eines VDAs funktioniert die USB-Umleitung mit Hardwareverschlüsselung möglicherweise nicht. [CVADHELP-13336]
- 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]
- Wenn Sie die HDX RealTime-Webcamvideokomprimierung verwenden, zeigt eine Webcam möglicherweise statt eines Live-Bildes einen schwarzen Bildschirm an. [CVADHELP-13877]
- 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]
- 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]
- Der Citrix Softwaregrafikprozess (Ctxgfx.exe) verbraucht möglicherweise kontinuierlich Speicher in einer Sitzung. [CVADHELP-14509]
- Wenn Sie versuchen, eine Datei (z. B. CRX-, EXE- oder ZIP-Datei) über die Citrix Workspace-App für HTML5 hochzuladen, kann die Sitzungszuverlässigkeit dazu führen, dass die Sitzung getrennt wird. [CVADHELP-14513]
- 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]
- In Microsoft Windows wird winlogon.exe möglicherweise unerwartet beendet. Das Problem tritt auf, wenn Sie eine Seamlesssitzung schließen, die über einen Server gestartet wurde. Das Problem tritt aufgrund eines Fehlers im Modul icagfxstack.dll auf. [CVADHELP-14579]
- 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]
- Einige 32-Bit-Scananwendungen von Drittanbietern funktionieren möglicherweise nicht auf einem VDA, wenn sie mithilfe der generischen USB-Umleitung an den VDA umgeleitet werden.

Das Problem tritt auf, wenn die Scananwendungen auf dem VDA den TWAIN DSM verwenden. Das Problem kann auch auf einem VDA mit Remote-PC-Zugriff auftreten. [CVADHELP-14698]

- Dieser Fix behebt ein Sicherheitsrisiko in einer Hintergrundkomponente. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX285059. [CVADHELP-14755]
- 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 Optimierung für Microsoft Teams funktioniert möglicherweise nicht in Microsoft Teams. Das Problem tritt auf, wenn Citrix HDX nicht verbunden ist. [CVADHELP-14967]
- Dieser Fix bietet einen Timer zum Senden eines kleinen Datagramms über eine UDP-Verbindung, um die Verbindung zwischen Host und Client aufrechtzuerhalten.

  Um den Fix zu aktivieren, erstellen Sie die Registrierungseinstellung wie folgt:

  - *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]
- Wenn Sie versuchen, sich erneut mit einer neuen virtuellen Maschine zu verbinden, wird möglicherweise die folgende Microsoft .NET Framework-Fehlermeldung angezeigt:

  Error Unhandled exception has occurred in your application

[CVADHELP-15267]

- Die neuesten virtuellen Kanäle werden möglicherweise nicht zur internen hartcodierten Positivliste hinzugefügt. Wenn Sie die Positivliste aktivieren, funktionieren solche neuen virtuellen Kanäle nicht mehr, es sei denn, sie werden der benutzerdefinierten Positivliste hinzugefügt. [CVADHELP-15296]
- Wenn Sie versuchen, über die Taskleistenvorschau zu einem Fenster zu wechseln, kann das Öffnen dieses Fensters lange dauern. [CVADHELP-15422]
- 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]
- Mit diesem Fix ist der WTS-Hook standardmäßig aktiviert, wenn Sie das Flag auf 0x80000000 setzen. [CVADHELP-15929]

Smartcards

- Mit diesem Fix können Sie unter Verwendung der Funktion **SCardGetStatusChange** verfolgen, wie oft eine Smartcard in einem Lesegerät eingesteckt oder entfernt wurde. [CVADHELP-15463]

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]

- 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]
- Der wfshell.exe-Prozess kann unerwartet beendet werden. [CVADHELP-14414]
- Auf einem Gerät mit mehr als neun Bildschirmen kann der Start einer Benutzersitzung mit einer schwerwiegenden Ausnahme, Bluescreen und Bugcheckcode 0x3B fehlschlagen. [CVADHELP-14775]
- 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]
- Der Prozess PicaShell.exe wird möglicherweise unerwartet beendet, wenn eine Heap-Beschädigung in der DLL des virtuellen Kanals für die Zwischenablage vorliegt. [CVADHELP-14945]
- Das für die Browser-Inhaltsumleitung erforderliche Browser-Add-On für Internet Explorer (Citrix HDXJsInjector) kann beim Verwenden der Entwicklertools einen Webseitenfehler verursachen. Bei InjectorScript.js tritt gelegentlich eine Laufzeitausnahme auf, wenn in einem HTML-Dokument auf das head-Element (document.head) zugegriffen wird. Die folgende Fehlermeldung wird angezeigt:

  Error: Unable to get property 'appendChild'of undefined or null reference

  [CVADHELP-14960]
- 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]
- 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 mithilfe einer Verknüpfung starten, die sich außerhalb des Anwendungspakets befindet, kann das Argument **appve** der Befehlszeile hinzugefügt werden. Dieses **appve**-Argument ist nicht erforderlich. [CVADHELP-14369]
- Das Starten einer App-V-Anwendung über eine Verknüpfung im Ordner **AppData** schlägt möglicherweise fehl. [CVADHELP-14691]

- Dieser Fix behebt ein Sicherheitsrisiko in einer Hintergrundkomponente. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX285059. [CVADHELP-14989]
- Wenn Sie App-V-Anwendungen unter Verwendung der Einzelverwaltung in Citrix Studio erstellen, erfolgt die Anwendungsaufzählung möglicherweise langsam. Das Problem tritt auf, wenn App-V-Pakete doppelte Anwendungen enthalten. [CVADHELP-15427]
- Dieser Fix behebt ein Sicherheitsrisiko in einer Hintergrundkomponente. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX285059. [CVADHELP-15612]

Cumulative Update 1 (CU1)

March 15, 2022

Releasedatum: 7. Mai 2020

Info zu diesem Release

Citrix Virtual Apps and Desktops 7 1912 LTSR Kumulatives Update 1 (CU1) behebt mehr als 70 Probleme, die seit dem Erstrelease von LTSR 1912 gemeldet wurden.

1912 LTSR (Allgemeine Informationen)

1912 LTSR (Informationen zu Features und Upgrades)

Behobene Probleme seit Citrix Virtual Apps and Desktops 7 1912 LTSR (Erstrelease)

Bekannte Probleme in diesem Release

Veraltete und entfernte Produkte und Features

Berechtigungsdaten des Citrix-Produkts für Subscription Advantage

Downloads

Citrix Virtual Apps and Desktops 7 1912 LTSR CU1

> **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.

Neue Bereitstellungen

Wie stelle ich das CU1 von Grund auf bereit?

Mit dem CU1-Metainstaller können Sie eine neue Citrix Virtual Apps and Desktops-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 Citrix Virtual Apps and Desktops 7 1912 LTSR (Erstrealease) mit besonderem Augenmerk auf 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 15 Basiskomponenten von 1912 LTSR. Nicht vergessen: Citrix empfiehlt, alle LTSR-Komponenten in Ihrer Bereitstellung auf CU1 zu aktualisieren. Beispiel: Wenn Citrix Provisioning zur LTSR-Bereitstellung gehört, aktualisieren Sie die Citrix Provisioning-Komponenten auf die CU1-Version. Wenn Citrix Provisioning nicht zu Ihrer Bereitstellung gehört, brauchen Sie es nicht zu installieren oder zu aktualisieren.

Basiskomponenten von Citrix Virtual Apps and Desktops 7 1912 LTSR CU1

1912 LTSR-Basiskomponente	Version wie unter “Programme und Funktionen”angezeigt	Hinweise
Einzelsitzungs-VDA	1912.0.1000	
Multisitzungs-VDA	1912.0.1000	

1912 LTSR-Basiskomponente	Version wie unter “Programme und Funktionen”angezeigt	Hinweise
Delivery Controller	1912.0.1000	
Citrix Studio	1912.0.1000	
Citrix Director	1912.0.1000	
Citrix Gruppenrichtlinienverwaltung	7.24.1000	
Citrix Gruppenrichtlinie - clientseitige Erweiterung	7.24.1000	
Citrix StoreFront	1912.0.1000	
Citrix Provisioning	1912.0.1	
Universeller Druckserver	1912.0.1000	
Sitzungsaufzeichnung	1912.0.1000	
Linux VDA	1912.0.1000	Informationen zu den unterstützten Plattformen finden Sie in der Linux VDA-Dokumentation.
Profilverwaltung	1912.0.1000	
Citrix Verbundauthen-tifizierungsdienst	1912.0.1000	
Umleitung des Browserinhalts	15.19.1000	

Kompatible Komponenten für Citrix Virtual Apps and Desktops 7 1912 LTSR CU1

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 1912 LTSR-Umgebung durchzuführen.

Kompatible Komponenten und Features	Version wie unter “Programme und Funktionen”angezeigt
App Layering	19.11.0
App-Schutzrichtlinien	1912.0.0

Kompatible Komponenten und Features	Version wie unter “Programme und Funktionen”angezeigt
HDX RealTime Optimization Pack	2.9 LTSR
Lizenzserver	11.16.3.0 Build 30000
Benutzerpersonalisierungslayer	19.11.0
Webplayer für die Sitzungsaufzeichnung	1912.0.0
Teams-Optimierung	1912.0.0
Self-Service-Kennwortzurücksetzung	1.1
Windows 10 32-Bit	
Workspace Environment Management	2003.0.0 und höher
XenApp und XenDesktop 7.15 LTSR VDA (aktuelles Release)*	Nur aktuelles kumulatives Update

> **Hinweis:**
>
> Windows 10 32-Bit wird nur für 18 Monate ab der ersten Veröffentlichung von 1912 LTSR unterstützt. Windows 10 32-Bit wird nur unter Windows 10 Enterprise 2019 LTSC unterstützt.
>
> * Die XenApp und XenDesktop 7.15 LTSR VDA-Unterstützung gilt in diesem Fall nur für Windows 7 und Windows 2008 R2. Die Unterstützung für XenApp und XenDesktop 7.15 für LTSR endet am August 2022. Die Citrix Unterstützung für Windows 7 und Windows 2008 R2 endet, wenn Microsoft die Unterstützung für das Betriebssystem einstellt oder wenn die Unterstützung für XenApp und XenDesktop 7.15 LTSR endet, je nachdem, was zuerst eintritt. Weitere Informationen finden Sie in der Citrix Produktmatrix.

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.

Ausgeschlossene Elemente für Citrix Virtual Apps and Desktops 7 1912 LTSR CU1

Für die folgenden Features, Komponenten und Plattformen können die 1912-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 Komponenten und Features
AppDisks
AppDNA
Citrix SCOM Management Pack
Framehawk
Personal vDisk
StoreFront/Citrix Online-Integration

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.

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 1912 LTSR. 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 1912-LTSR-Kernkomponenten und dem Erstellen einer Site wird der Migrationsprozess in der folgenden Reihenfolge ausgeführt:

- Führen Sie das 1912-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 1912-LTSR-Site importieren.
- Führen Sie PowerShell-Import-Cmdlets auf dem neuen 1912-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

March 15, 2022

Die folgenden Probleme wurden seit Citrix Virtual Apps and Desktops 7 1912 LTSR (Erstrelease) behoben:

Citrix Director

- Wenn ein Delivery Controller ausgeschaltet ist, zeigt Citrix Director den Status des Delivery Controller falsch an. Auf der Registerkarte *Infrastruktur* in Citrix Director werden daraufhin falsche Warnungen angezeigt. [CVADHELP-13835]

Citrix Richtlinie

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

Citrix Provisioning

Die Dokumentation zu Citrix Provisioning 1912 CU1 enthält Informationen zu den Updates in diesem Release.

Citrix Studio

- 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]

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]
- 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]
- Mit diesem Fix unterstützen die Maschinenerstellungsdienste (MCS) die folgenden neuen Citrix Hypervisor-Features: Start von Gast-Betriebssystemen im UEFI-Modus und Secure Boot [CVADHELP-14210]
- In Citrix Hypervisor kann das Hinzufügen von Maschinen zu einem vorhandenen Katalog der Maschinenerstellungsdienste (MCS) fehlschlagen. [CVADHELP-14212]

Verbundauthentifizierungsdienst

- In den Eigenschaften der Zertifikatsvorlage Citrix_SmartcardLogon sollte die Beschreibung der Erweiterung “Key Usage”nur “Digital signature”und “Key encipherment”enthalten, enthält aber zusätzliche Elemente. Die mit dieser Vorlage ausgestellten Zertifikate sind jedoch korrekt. [CVADHELP-14040]

Linux Virtual Delivery Agent

Die Dokumentation zu Linux Virtual Delivery Agent 1912 CU1 enthält spezifische Informationen zu den Updates in diesem Release.

Metainstaller

- Beim Start eines Desktops wird möglicherweise ein grauer Bildschirm angezeigt. Das Problem tritt nach dem Update eines VDAs von Version 7.6 LTSR Kumulatives Update auf Version 1912 auf. [CVADHELP-13969]

Profilverwaltung

Die Dokumentation zur Profilverwaltung 1912 CU1 enthält Informationen zu den Updates in diesem Release.

Sitzungsaufzeichnung

Die Dokumentation zur Sitzungsaufzeichnung 1912 CU1 enthält Informationen zu den Updates in diesem Release.

StoreFront

Die Dokumentation zu StoreFront 1912 CU1 enthält Informationen zu den Updates in diesem Release.

Universeller Druckserver

Client

- 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]

VDA für Einzelsitzungs-OS

Installieren, Deinstallieren und Aktualisieren

- Beim Upgrade eines VDAs wird der Registrierungsschlüssel `MaxVideoMemoryBytes` möglicherweise auf den Standardwert zurückgesetzt. [CVADHELP-13629]

Drucken

- Beim Start einer Anwendung wird der Citrix Druckmanagerdienst (CpSvc.exe) möglicherweise unerwartet beendet. [CVADHELP-13945]
- Automatisch erstellte PDF-Drucker werden möglicherweise nicht gelöscht. Das Problem tritt auf, wenn Drucker nicht unter HKEY_CURRENT_CONFIG, sondern unter HKEY_LOCAL_MACHINE\SOFTWARE erstellt werden. [CVADHELP-14280]

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]
- 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]
- Das Lesen von Daten von einem Clientlaufwerk kann länger dauern, nachdem Sie auf einem VDA den Wert für folgenden Registrierungsschlüssel in 1 ändern:

  Zum Implementieren dieses Fixes erstellen Sie folgenden Registrierungsschlüssel:

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

  Name: PacketIntegrityChecks

  Typ: DWORD

  Wert: 1

  [CVADHELP-13063]
- Das Starten einer Sitzung auf einem VDA kann fehlschlagen, wenn Sie den Schwachstellenscanner einiger Drittanbieter verwenden. [CVADHELP-13306]

- Das Wiederverbinden mit einer Sitzung kann fehlschlagen und die folgende Fehlermeldung wird angezeigt:

  Fehler beim Desktopstart.

  [CVADHELP-13320]

- Wenn Sie versuchen, die Fenstergröße eines veröffentlichten Desktops zu ändern, wird die Hardwarecodierung möglicherweise deaktiviert. [CVADHELP-13818]
- 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]
- Ist die Richtlinie **Automatische Anzeige der Tastatur** aktiviert und Sie klicken in das **Google-Suchfeld**, wird möglicherweise die Tastatur nicht automatisch angezeigt. Das Problem tritt bei Sitzungen im Internet Explorer-, Firefox- oder Chrome-Browser auf. [CVADHELP-14065]
- Wenn Sie im Startmenü mit der rechten Maustaste auf das Benutzersymbol klicken, werden im Kontextmenü nicht die Optionen **Herunterfahren** oder **Abmelden** angezeigt. Stattdessen werden im Kontextmenü die Optionen angezeigt, die erscheinen, wenn Sie mit der rechten Maustaste auf eine Kachel klicken. [CVADHELP-14149]
- Wenn Sie für die Zeitzonenrichtlinie die Einstellung **Lokale Zeit des Clients verwenden** wählen, wird die Zeitzone möglicherweise falsch umgeleitet, wenn Sie eine Sitzung über die Citrix Workspace-App für HTML5 starten. Beispielsweise wird die Uhrzeit auf **UTC+ 01:00** statt auf **UTC+ 00:00**festgelegt. Die Einstellung **Uhr automatisch auf Sommer-/Winterzeit umstellen** wird daraufhin deaktiviert. [CVADHELP-14471]
- In einem Double-Hop-Szenario kann es vorkommen, dass ein einzelner Benutzer zwei Citrix-Lizenzen (CCU-Lizenzen) verbraucht. Beim Double-Hop-Szenario starten Benutzer die HDX-Sitzung innerhalb einer anderen HDX-Sitzung (z. B. beim Start einer veröffentlichten Anwendung in einer virtuellen Desktopsitzung). [CVADHELP-14409]
- Beim Versuch, kleine Objekte auf dem Bildschirm zu verschieben, kann ein einzelnes Pixel beschädigt werden. Das Problem tritt auf, wenn die Richtlinie **Bildqualität** auf **Zu verlustfrei verbessern** festgelegt ist. [CVADFIX-8214]

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]

- Wenn Sie sich mit einer schnellen Smartcard an einer Sitzung anmelden, wird die PIN-Eingabeaufforderung u. U. zweimal angezeigt. [CVADHELP-12949]

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 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]
- Auf VDAs kann es in picadm.sys zu einer schwerwiegenden Ausnahme mit Bluescreen und Bugcheckcode 0x22 kommen. [CVADHELP-14431]

Benutzererfahrung

- Bei Desktopsitzungen werden möglicherweise Artefakte angezeigt, die den Bildschirminhalt und andere Teile der Anzeige verdecken. [CVADHELP-13301]

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 Multisitzungs-OS

Inhaltsumleitung

- Wen Sie die Richtlinie zur Browserinhaltsumleitung im Modus **Serverseitiger Abruf und clientseitige Wiedergabe** konfigurieren, leiten Sie den Datenverkehr nur über einen statisch konfigurierten Webproxy. [CVADHELP-14134]

Drucken

- 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]
- Automatisch erstellte PDF-Drucker werden möglicherweise nicht gelöscht. Das Problem tritt auf, wenn Drucker nicht unter HKEY_CURRENT_CONFIG, sondern unter HKEY_LOCAL_MACHINE\SOFTWARE erstellt werden. [CVADHELP-14280]

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 Multisitzungs-VDA starten, wird der Registrierungsschlüssel "Windows RunOnce"möglicherweise nicht ausgeführt. [CVADHELP-11991]
- 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]
- Das Lesen von Daten von einem Clientlaufwerk kann länger dauern, nachdem Sie auf einem VDA den Wert für folgenden Registrierungsschlüssel in 1 ändern:

  Zum Implementieren dieses Fixes erstellen Sie folgenden Registrierungsschlüssel:

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

  Name: PacketIntegrityChecks

  Typ: DWORD

  Wert: 1

  [CVADHELP-13063]
- Das Wiederverbinden mit einer Sitzung kann fehlschlagen und die folgende Fehlermeldung wird angezeigt:

Fehler beim Desktopstart.

[CVADHELP-13320]

- Beim Versuch, sich erneut mit einer Sitzung zu verbinden, wird der Desktop möglicherweise nicht geladen und es wird ein graues Fenster angezeigt. Das Problem tritt auf, wenn VDA Version 1909 unter Microsoft Windows Server 2019 ausgeführt wird. [CVADHELP-13376]
- 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]
- Eine Benutzersitzung wird möglicherweise unerwartet geschlossen. Das Problem tritt auf, wenn nicht authentifizierte (anonyme) Benutzer eine zweite Anwendung im Fenstermodus starten. [CVADHELP-13917]
- Nach dem Upgrade eines VDA auf Version 1909.1 kann es bei einigen Drittanbieter-Apps (z. B. `RemoteScan`) beim Scannen eines Dokuments dazu kommen, dass die Apps nicht mehr reagieren. Grund für dieses Problem ist das fehlerhafte Modul twnhook.dll. [CVADHELP-13937]
- Die virtuelle Tastatur wird in einer veröffentlichten Anwendung u. U. nicht automatisch angezeigt. [CVADHELP-14012]
- Beim Versuch, Version 1912 des VDA über die Befehlszeile neu zu konfigurieren, um einen benutzerdefinierten VDA-Port zu verwenden, kann folgende Fehlermeldung angezeigt werden:

  The process could not be completed …Cannot find Ica Configuration file …IcaConfigConsole.exe.

  [CVADHELP-14052]
- Ist die Richtlinie **Automatische Anzeige der Tastatur** aktiviert und Sie klicken in das **Google-Suchfeld**, wird möglicherweise die Tastatur nicht automatisch angezeigt. Das Problem tritt bei Sitzungen im Internet Explorer-, Firefox- oder Chrome-Browser auf. [CVADHELP-14065]
- Dieser Fix enthält eine neue Richtlinieneinstellung, die festlegt, dass virtuelle Kanäle, die Multistream-ICA verwenden, über eine Citrix-Richtlinie und nicht über einen Registrierungsschlüssel konfiguriert werden. [CVADHELP-14136]
- 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. [CVADHELP-14301]
- In einem Double-Hop-Szenario kann es vorkommen, dass ein einzelner Benutzer zwei Citrix-Lizenzen (CCU-Lizenzen) verbraucht. Beim Double-Hop-Szenario starten Benutzer die HDX-Sitzung innerhalb einer anderen HDX-Sitzung (z. B. beim Start einer veröffentlichten Anwendung in einer virtuellen Desktopsitzung). [CVADHELP-14409]

- Beim Versuch, kleine Objekte auf dem Bildschirm zu verschieben, kann ein einzelnes Pixel beschädigt werden. Das Problem tritt auf, wenn die Richtlinie **Bildqualität** auf **Zu verlustfrei verbessern** festgelegt ist. [CVADFIX-8214]

Smartcards

- Wenn Sie sich mit einer schnellen Smartcard an einer Sitzung anmelden, wird die PIN-Eingabeaufforderung u. U. zweimal angezeigt. [CVADHELP-12949]

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 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]
- Auf VDAs kann es in picadm.sys zu einer schwerwiegenden Ausnahme mit Bluescreen und Bugcheckcode 0x22 kommen. [CVADHELP-14431]

Benutzererfahrung

- Bei Desktopsitzungen werden möglicherweise Artefakte angezeigt, die den Bildschirminhalt und andere Teile der Anzeige verdecken. [CVADHELP-13301]

Benutzeroberfläche

- Wenn Sie ein Seamlessfenster verschieben, werden Grafikinhalte für eine Anwendung möglicherweise verzerrt. Das Problem tritt auf, wenn Sie einige Teile des Fensters an eine Position außerhalb des Desktopbereichs verschieben. [CVADHELP-14209]

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]
- Wenn Sie eine Datei mit der zugeordneten veröffentlichten App-V-Anwendung öffnen, wird die Anwendung geöffnet. Die Datei kann jedoch nicht in der zugeordneten Anwendung geöffnet werden. [CVADHELP-13971]

1912 LTSR (Erstrelease)

June 27, 2024

Info zu diesem Release

Das Long Term Service Release (LTSR)-Programm für Citrix Virtual Apps and Desktops bietet Stabilität und langfristige Unterstützung für Citrix Virtual Apps and Desktops-Releases.

LTSRs sind derzeit für Citrix Virtual Apps and Desktops 7 1912 (dieses Release) und für die XenApp und XenDesktop-Versionen 7.6 und 7.15 verfügbar. Wenn Sie das LTSR-Programm erstmals nutzen, können Sie Citrix Virtual Apps and Desktops 7 1912 von Grund auf neu installieren. Wenn Sie eines der früheren LTSRs verwenden, können Sie dieses aktualisieren (einschließlich alle kumulativen Updates). Informationen zu unterstützten Upgradepfaden finden Sie im Upgradehandbuch.

Citrix empfiehlt außerdem bestimmte Versionen der Citrix Workspace-App und anderer Komponenten. Obwohl es nicht für LTSR erforderlich ist, wird durch ein Upgrade auf die empfohlenen Versionen dieser Komponenten sichergestellt, dass Ihre Bereitstellung wartungsfreundlich ist und die aktuellen Fixes vorhanden sind.

Eine Übersicht über die in Citrix Virtual Apps and Desktops 7 1912 neu eingeführten Features finden Sie in der Tabelle Citrix Virtual Apps and Desktops –Vergleich der Features.

Dieses Release von Citrix Virtual Apps and Desktops enthält neue Versionen der Virtual Delivery Agents (VDAs) für Windows und einiger Kernkomponenten von Citrix Virtual Apps and Desktops. Sie haben folgende Möglichkeiten:

- **Site installieren oder aktualisieren**

  Installieren oder aktualisieren Sie Kernkomponenten und 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 bereits eine 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.

  Nach dem Upgrade der VDAs von Version 7.9 oder höher auf die aktuelle Version 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.

Anweisungen:

- Wenn Sie eine neue Site erstellen, folgen Sie den Anweisungen unter Installation und Konfiguration.
- Wenn Sie eine Site aktualisieren, lesen Sie Upgrade einer Bereitstellung.

Citrix Virtual Apps and Desktops 7 1912 LTSR

Wichtiger Hinweis zum Upgrade von VDAs

Wurde die PvD-Komponente (persönliche vDisk) jemals auf einem VDA installiert, kann dieser nicht auf Version 1912 LTSR oder höher aktualisiert werden. Um den neuen VDA zu verwenden, müssen Sie den bestehenden VDA deinstallieren und dann den neuen VDA installieren.

Dies ist auch dann erforderlich, wenn Sie PvD zwar installiert, aber nie verwendet haben.

Herausfinden, ob Sie das betrifft Wie PvD eventuell in früheren Versionen installiert wurde:

- Auf der grafischen Benutzeroberfläche des VDA-Installationsprogramms war PvD eine Option (Kontrollkästchen auf der Seite **Zusätzliche Komponenten**). In den 7.x-Versionen bis 7.15 LTSR war diese Option standardmäßig aktiviert. Wenn Sie die Standardeinstellungen akzeptiert haben (oder die Option in einem Release explizit aktiviert haben), wurde PvD installiert.
- In der Befehlszeile wurde PvD über die Option `/baseimage` installiert. Wenn Sie diese Option angegeben oder ein Skript verwendet haben, das diese Option enthielt, wurde PvD installiert.

Wenn Sie nicht wissen, ob auf Ihrem VDA PvD installiert ist, führen Sie das Installationsprogramm für den neuen VDA (1912 LTSR oder höher) auf der Maschine bzw. dem Image aus.

- Wenn PvD installiert ist, weist eine Meldung darauf hin, dass eine inkompatible Komponente vorhanden ist.

  - Klicken Sie auf der grafischen Benutzeroberfläche auf der Seite mit der Meldung auf **Abbrechen** und bestätigen Sie, dass Sie das Installationsprogramm schließen möchten.
  - Wenn Sie die Befehlszeile verwenden, schlägt der Befehl unter Anzeige der Meldung fehl.
- Wenn PvD nicht installiert ist, wird das Upgrade fortgesetzt.

Aktion Wenn PvD auf dem VDA nicht installiert ist, folgen Sie dem normalen Upgradeverfahren.

Wenn PvD auf dem VDA installiert ist, gehen Sie folgendermaßen vor:

1. Deinstallieren Sie den VDA. Einzelheiten finden Sie unter Entfernen von Komponenten.
2. Installieren Sie den neuen VDA.

Wenn Sie PvD auf Windows 7- oder Windows 10-Maschinen (bis 1607 ohne Updates) weiterverwenden möchten, ist VDA 7.15 LTSR die neueste unterstützte Version.

Installation und Upgrade: Neue Benutzerpersonalisierunglayer-Komponente in VDAs für Einzelsitzungs-OS

Beim Installieren oder Upgrade eines VDAs für Einzelsitzungs-OS können Sie die Benutzerpersonalisierungslayer-Komponente einschließen. Das Feature basiert auf Citrix App Layering. Auf nicht persistenten Maschinen speichert das Feature Benutzerdaten und lokal installierte Anwendungen für Sitzungen.

Das Feature ersetzt das veraltete PvD-Feature (persönliche vDisk). Bei einem Upgrade von VDAs, auf denen zuvor PvD installiert war, konsultieren Sie die Informationen unter Wichtiger Hinweis zum Upgrade von VDAs.

Weitere Informationen zu dem neuen Feature finden Sie in der Dokumentation zum Benutzerpersonalisierungslayer. Anweisungen zur VDA-Installation finden Sie unter Installieren von VDAs.

Installation und Upgrade: Voraussetzung für Microsoft Visual C++ Runtime 2017

Bei der Installation eines Delivery Controllers oder Windows-VDA wird Microsoft Visual C++ Runtime 2017 automatisch installiert, falls es (oder eine höhere unterstützte Version) noch nicht vorhanden ist. Es handelt sich um eine neuere Version von Visual C++ Runtime, als bei früheren Versionen von Citrix Virtual Apps and Desktops installiert wurde.

Installation und Upgrade: SQL Server Express-Version

Bei der Installation des ersten Delivery Controllers können Sie festlegen, dass Microsoft SQL Server Express von Citrix auf derselben Maschine zur Verwendung als Sitedatenbank installiert wird. Ab diesem Release wird für neue Installationen SQL Server Express 2017 mit kumulativem Update 16 installiert.

Es handelt sich um eine neuere Version als bei früheren Versionen von Citrix Virtual Apps and Desktops. Bei Upgrades wird die vorhandene SQL Server Express-Version nicht aktualisiert.

Wenn Sie einen Controller installieren, wird automatisch SQL Server Express LocalDB zur Verwendung mit dem lokalen Hostcache installiert. (Diese Installation erfolgt separat von SQL Server Express, das für die Sitedatenbank verwendet wird.) Bei neuen Installationen wird SQL Server Express LocalDB 2017 mit kumulativem Update 16 installiert. Es handelt sich um eine neuere Version als bei früheren Versionen von Citrix Virtual Apps and Desktops. Bei Upgrades wird eine vorhandene SQL Server Express LocalDB-Version nicht aktualisiert.

Installation und Upgrade: Unterstützte Windows 10-Versionen für VDAs

Dieses Release unterstützt die Betriebssysteme Windows 10 32 Bit (x86) und 64 Bit (x64). Windows 10 32-Bit wird nur für 18 Monate ab der ersten Veröffentlichung von 1912 LTSR unterstützt. Windows 10 32-Bit wird nur unter Windows 10 Enterprise 2019 LTSC unterstützt. Citrix empfiehlt die Verwendung der 64-Bit-Version (x64) von Windows 10.

Installation und Upgrade: Prüfung auf ausstehende Neustarts verhindern

Beim Installieren oder Upgrade von Kernkomponenten hält das Installationsprogramm an, wenn ein ausstehender Neustart aus einer vorherigen Windows-Installation auf einer Maschine erkannt wird. Wenn Sie die Befehlszeilenschnittstelle verwenden, können Sie nun die Prüfung auf einen ausstehenden Neustart mit der Option `/no_pending_reboot_check` verhindern. Weitere Informationen finden Sie unter Bei der Installation aller Komponenten.

VDAs und Maschinenkataloge: Änderungen des Betriebssystemnamens

Die Betriebssystemnamen für VDAs und Maschinenkataloge wurden geändert.

- **Multisitzungs-OS** (früher "Serverbetriebssysteme"): Der Maschinenkatalog für Multisitzungs-OS stellt gehostete, freigegebene Desktops für großvolumige Bereitstellungen von standardisierten Windows-Betriebssystemen für mehrere Sitzungen oder Linux-OS-Maschinen bereit.
- **Einzelsitzungs-OS** (früher "Desktopbetriebssysteme"): Der Maschinenkatalog für Einzelsitzungs-OS bietet VDI-Desktops, die sich ideal für diverse Benutzer eignen.

Versionsnummer von Komponenten: Änderung bei On-Premises-Wert

Bei Versionsnummern für Produkte und Komponenten (*JJMM.c.m.b*) steht an Position *c* bei On-Premises-Versionen **0**. Unter **Apps & Features** wird die Version beispielsweise als 1912.0.0*Buildnummer* angezeigt.

Bei früheren On-Premises-Versionen und in Citrix Cloud-Releases stand an Position *c* der Wert **1.**

Weitere Informationen finden Sie unter Versionsnummern für Produkte und Komponenten.

Citrix Studio

Unterstützung für das Provisioning von Linux-Maschinen auf Amazon Web Services

Citrix Studio unterstützt jetzt die Verwendung von Maschinenerstellungsdiensten (MCS) für das Provisioning von Linux-Maschinen auf Amazon Web Services (AWS). Weitere Informationen finden Sie unter Verwenden von MCS zum Erstellen von Linux-VMs.

Virtual Delivery Agents (VDAs) 1912

Version 1912 des VDAs für Multisitzungs-OS und des VDAs für Einzelsitzungs-OS bietet neben den oben genannten Änderungen an Installation und Upgrade folgende Verbesserungen:

> **Hinweis:**
>
> Die VDA-Versionsnummer gibt zwar "Citrix Virtual Apps and Desktops 7 1912 LTSR"an, die VDAs werden jedoch für LTSR- und CR-Bereitstellungen unterstützt.

Unterstützung für Schutz durch lokale Sicherheitsautorität

Citrix unterstützt jetzt den LSA-Schutz (Local Security Authority) unter Multisitzungs-OS und Einzelsitzungs-OS für die Standardauthentifizierung, die FAS-Authentifizierung (Federated Authentication Service) und die Smartcard-Authentifizierung. Weitere Informationen zum LSA-Schutz finden Sie im Microsoft-Artikel Konfigurieren von zusätzlichem LSA-Schutz.

App-Schutz

Ab diesem Release gibt es ein Add-On-Feature, das bei der Verwendung der Citrix Workspace-App mehr Sicherheit bietet. Neue Richtlinien bieten Keylogging- und Screenshotschutzfunktionen für Sitzungen. Zusammen mit der Citrix Workspace-App 1912 oder höher für Windows können die neuen Richtlinien zum Schutz von Daten vor Keylogging und Screen Scraping beitragen. Weitere Informationen finden Sie unter App-Schutz.

Citrix Lizenzierung 11.16.3.0 Build 29000

Version 11.16.3.0 Build 29000 der Citrix Lizenzierung enthält neue Features sowie behobene und bekannte Probleme.

Citrix Verbundauthentifizierungsdienst 1912

Citrix Verbundauthentifizierungsdienst 1912 enthält neue Features.

Weitere Informationen

- Lesen Sie den Artikel Einstellung von Features und Plattformen zu geänderten Ankündigungen.
- Informationen über seit 2018 geänderte Produktnamen und Versionsnummern finden Sie unter Neue Namen und Nummern.

Basiskomponenten

1912 LTSR-Basiskomponente	Version	Hinweise
Einzelsitzungs-VDA	1912.0	
Multisitzungs-VDA	1912.0	
Delivery Controller	1912.0.0	
Citrix Studio	7.24.0	
Citrix Director	7.24.0	
Gruppenrichtlinienverwaltung	7.24.0	
StoreFront	19.12.0.0	
Provisioning Services	1912	
Universeller Druckserver	7.24.0	
Sitzungsaufzeichnung	1912.0.0	
Linux VDA	1912.0.0	Informationen zu den unterstützten Plattformen finden Sie in der Linux VDA-Dokumentation.
Profilverwaltung	1912.0.0	
Verbundauthentifizierungsdienst	7.24.0	
Browserinhaltsumleitung	15.19.0	

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 1912 LTSR-Umgebung durchzuführen.

Kompatible Komponenten und Features	Version
App Layering	19.11.0
App-Schutzrichtlinien	1912.0.0
HDX RealTime Optimization Pack	2.8
Lizenzserver	11.16.3.0 Build 29000
Benutzerpersonalisierungslayer	19.11.0
Webplayer für die Sitzungsaufzeichnung	1912.0.0
Teams-Optimierung	1912.0.0
Self-Service-Kennwortzurücksetzung	1.1
Windows 10 32-Bit	
Workspace Environment Management	1912.0.0
XenApp und XenDesktop 7.15 LTSR VDA (aktuelles Release)*	Nur aktuelles kumulatives Update

> **Hinweis:**
>
> Windows 10 32-Bit wird nur für 18 Monate ab der ersten Veröffentlichung von 1912 LTSR unterstützt. Windows 10 32-Bit wird nur unter Windows 10 Enterprise 2019 LTSC unterstützt.
>
> * Die XenApp und XenDesktop 7.15 LTSR VDA-Unterstützung gilt in diesem Fall nur für Windows 7 und Windows 2008 R2. Die Unterstützung für XenApp und XenDesktop 7.15 für LTSR endet am August 2022. Die Citrix Unterstützung für Windows 7 und Windows 2008 R2 endet, wenn Microsoft die Unterstützung für das Betriebssystem einstellt oder wenn die Unterstützung für XenApp und XenDesktop 7.15 LTSR endet, je nachdem, was zuerst eintritt. Weitere Informationen finden Sie in der Citrix Produktmatrix.

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.

Ausnahmen

Für die folgenden Features, Komponenten und Plattformen können die 1912-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 Komponenten und Features
AppDisks
AppDNA
Citrix SCOM Management Pack
Framehawk
Personal vDisk
StoreFront/Citrix Online-Integration

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.

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 1912 LTSR. 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 1912-LTSR-Kernkomponenten und dem Erstellen einer Site wird der Migrationsprozess in der folgenden Reihenfolge ausgeführt:

- Führen Sie das 1912-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 1912-LTSR-Site importieren.
- Führen Sie PowerShell-Import-Cmdlets auf dem neuen 1912-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

April 19, 2024

Die folgenden Probleme wurden seit Version 7 1909 von Citrix Virtual Apps and Desktops behoben:

Citrix Studio

- Citrix Studio zeigt ggf. die Symbole für erkannte Anwendungen falsch an, wenn Sie Anwendungen aus dem Startmenü hinzufügen. Das Problem tritt bei integrierten Windows-Anwendungen unter Windows 10 1903 auf. Wählen Sie als Workaround die Anwendung aus, klicken Sie auf **Eigenschaften**, klicken Sie auf der Seite "Bereitstellung"auf **Ändern** und wählen Sie dann ein Symbol für die Anwendung aus. [BRK-4430]

Citrix Provisioning

Die Dokumentation zu Citrix Provisioning 1912 enthält Informationen zu den Updates in diesem Release.

Delivery Controller

- Das Anhalten des Citrix Broker-Diensts kann fehlschlagen. [CVADHELP-12715]
- In VMware vSAN 6.7-Umgebungen schlägt das Löschen einer mit den Maschinenerstellungsdiensten (MCS) erstellten VM möglicherweise fehl, weil das Basisdatenträgerimage entfernt wurde. Dieses Image wird von mehreren VMs gemeinsam genutzt. Das Problem tritt auf, wenn die VMDK-Datei das Flag `dbb.deletable=false` enthält. [CVADHELP-13127]
- Wenn Sie versuchen, einen Maschinenkatalog mit Maschinenerstellungsdienste in einer VMware Umgebung zu erstellen, schlägt die Katalogerstellung mit der folgenden Fehlermeldung fehl:

  FailedToCreateImagePreparationVm

  [CVADHELP-13143]
- 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"

  [CVADHELP-13146]

HDX RealTime Optimization Pack

Die Dokumentation zu HDX RealTime Optimization Pack 1912 enthält Informationen zu den Updates in dieser Version.

Lizenzierung

Die Dokumentation zur Lizenzierung 1912 enthält Informationen zu den Updates in diesem Release.

Linux VDA

Die Dokumentation zum Linux VDA 1912 enthält Informationen zu den Updates in diesem Release.

Profilverwaltung

Die Dokumentation zur Profilverwaltung 1912 enthält Informationen zu den Updates in diesem Release.

StoreFront

Die Dokumentation zu StoreFront 1912 enthält Informationen zu den Updates in diesem Release.

VDA für Einzelsitzungs-OS

Drucken

- 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. [CVADHELP-13357]
- Sind Nicht-Standard-Schriftarten (z. B. die Barcode-Schriftart CCode390) auf einem VDA der Version 7.18 oder höher installiert, kann ein Druckproblem auftreten, wenn Sie XenApp und XenDesktop von Version 7.17 auf 7.18 oder höher aktualisieren. Die Barcode-Schriftart wird möglicherweise nicht gedruckt, wenn Sie ein Dokument aus einer Sitzung drucken. [CVADHELP-12454]

Sitzung/Verbindung

- Bei der Audiowiedergabe in einer Benutzersitzung ist möglicherweise ein Knacken zu hören. [CVADHELP-11241]
- In Citrix Receiver für Windows wird die Audiowiedergabe möglicherweise ab und zu unterbrochen. [CVADHELP-11440]
- Auf einigen Benutzergeräten kann es lange dauern, bis eine zweite Anwendung gestartet wird, wenn Sie die Grafikkarten auf "Ein"einstellen. [CVADHELP-12387]
- Die optimierte Webcam der Media Foundation-basierten Videoanwendungen funktioniert möglicherweise nicht für einige APIs. [CVADHELP-12427]
- Wenn Sie visuelle Effekte in einer Benutzersitzung ändern, wird der Wert `UserPreferencesMask` des Registrierungsschlüssels HKEY_CURRENT_USER\Control Panel\Desktop möglicherweise nicht auf den neuen Wert aktualisiert.

  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

[CVADHELP-12796]

- Das Kopieren von Text aus einer veröffentlichten Anwendung auf einen Endpunkt kann bei Verwendung der Citrix Workspace-App 1902 für Windows oder höher fehlschlagen. [CVADHELP-12945]
- Eine Zugriffsverletzung kann dazu führen, dass der Prozess wfshell.exe unerwartet beendet wird. Anwendungen können dann nicht gestartet werden. [CVADHELP-13032]

Systemausnahmen

- Wenn Sie versuchen, Videoclips auf einem VDA für Desktopbetriebssysteme zu exportieren, werden bestimmte Anwendungen von Drittanbietern möglicherweise unerwartet beendet. [CVADHELP-11303]
- Bei Servern kann bei tdica.sys eine schwerwiegende Ausnahme mit Bluescreen und Bugcheckcode **SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (7e)** auftreten.

  [CVADHELP-12611]
- Der wfshell.exe-Prozess kann auf VDAs unerwartet beendet werden. [CVADHELP-12819]
- Das Starten von Anwendungen kann fehlschlagen, wenn der Prozess wfshell.exe unerwartet beendet wird. Das Problem tritt aufgrund des fehlerhaften Moduls cmpcom.dll auf. [CVADHELP-13089]

VDA für Multisitzungs-OS

Drucken

- Sind Nicht-Standard-Schriftarten (z. B. die Barcode-Schriftart CCode390) auf einem VDA der Version 7.18 oder höher installiert, kann ein Druckproblem auftreten, wenn Sie XenApp und XenDesktop von Version 7.17 auf 7.18 oder höher aktualisieren. Die Barcode-Schriftart wird möglicherweise nicht gedruckt, wenn Sie ein Dokument aus einer Sitzung drucken. [CVADHELP-12454]

Sitzung/Verbindung

- 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. [CVADHELP-10657]
- Auf einigen Benutzergeräten kann es lange dauern, bis eine zweite Anwendung gestartet wird, wenn Sie die Grafikkarten auf "Ein"einstellen. [CVADHELP-12387]
- Die optimierte Webcam der Media Foundation-basierten Videoanwendungen funktioniert möglicherweise nicht für einige APIs. [CVADHELP-12427]
- Wenn Sie visuelle Effekte in einer Benutzersitzung ändern, wird der Wert UserPreferencesMask des Registrierungsschlüssels HKEY_CURRENT_USER\Control Panel\Desktop möglicherweise nicht auf den neuen Wert aktualisiert.

  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

  [CVADHELP-12796]
- Das Kopieren von Text aus einer veröffentlichten Anwendung auf einen Endpunkt kann bei Verwendung der Citrix Workspace-App 1902 für Windows oder höher fehlschlagen. [CVADHELP-12945]
- Eine Zugriffsverletzung kann dazu führen, dass der Prozess wfshell.exe unerwartet beendet wird. Anwendungen können dann nicht gestartet werden. [CVADHELP-13032]

Systemausnahmen

- Microsoft Internet Explorer kann unerwartet beendet werden. Das Problem tritt aufgrund des fehlerhaften Moduls icaendpoint.dll auf. [CVADHELP-12171]
- Bei Servern kann bei tdica.sys eine schwerwiegende Ausnahme mit Bluescreen und Bugcheckcode **SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (7e)** auftreten. [CVADHELP-12611]
- Der wfshell.exe-Prozess kann auf VDAs unerwartet beendet werden. [CVADHELP-12819]
- Das Starten von Anwendungen kann fehlschlagen, wenn der Prozess wfshell.exe unerwartet beendet wird. Das Problem tritt aufgrund des fehlerhaften Moduls cmpcom.dll auf. [CVADHELP-13089]

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. [CVADHELP-10739]

Bekannte Probleme

May 24, 2024

Hinweise

- Bekannte Probleme, die in den Abschnitten zum Erstrelease von 1912 und für CU1, CU2, CU3, CU4, CU5, CU6, CU7 und CU8 in diesem Artikel beschrieben werden, sind auch in CU9 vorhanden, sofern sie nicht in der Liste der behobenen Probleme aufgeführt werden.
- Wenn es für ein bekanntes Problem einen Workaround gibt, wird dieser nach der Beschreibung des Problems angegeben.
- Der folgende Warnhinweis gilt für alle Workarounds, bei denen ein Registrierungseintrag geändert werden muss:

> **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. Erstellen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

Bekannte Probleme in 1912 CU9

- Sie können während einer VDA-Installation oder eines VDA-Upgrades keinen VDA unter Windows 2012 R2 mit der Citrix Workspace-App installieren.

  Problemumgehung: Schließen Sie die Citrix Workspace-App während einer VDA-Installation oder eines VDA-Upgrades aus. Lesen Sie die Systemanforderungen der Citrix Workspace-App, bevor Sie den VDA bereitstellen.
  [LCM-14080]

- Wenn Sie CVAD LTSR 1912 CU9 mit der Befehlszeileninstallationsmethode installieren und Befehle in die Befehlszeile eingeben, wird eine neue Zeile eingegeben und die automatische Installation initiiert. Nach Abschluss der Installation erhalten Sie jedoch keine Meldung, dass die Installation abgeschlossen ist. [LCM-14108]

Bekannte Probleme in 1912 CU8

- Wenn Sie Windows, IIS und Citrix Director in einem anderen Laufwerk als C:\ installieren und Citrix Director auf Version 1912 LTSR CU8 aktualisieren, wird das Citrix Director-Symbol möglicherweise leer angezeigt. Sie können jedoch auf das Symbol klicken, um Citrix Director zu starten.

  Verwenden Sie den folgenden Workaround, um das Symbol korrekt anzuzeigen.

1. Öffnen Sie die Eingabeaufforderung und führen Sie den Befehl echo **%systemdrive%** aus.
2. Kopieren Sie die Ausgabe des Befehls.
3. Klicken Sie mit der rechten Maustaste auf das Citrix Director-Symbol > Mehr > Dateispeicherort öffnen.
4. Öffnen Sie den Editor und ziehen Sie das Symbol aus dem Datei-Explorer in den Editor.
5. Ersetzen Sie im Inhalt dann “C:”durch die in Schritt 2 kopierte Ausgabe und speichern Sie.
6. Das Citrix Director-Symbol wird jetzt korrekt angezeigt.

[DIR-21012]

Bekannte Probleme in 1912 CU7

- Versuche, die Citrix Workspace-App zu installieren, schlagen unter Windows Server 2012 R2 möglicherweise fehl. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX477888. [LCM-12342]
- Versuche, die Citrix Workspace-App gleichzeitig mit dem VDA zu installieren, schlagen möglicherweise fehl, wenn kein Internetzugang besteht. Als Workaround müssen Sie entweder die Installation der Citrix Workspace-App überspringen oder Microsoft WebView installieren (was eine Voraussetzung für die Citrix Workspace-App ist), bevor Sie den VDA installieren. [LCM-12992]

Bekannte Probleme in 1912 CU6

- Microsoft unterstützt nicht mehr das Erstellen neuer VMs mit nicht-verwalteten Datenträgern in Azure. Bereits erstellte Mastervorlagen mit nicht-verwalteten Datenträgern können jedoch verwendet werden. [LCM-10287]

- Der Installationsbefehlszeilenparameter /`IGNORE_DB_CHECK_FAILURE` wird in 1912 LTSR-CUs nicht unterstützt. [LCM-11958]
- Versuche, die Citrix Workspace-App zu installieren, schlagen unter Windows Server 2012 R2 möglicherweise fehl. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX477888. [LCM-12342]
- Versuche, die Citrix Workspace-App gleichzeitig mit dem VDA zu installieren, schlagen möglicherweise fehl, wenn kein Internetzugang besteht. Als Workaround müssen Sie entweder die Installation der Citrix Workspace-App überspringen oder Microsoft WebView installieren (was eine Voraussetzung für die Citrix Workspace-App ist), bevor Sie den VDA installieren. [LCM-12992]
- Das Feature "Positivliste für virtuelle Kanäle"funktioniert möglicherweise nicht in Microsoft Teams. [CVADHELP-21287]

Bekannte Probleme in 1912 CU5

- 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]
- Wenn Sie diese Version des VDAs verwenden, schlagen die von der Organisationseinheit auf eine Maschine angewendeten Citrix-Richtlinien manchmal fehl. [CVADHELP-19826]
- Nach dem Upgrade des Delivery Controller auf Version 1912 CU5 kann beim geplanten Neustart von nicht energieverwalteten VDAs ein Fehler auftreten. [CVADHELP-20138]
- Das Feature "Positivliste für virtuelle Kanäle"funktioniert möglicherweise nicht in Microsoft Teams. [CVADHELP-21287]

Bekannte Probleme in 1912 CU4

- Wenn Sie diese Version des VDAs verwenden, schlagen die von der Organisationseinheit auf eine Maschine angewendeten Citrix-Richtlinien manchmal fehl. [CVADHELP-19826]
- 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]
- Wenn Sie eine virtuelle Citrix-Sitzung verlassen, können eines oder mehrere der folgenden Probleme auftreten:

  - Der VDA listet weiterhin die abgebrochene Sitzung und den Prozess logonui.exe auf. Der Prozess logonui.exe kann zwangsweise beendet werden.
  - Die Sitzung wird mit einem leeren Benutzernamen in Citrix Studio angezeigt.
  - Möglicherweise können Sie keine weiteren Sitzungen starten.

  Ein privater Fix ist unter CTX340125 verfügbar.

  [CVADHELP-19182]

- Das Feature "Positivliste für virtuelle Kanäle"funktioniert möglicherweise nicht in Microsoft Teams. [CVADHELP-21287]

Bekannte Probleme in 1912 CU3

- Die Aktualisierung der CEIP-Option für die Lizenzierung mit dem Cmdlet `Set-LicCEIPOption` schlägt mit einem Kommunikationsfehler fehl. Als Workaround kann die CEIP-Option über Citrix Licensing Manager aktiviert werden. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX220679. [LCM-9169]
- 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]
- Das Feature "Positivliste für virtuelle Kanäle"funktioniert möglicherweise nicht in Microsoft Teams. [CVADHELP-21287]

Bekannte Probleme in 1912 CU2

- Das Konfigurieren Ihrer On-Premises-Site mit Citrix Analytics for Performance von Director aus schlägt möglicherweise fehl, wenn der Delivery Controller eine Version von Microsoft .NET Framework vor 4.8 ausführt. Aktualisieren Sie als Workaround das .NET Framework für den Delivery Controller auf Version 4.8. [LCM-9255]
- Die Anmeldung bei einer nicht vermittelten RDP-Sitzung mit UPN-Anmeldeinformationen kann zu einer nicht abgefangenen Ausnahme führen. In 1912 LTSR CU2 wurde eine Namensübersetzung für UPN-Benutzernamen eingeführt. Die Kürzung des Benutzernamens aufgrund des in RDS-Datenstrukturen festgelegten Limits führt zu einem falschen Benutzernamen. Dies führt zu der nicht abgefangenen Ausnahme. [CVADHELP-16510]
- Wenn die .NET Framework-Version nach dem Upgrade auf 1912 LTSR CU2 nicht mindestens 4.7.2 ist, schlägt Azure Resource Manager fehl. [CVADHELP-16533]

- 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]
- Citrix Director zeigt möglicherweise Richtlinieninformationen nicht an. Das Problem tritt auf, wenn Sie Sitzungsdetails für 1912 LTSR CU2-VDAs in einer älteren Director-Version anzeigen. Führen Sie als Workaround die in der Aktualisierungsreihenfolge aufgeführten Schritte aus. [LCM-8201]
- Manche Dateioperationen, die in einer veröffentlichten App oder einer veröffentlichten Desktopsitzung an einem Clientlaufwerk ausgeführt werden, schlagen möglicherweise mit einer Fehlermeldung "Berechtigung verweigert"fehl. Auf der lokalen Maschine wird evtl. auch gemeldet, dass eine Datei in Verwendung ist. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX285248. [HDX-26969]

Bekannte Probleme in 1912 CU1

Zusätzlich zu den bekannten Problemen im Erstrelease von 1912 LTSR sind für CU1 folgende Probleme bekannt:

Citrix Provisioning

- Beim Versuch, ein Citrix Provisioning-Zielgerät mit Version 1912 LTSR oder 1912 LTSR CU1 auf eine frühere Version herabzustufen, wird möglicherweise die folgende Meldung angezeigt:

  Installation fehlgeschlagen.

  Um das Problem zu umgehen, deinstallieren Sie zunächst die Version 1912 LTSR oder 1912 LTSR CU1 und installieren dann die frühere Version neu. [LCM-7341]
- Beim Upgrade von Provisioning Server von Version 7.15 Cumulative Update 5 auf Version 1912 wird möglicherweise zweimal eine Warnmeldung angezeigt. Die Meldung wird aufgrund einer Abhängigkeit vom CDF-Installationsprogramm (einer separaten Komponente von Citrix Virtual Apps and Desktops) bei der Installation von Citrix Provisioning angezeigt. Das Provisioning-Installationsprogramm kann die vom CDF-Installationsprogramm erstellte Neustartmeldung nicht unterdrücken. Infolgedessen wird die Neustartmeldung zweimal angezeigt. [LCM-7594]

Allgemein

- 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]

Protokollanzeige

- Nach Ausführung des PowerShell-Cmdlets `BrokerHostingPowerAction` wird auf der Studio-Seite **Protokollierung** fälschlicherweise angezeigt, dass das Cmdlet fehlgeschlagen sei. Überprüfen Sie als Workaround das Ergebnis auf dem Host. [BRK-7002]

Inhaltsumleitung

- Bei aktivierter Browser-Inhaltsumleitung kann ein Fehler auftreten, wenn Sie in Chrome mit der rechten Maustaste auf einen Hyperlink klicken, um eine neue Registerkarte zu öffnen. Wählen Sie als Workaround in der Meldung `Always allow pop-ups and redirects` die Option `Pop-ups blocked`. [LCM-7480]

Installation und Upgrade

- Bei aktiviertem App-Schutz wird die importierte App-Schutz-Featuretabelle möglicherweise entfernt, wenn Sie ein Upgrade von Version 1912 auf Version 1912 LTSR CU1 durchführen. Das Update des StoreFront-Features kann ebenfalls verloren gehen. Führen Sie als Workaround die folgenden Schritte aus:

  1. Importieren Sie auf einem aktualisierten CU1-Controller erneut die mit dem CU1-Download verfügbare XML-Featuretabelle.
  2. Aktivieren Sie auf dem StoreFront-Server die App-Schutzfunktion neu.

  [LCM-7872]

Bekannte Probleme im Erstrelease von 1912

Installation und Upgrade

- Wenn Sie bereits den universellen (UPS) Version 19061022052 installiert haben, fügt das Upgrade von UPS mit dem Metainstaller 1906.2 keine neuen UPS-Funktionen hinzu. Nach dem Upgrade wird nur die Versionsnummer des universellen Druckservers unter “Programme und Features”in 19062022068 geändert. [HDX-20674]
- Wenn Sie den Citrix Virtual Apps and Desktops-Metainstaller ausführen und auf der Seite “Diagnose”auf **Verbinden** klicken, ohne zuerst **Diagnoseinformationen sammeln** auszuwählen,

ist nach dem Schließen des Dialogfelds "Mit Citrix Insight Services verbinden"die Schaltfläche **Weiter** deaktiviert und Sie können nicht zur nächsten Seite wechseln. Um die Schaltfläche **Weiter** wieder zu aktivieren, aktivieren Sie die Option **Diagnoseinformationen sammeln** und deaktivieren Sie sie sofort wieder. [XAXDINST-572]

- Wenn Sie ein Upgrade von Studio von XenApp und XenDesktop 7.15 LTSR (7.15 Studio) auf Citrix Virtual Apps and Desktops 7 1912 LTSR (1912 Studio) durchführen, dann 1912 Studio deinstallieren und 7.15 Studio neu installieren, wird Studio nicht gestartet mit dem Fehler: Cannot load windows PowerShell snap-in PvsPsSnapIn error. Um dieses Problem zu beheben, löschen Sie vor der Neuinstallation von 7.15 Studio manuell PvsPsSnapIn.dll unter `C:\Program Files\Citrix\PowerShell SDK`. [XAXDINST-610]
- Wenn Sie eine Liste gültiger Optionen für den Befehl `XenDesktopServerSetup.exe` anfordern, wird die Option `/no_webstudio` aufgelistet. Diese Option ist nur zur internen Verwendung bestimmt. Bitte nicht verwenden. [STUD-9701]

VDA-Installation

- Nach der Installation eines VDA und vor dem Neustart des Computers wird eine Citrix Files Fehlermeldung angezeigt: "Incompatible .NET Framework, shutting down. Install one of the KBs listed on this Known Issue page to resolve:.."Als Workaround installieren Sie KB4054856 vor der VDA-Installation auf `NDP471-KB4033342-x86-x64-AllOS-ENU.exe`. [LCM-7563]

Allgemein

- Wenn MCS nicht-persistente 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]
- In Citrix Hypervisor legt der Citrix Desktopdienst nach Installation eines neuen VDA den XenTools-Registrierungswert fälschlicherweise auf UTC fest. Der Dienst überprüft nicht die Systemzeit, was zu einem Verbindungsfehler führt, sodass die Maschine nicht registriert wird. Dies ist ein vorübergehendes Problem. Der VDA korrigiert die Systemzeit, wenn er aus verschiedenen Quellen synchronisiert wird. Der aktuelle Fix setzt den XenTools-Registrierungswert nur dann auf UTC, wenn auch die Betriebssystemzeit UTC ist. [PMCS-5425]
- Wenn Sie den Hypervisor verwenden, um eine mit Citrix Virtual Apps and Desktops bereitgestellte virtuelle Maschine zu löschen, können Sie die Maschine möglicherweise nicht dem Katalog hinzufügen, da der Basisdatenträger als Teil des Löschvorgangs der virtuellen Maschine auch gelöscht wird. [PMCS-8591]

- Verwenden einer Vorlage für das Provisioning eines Katalogs wird als experimentelles Feature betrachtet. Mit dieser Methode schlägt die Vorbereitung der virtuellen Maschine möglicherweise fehl. Daher kann der Katalog nicht mit der Vorlage veröffentlicht werden. [PMCS-602]
- Wenn Sie versuchen, eine geschützte App zu Ihren **Favoriten**hinzuzufügen, wird möglicherweise folgende Meldung angezeigt: "Die Apps stehen zurzeit nicht zur Verfügung…". Wenn Sie dann auf **OK** klicken, wird gemeldet, dass die App nicht hinzugefügt werden kann. Wenn Sie dann zur Seite **Favoriten** wechseln, wird die geschützte App dort angezeigt, kann aber nicht aus den **Favoriten** entfernt werden. [WSP-5497]
- Jedes Mal, wenn Sie eine komprimierte Datei mit der Citrix Workspace-App für HTML5 mit End-to-End-SSL über einen Chrome- oder Safari-Browser hochladen, wird die Sitzungszuverlässigkeit möglicherweise gestartet und schließlich eine unbrauchbare Sitzung erstellt. Starten Sie die Sitzung neu, um das Problem zu beheben. Um die Dateiübertragung wieder zu aktivieren, melden Sie sich von der aktuellen Sitzung ab. [HDX-22106]
- Nach der Installation des Web-App-Plug-Ins für Skype for Business werden Webcams möglicherweise nicht aufgelistet und Besprechungsseiten in Firefox werden möglicherweise nicht automatisch aktualisiert. [HDX-13288]
- Beim Upgrade des VDA auf Version 1906 wird automatisch der neue MCS-E/A-Treiber installiert, wenn er zuvor nicht installiert war. Zielgeräte können daraufhin nicht im schreibgeschützten Modus gestartet werden. Citrix empfiehlt, aktualisierte MCS-E/A-Funktionen und Citrix Provisioning nicht in derselben Windows-Umgebung zu installieren. [PVS-4151]
- 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]
- Wenn Sie eine Verbindung zu einer neuen Sitzung herstellen, die Verbindung trennen und anschließend wieder herstellen, können die Symbole auf dem Desktop flimmern. Um dieses Problem zu umgehen, setzen Sie das Benutzerprofil zurück, melden sich ab und melden sich neu an. [HDX-15926, UPM-1362]
- Bei Verwendung von Windows 10 1809 LTSC werden VCLibs-Abhängigkeiten nicht installiert. [HDX-16754]
- Das Kombinationsfeld wird möglicherweise fehlerhaft angezeigt, wenn ein Benutzer ein Kombinationsfeld auswählt, das bereits auf dem Host im Fokus ist. Um dieses Problem zu umgehen, wählen Sie zuerst ein anderes UI-Element und dann das Kombinationsfeld aus. [HDX-21671]
- Beim Versuch, sich erneut mit einer Sitzung zu verbinden, wird der Desktop möglicherweise nicht geladen und es wird ein graues Fenster angezeigt. Das Problem tritt auf, wenn VDA Version 1909 unter Microsoft Windows Server 2019 ausgeführt wird. [HDX-21804]

- Sie haben den lokalen App-Zugriff aktiviert. Wenn Sie eine VDA-Sitzung mit Windows 2012 R2 starten, die Sitzung trennen und erneut eine Verbindung herstellen und dann eine lokale Anwendung starten und diese maximieren, wird die Anwendung möglicherweise von der VDA-Taskleiste abgeschnitten. [HDX-21913]
- Bei konfigurierter IPv4- und IPv6-Adressierung im Netzwerk kann es vorkommen, dass auf Ressourcen in einer Bereitstellungsgruppe nicht zugegriffen werden kann, wenn die Bereitstellungsgruppe eine Broker-Zugriffsrichtlinienregel verwendet, die nur eine IPv4-Adressfilterung zulässt. Für eine fehlerfreie Funktion der Ressourcenfilterung konfigurieren Sie die Broker-Zugriffsrichtlinienregel so, dass IPv4- und IPv6-Clientadressen enthalten sind. [WADA-7776]

  Um beispielsweise Regeln zu definieren, die einen Zugriff auf IPv4- und IPv6-Adressen über 'direct to StoreFront'und 'Citrix Gateway'ermöglichen, verwenden Sie PowerShell wie folgt:

  ```
  1  Set-BrokerAccessPolicyRule -Name "Apps_Direct" -
         IncludedClientIPFilterEnabled $True -IncludedClientIPs @("
         10.0.0.1","2001::3")
  2  Set-BrokerAccessPolicyRule -Name "Apps_AG" -
         IncludedClientIPFilterEnabled $True -IncludedClientIPs @("
         10.0.0.1","2001::3")
  ```

  Um eine Regel zu bestätigen, verwenden Sie PowerShell wie folgt:

  ```
  1  Get-BrokerAccessPolicyRule -Name \"Apps\_Direct\" | Select Name,
         IncludedClientIPFilterEnabled,IncludedClientIPs
  ```

  Bei korrekt definierter Regel für IPv4- und IPv6-Adressen wird Folgendes angezeigt:

  ```
  1  Name          IncludedClientIPFilterEnabled IncludedClientIPs
  2  --                  -------------------------- -----------------
  3  Apps_Direct                           True {
  4  10.0.0.1/32, 2001::3/128 }
  ```

- Wenn Anwendungen aus Microsoft Office 365 Build 16.0.7967 und später als Anwendungen von einem Windows Server 2019-Host veröffentlicht werden, schlägt die Office-Lizenzaktivierung fehl. Citrix arbeitet mit Microsoft zusammen, um diese Microsoft-Einschränkung zu beheben. Der unterstützte Workaround besteht darin, Windows Server 2016-VDAs zu installieren, die die Web Authentication Manager-Komponente, welche die Probleme verursacht, nicht enthalten. [LCM-7637]
- Citrix Virtual Apps and Desktops unterstützt nicht die delegierten Administratoren von System Center Virtual Machine Manager (SCVMM) mit Zugriff auf mehrere Hostgruppen der obersten Ebene (ohne Root) und doppelten Hostgruppennamen. Die folgende Fehlermeldung wird beim Hinzufügen einer SCVMM-Hostingverbindung über das delegierte Administratorkonto angezeigt:

  Unerwarteter Fehler. Wenden Sie sich an den Citrix Support.

[CVADHELP-10669]

- 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]

Studio

- In einigen Fällen wird der Energiezustand der virtuellen Maschine als unbekannt angezeigt, selbst wenn das Gerät registriert ist. Um dieses Problem zu beheben, bearbeiten Sie den Registrierungsschlüsselwert `HostTime`, um die Zeitsynchronisierung mit dem Host zu deaktivieren:

  ```
  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\XenTools\HostTime="Local"
  ```

  ```
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\XenTools\HostTime="Local"
  ```

> **Tipp:**
>
> Der Standardwert ist `HostTime="UTC"`. Wählen Sie einen anderen Wert als UTC, zum Beispiel `Local`. Diese Änderung deaktiviert die Zeitsynchronisierung mit dem Host. [BRK-4187]

Director

- Der Link **Konsole** unter "Citrix Director > Maschinendetails"startet in Microsoft Edge 44 und Firefox ESR 68 nicht die Maschinenkonsole. [DIR-8160]
- Wenn Sie ein Upgrade auf Director 7 1903 oder höher durchführen und den Browsercache nicht löschen (das Kontrollkästchen "Cache deaktivieren"nicht aktiviert haben), gehen benutzerdefinierte Berichte verloren und auf der Director-Registerkarte "Benutzerdefinierte Berichte"wird ein unerwarteter Serverfehler gemeldet. UI-Designunterschiede zwischen früheren und aktuellen Versionen von Director können dieses Problem verursachen. Deaktivieren Sie den Cache und erzwingen Sie eine Aktualisierung, um alte benutzerdefinierte Berichte anzuzeigen und neue zu erstellen und anzuzeigen. [DIR-7634]

Grafik

- Das Festlegen der Richtlinie **Fensterinhalt beim Verschieben anzeigen** auf **Nicht zugelassen** funktioniert nicht auf ESXi und Hyper-V. [HDX-22002]

- Wenn Sie eine Videovorschau mit einer 64-Bit-Webcam-App über die Theora-Komprimierung starten, kann die Sitzung abstürzen. [HDX-21443]
- Skype Universal Windows-App (UWA) wird mit einem schwarzen Hintergrund gestartet. In einigen Fällen nimmt dieser Hintergrund den gesamten Bildschirm des Clients ein. [HDX-22088]
- In einigen Fällen kann eine Anwendung im Hintergrund gestartet werden, während eine andere Anwendung gerade im Fokus steht. Dadurch geht die lokale Fensterreihenfolge verloren. [HDX-21569]
- In der XenCenter-Konsole wird nach dem Trennen einer XenDesktop-Sitzung möglicherweise ein leerer Bildschirm angezeigt. Senden Sie als Workaround STRG+ALT+LÖSCH an die XenCenter-Konsole, damit der Konsolenbildschirm angezeigt wird. [HDX-17261]
- DPI stimmt während einer Sitzung mit Windows-Multisitzungs-OS 2016 oder 2019 möglicherweise nicht überein, wenn die DPI auf dem Client geändert und die Sitzung wieder verbunden wird. Als Workaround ändern Sie die Größe des Sitzungsfensters auf die DPI. [HDX-17313]
- Diese Probleme betreffen die ADM-Hardwarecodierung. [HDX-20476]:
  - Pixelierung kann auftreten, wenn die Citrix Workspace-App für Windows verwendet wird. Legen Sie als Workaround die folgende Registrierungseinstellung auf dem Client vor, auf dem die Citrix Workspace-App für Windows installiert ist:

    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\GfxRe
    (32-Bit)

    HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced
    (64-Bit)

    Name: MaxNumRefFrames

    Typ: DWORD

    Wert: 5
  - Bei Verwendung der 4k-Auflösung ist die Leistung evtl. nicht optimal. Das Problem bewirkt eine Bildfrequenz von nur 7–10 Frames pro Sekunde. Außerdem erhöht sich die Codierungszeit.
  - Bei Verwendung des Selective H.264-Grafikmodus kann während der ersten zwei bis fünf Videosekunden ein Ruckeln auftreten. Das RapidFire-SDK ist nicht für diesen Anwendungsfall konzipiert.

Drucken

- 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 unter CTX213540. [HDX-5043, 335153]

- Der Standarddrucker ist im Druckdialogfeld möglicherweise nicht korrekt gekennzeichnet. Dieses Problem hat keine Auswirkungen auf Druckaufträge, die an den Standarddrucker gesendet werden. [HDX-12755]

Maschinenerstellungsdienste

- In AWS-Umgebungen werden beim Starten und Beenden von Volumeworker-Instanzen die zugehörigen Netzwerkschnittstellen nicht entfernt. Um dieses Problem zu beheben, löschen Sie Netzwerkschnittstellen manuell, deren Bedingungen in folgendem Zustand sind: `Available && Description: "XD NIC"&& tag: "XdConfig : XdProvisioned=true"` [PMCS-20775]

App-V

- Wenn Sie mehr als 100 App-V-Anwendungen in einer einzelnen Bereitstellungsgruppe veröffentlichen, werden Anwendungen möglicherweise nicht gestartet. Um diesen Grenzwert zu erhöhen, erhöhen Sie mit der MaxReceivedMessageSize-Eigenschaft für das entsprechende Bindungselement die maximal zu empfangene Nachrichtengröße. Führen Sie dies in der Konfiguration des Delivery Controllers und/oder Broker-Agent auf dem VDA aus. [APPV-11]

Probleme mit Drittanbieterprodukten

- Chrome unterstützt UI Automation nur für Symbolleisten, Registerkarten, Menüs und Schaltflächen von Webseiten. Aufgrund dieses Chrome-Problems funktioniert die automatische Tastaturanzeige möglicherweise nicht in einem Chrome-Browser auf Touchgeräten. Führen Sie als Problemumgehung `chrome --force-renderer-accessibility` aus. Alternativ können Sie eine neue Browserregisterkarte öffnen, `chrome://accessibility` eingeben und die Unterstützung für **Native accessibility API** für spezifische oder alle Seiten aktivieren. Außerdem können Sie beim Veröffentlichen einer nahtlosen App Chrome mit dem Switch `--force-renderer-accessibility` veröffentlichen. [HDX-20858]
- Ein Problem in Microsoft Windows 10 Version 1809 kann bei Verwendung des Surface Pro mit Surface Book-Stift zu leicht unberechenbarem Verhalten führen. [HDX-17649]
- Ein unter Azure ausgeführter VDA kann bei Verwendung von Enlightened Data Transport (EDT) abstürzen und eine Wiederherstellung der Sitzungsverbindung erfordern. Legen Sie

als Workaround in Azure-Umgebungen edtMSS=1350 und OutbufLength=1350 fest. Weitere Informationen finden Sie unter CTX231821. [HDX-12913]

- Bei der Browserinhaltsumleitung funktioniert beim Abspielen eines YouTube-Videos mit dem YouTube-HTML5-Videoplayer der Vollbildmodus möglicherweise nicht. Nach dem Klicken auf das Symbol in der unteren rechten Ecke des Videos wird das Video nicht vergrößert und im gesamten Seitenbereich verbleibt ein schwarzer Hintergrund. Als Workaround klicken Sie auf die Schaltfläche "Vollbild"und wählen Sie Kinomodus. [HDX-11294]

Auslaufende Features

October 9, 2023

Die Ankündigungen in diesem Artikel bieten Ihnen frühzeitige Informationen über Plattformen, Citrix Produkte und Features, die ausgemustert werden, sodass Sie rechtzeitig Geschäftsentscheidungen treffen können. Citrix überwacht die Nutzung von Features und Feedback, um den geeigneten Zeitpunkt für eine Außerbetriebnahme zu wählen. Diese Informationen unterliegen Änderungen in nachfolgenden Releases und enthalten ggf. nicht jedes veraltete Element. Informationen zum Produktlebenszyklussupport finden Sie unter Product Lifecycle Support Policy. Hinweise zur Wartungsoption für Long Term Service Release (LTSR) finden Sie unter https://support.citrix.com/article/CTX205549.

Veraltete und entfernte Produkte und Features

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

Veraltete Elemente werden nicht sofort entfernt. Citrix unterstützt sie in diesem Citrix Virtual Apps and Desktops 7 1912 Long Term Service Release (LTSR) weiterhin, in einer zukünftigen Version werden sie jedoch entfernt.

Entfernte Elemente wurden entweder entfernt oder in Citrix Virtual Apps and Desktops nicht mehr unterstützt. Die **fett** formatierten Datumsangaben weisen auf Änderungen in diesem Release hin.

Element	Einstellung der Unterstützung angekündigt	Entfernt in	Alternative
Unterstützung für das WebRTC SDP-Format (Plan B)	2308	—	Aktualisieren Sie die Citrix Workspace-App auf eine unterstützte Version.
Unterstützung für den Einzelfenstermodus in Optimierung für Microsoft Teams	2308	—	Aktualisieren Sie die Citrix Workspace-App auf eine Version, die den Mehrfenstermodus unterstützt. Weitere Informationen finden Sie unter Featurematrix und Versionsunterstützung.
Citrix Provisioning-Zielgeräte zur Verwaltung in Citrix Virtual Apps and Desktops-Kataloge importieren	1912 LTSR	-	Verwenden Sie den Citrix Provisioning-Assistenten zum Exportieren von Geräten.
StoreFront-Browserunterstützung für Microsoft Edge (Legacy)	1912 LTSR CU2	**1912 LTSR CU3**	Upgrade auf Microsoft Edge (basierend auf Chromium).
Citrix License Administration Console (zuletzt enthalten in Windows-Lizenzserver 11.16.3 Build 30000, ab Windows-Lizenzserver v11.16.6 Build 31000 entfernt).	1912 LTSR CU2	1912 LTSR CU2	Verwenden Sie den Citrix Licensing Manager.

Element	Einstellung der Unterstützung angekündigt	Entfernt in	Alternative
Citrix SCOM Management Packs für XenApp und XenDesktop, Provisioning Services und StoreFront. Informationen zu Produktversionen, die überwacht werden können, finden Sie in der Dokumentation zu Citrix SCOM Management Packs.	**1912†**		Verwenden Sie Director zur Überwachung und Verwaltung Ihrer Bereitstellung. Weitere Informationen zum Ende des Lebenszyklus von SCOM und Alternativen finden Sie unter https://support.citrix.com/article/CTX266943.
Unterstützung für Microsoft .NET Framework-Versionen vor Version 4.8 für VDAs und Serverkernkomponenten. Lieferumfang: Delivery Controller, Studio, Director und StoreFront.	**1912**		Upgrade auf .NET Framework Version 4.8.
VDAs unter Windows Server 2012 R2.	**1912**		Installation von VDAs unter einem unterstützten Betriebssystem.
AppDNA - Komponente für die Anwendungsmigration in Citrix Virtual Apps and Desktops Premium Edition.	1909		
Installieren von Studio auf 32-Bit-Maschinen (x86).	1909		Installation unter einem unterstützten x64-Betriebssystem.

Element	Einstellung der Unterstützung angekündigt	Entfernt in	Alternative
Unterstützung für den Excel-Hook in Seamlessanwendungen. Dieser wurde zum Erstellen separater Taskleistensymbole für jede Microsoft Excel 2010-Arbeitsmappe verwendet.	1909	1909	
Kernserverkomponenten unter Windows Server 2012 R2 (einschließlich Service Packs). Lieferumfang: Delivery Controller, Studio und Director.	1906		Installation unter einem neueren unterstützten Betriebssystem.
Unterstützte Sitekonfiguration, Konfigurationsprotokollierung und Datenbanküberwachung für Microsoft SQL Server Version 2008, R2, 2012 und 2014 (einschließlich aller Service Packs und Editionen).	1906		Datenbankinstallation auf einer unterstützten Microsoft SQL Server-Version.

Element	Einstellung der Unterstützung angekündigt	Entfernt in	Alternative
Unterstützung für VDAs unter Windows 10 auf x86-Plattformen.	1906	1909*	Installation von VDAs unter einem unterstützten x64-Betriebssystem. **Dieses Feature wird in Citrix Virtual Apps and Desktops 7 1912 LTSR weiterhin unterstützt.**
Entfernen von Citrix Smart Tools Agent von Citrix Virtual Apps and Desktops-Installationsmedien.	1903	1906	
Entfernen der Delivery Controller-Optionen für die folgenden veralteten Produkte in StoreFront: VDI-in-a-Box und XenMobile (9.0 oder früher).	1903	1903	
Unterstützung für Linux VDAs unter Red Hat Enterprise Linux/CentOS 7.5.	1903	1903	Installation von Linux VDAs unter einer späteren Version von Red Hat Enterprise Linux
StoreFront-Unterstützung für Benutzer zum Zugriff auf Desktops auf Desktopgerätewebsites	1811	**1912**	Verwenden Sie Desktop Lock für Anwendungsfälle ohne Domänenanbindung.
Unterstützung für Framehawk-Anzeigeremoting	1811	1903	Verwenden Sie Thinwire mit aktiviertem adaptivem Transport.

Element	Einstellung der Unterstützung angekündigt	Entfernt in	Alternative
Unterstützung für Citrix Smart Scale in allen Versionen von Citrix Virtual Apps and Desktops (und XenApp und XenDesktop) Diese Funktionalität erreicht am 31. Mai 2019 das Ende des Lebenszyklus.	1808	1906	Erwägen Sie, die Verwendung von Virtual Apps and Desktops Service in Citrix Cloud für bessere Funktionen zur Energieverwaltung.
Unterstützung für Microsoft .NET Framework-Versionen 4.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2 und 4.7 durch Citrix StoreFront, Citrix VDAs, Citrix Studio, Citrix Director und Citrix Delivery Controller.	7.18	1808	Upgrade auf .NET Framework Version 4.7.1 oder höher (Das Installationsprogramm installiert .NET Framework 4.7.1 automatisch, wenn es nicht bereits installiert ist.)
Unterstützung für Linux VDAs unter Red Hat Enterprise Linux 7.3.	7.18	1808	Installation von Linux VDAs unter einer späteren Version von Red Hat Enterprise Linux
StoreFront-Unterstützung für TLS 1.0- und TLS 1.1-Protokolle zwischen Citrix Virtual Apps and Desktops (zuvor “XenApp und XenDesktop”) sowie Citrix Receiver und Workspace Hub.	7.17		Aktualisieren Sie Citrix Receiver auf eine Citrix Workspace-App-Version, die TLS 1.2 unterstützt Weitere Informationen zur Citrix Workspace-App finden Sie unter https://docs.citrix.com/en-us/citrix-workspace-app.

Element	Einstellung der Unterstützung angekündigt	Entfernt in	Alternative
VDA-Unterstützung für die Richtlinieneinstellung "Automatische Installation von mitgelieferten Druckertreibern"	7.16	7.16	Keine. Richtlinieneinstellung, die nur von VDAs unter früheren Betriebssystemen (Windows 7, Windows Server 2012 R2 und früher) unterstützt wird.
Unterstützung für den Linux VDA unter SUSE Linux Enterprise Server 11 Service Pack 4.	7.16	7.16	Installation von Linux-VDAs unter einer unterstützten SUSE-Version
Unterstützung für Citrix WDDM-Treiber auf VDAs	7.16	7.16	Der Citrix WDDM-Treiber wird nicht mehr mit VDAs installiert.
Mobility SDK/Mobile SDK (aus dem älteren Citrix Labs)	7.16		Ersetzt durch Einstellungen der Richtlinie "Mobilerfahrung"und native Benutzeroberflächen für gehostete Desktops / Apps.

Element	Einstellung der Unterstützung angekündigt	Entfernt in	Alternative
VDAs unter Windows 10 Version 1511 (Schwellenwert 2) und früheren Releases von Windows-Einzelsitzungs-OS, einschließlich Windows 8.x oder Windows 7 (siehe https://www.citrix.com/blogs/2018/01/08/the-citrix-strategy-for-windows-7-virtual-desktop-users/).	7.15 LTSR (und 7.12)	7.16	Installieren Sie VDAs für Einzelsitzungs-OS unter der Mindestversion von Windows 10 (1607, Redstone 1) oder neueren Semi-Annual Channels. Bei der Verwendung von 1607 LTSB empfehlen wir einen VDA der Version 7.15. Siehe CTX224843.
VDAs unter Windows Server 2008 R2 und Windows Server 2012 (einschließlich Service Packs)	7.15 LTSR (und 7.12)	7.16	Installation von VDAs unter einem unterstützten Betriebssystem.
Desktopgestaltungsumleitung (bisher “DirectX Command Remoting”, DCR)	7.15 LTSR	7.16	Verwenden Sie Thinwire.
Citrix Receiver für Web, klassisches Design mit “grünen Blasen”	7.15 LTSR (und StoreFront 3.12)	1903	Citrix Receiver für Web, einheitliche Benutzeroberfläche.

Element	Einstellung der Unterstützung angekündigt	Entfernt in	Alternative
Kernkomponenten unter Windows Server 2008 R2 und Windows Server 2012 (einschließlich Service Packs). Umfasst: Delivery Controller, Studio, Director, StoreFront, Lizenzserver und universeller Druckserver.	7.15 LTSR	7.18	Installation von Komponenten auf einem unterstützten Betriebssystem.
Self-Service-Kennwortzurücksetzung unter Windows Server 2012 und Windows Server 2008 R2 (einschließlich Service Packs)	7.15 LTSR	7.18	Installation unter einem neueren unterstützten Betriebssystem.
Studio unter Windows 7, Windows 8 und Windows 8.1 (einschließlich Service Packs)	7.15 LTSR	7.18	Installieren Sie Studio unter einem unterstützten Betriebssystem.

Element	Einstellung der Unterstützung angekündigt	Entfernt in	Alternative
Flash-Umleitung	7.15 LTSR	**1912**	Erstellen Sie Videos als HTML5-Video. Verwenden Sie die HTML5-Videoumleitung für verwalteten Inhalt und die Browserinhaltsum-leitung für öffentliche Websites. Weitere Informationen finden Sie unter Hinweis zum End of Life von Flash-Umleitung.
Citrix Online-Integration (GoTo-Produkt) in StoreFront	7.14 (und StoreFront 3.11)	StoreFront 3.12	
Das Benutzerkonto “CtxAppVCOMAdmin”, das bei der VDA-Installation erstellt und der lokalen Administratorgruppe auf der VDA-Maschine hinzugefügt wurde, wird nicht mehr erstellt. Der zu Grunde liegende “COM” -Mechanismus wird ebenfalls entfernt.	7.14	7.14	Der Windows-Dienst “CtxAppVService”hat dieselbe Funktion. Er wird automatisch installiert und konfiguriert und erfordert keinen Benutzereingriff.
Unterstützung des universellen Druckservers (UpsServer) unter Windows Server 2008 (32-Bit)	7.14	7.14	Installation unter einem neueren unterstützten Betriebssystem.

Element	Einstellung der Unterstützung angekündigt	Entfernt in	Alternative
StoreFront und Receiver für Web unter Internet Explorer 8	7.13	7.13	
VDA-Befehlszeilenoption "/no_appv"zum Verhindern der Installation der Citrix App-V-Komponenten	7.13	7.13	Verwenden Sie folgende Befehlszeilenoption zum Verhindern der Komponenteninstallation: /exclude "Citrix Personalization for App-V –VDA".
Das vollständige Produktinstallationsprogramm installiert das Snap-In Citrix.Common.Commands nicht mehr. Bei vorhandenen Bereitstellungen wird es automatisch entfernt.	7.13	7.13	Einige PowerShell-Befehle des Citrix.Common.Commands-Snap-Ins sind im XenApp 6.5-SDK weiterhin verfügbar.
Teile der Funktionen des *-CtxIcon-Cmdlets zum Bearbeiten von Symboldaten.	7.13	7.13	Jetzt im Broker-Service-Cmdlet *-BrokerIcon enthalten.
Legacy-Thinwire-Modus	7.12	7.16	Verwenden Sie Thinwire. Wenn Sie den Legacy-Thinwire-Modus unter Windows Server 2008 R2 verwenden, migrieren Sie zu Windows Server 2012 R2 oder Windows Server 2016 und verwenden Sie Thinwire.

Element	Einstellung der Unterstützung angekündigt	Entfernt in	Alternative
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 7.16 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. Führen Sie hierfür zunächst ein Upgrade auf XenDesktop 7.6 LTSR (mit dem aktuellen CU) und dann auf die aktuelle oder die LTSR-Version von Citrix Virtual Desktops (zuvor "XenDesktop") durch.
Installation der Komponenten Delivery Controller, Director, StoreFront und Lizenzserver auf 32-Bit-Maschinen (x86).	7.12	7.16	Installation unter einem unterstützten x64-Betriebssystem.
Verbindungsleasing	7.12	7.16	Verwenden Sie den lokalen Hostcache.

Element	Einstellung der Unterstützung angekündigt	Entfernt in	Alternative
XenDesktop 5.6 unter Windows XP. VDA-Installationen unter Windows XP werden nicht unterstützt.	7.12	7.16	Installation von VDAs unter einem unterstützten Betriebssystem.
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.
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.

† **Wichtig**: Nach dem Juni 2020 müssen Sie sämtliche SCOM Management Packs von Ihrer Citrix Virtual Apps and Desktops 7 1912 LTSR-Site entfernen, um Ihre LTSR-Unterstützung und Vorteile zu behalten.

*Feature nicht von der LTSR-Wartungsoption abgedeckt.

Systemanforderungen

June 27, 2024

Einführung

Die Systemanforderungen in diesem Dokument galten zum Zeitpunkt der Freigabe der Produktversion. Das Dokument wird regelmäßig aktualisiert. Nicht in diesem Dokument aufgeführte Systemanforderungen (z. B. Hostsysteme, Citrix Workspace-App und Citrix Provisioning) werden in der jeweiligen Dokumentation beschrieben.

Vor Beginn einer Installation lesen Sie den Artikel Vorbereiten der Installation.

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.

Globalisierungshinweise finden Sie im Knowledge Center-Artikel CTX119253.

Für Komponenten und Features, die auf Windows-Servern installiert werden können, werden Nano Server-Installationen nicht unterstützt, es sei denn, dies wird ausdrücklich erwähnt. Die Server Core-Unterstützung wird nur für Delivery Controller und Director unterstützt.

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. Zur Konfiguration gehören die verwendeten Features, die Anzahl der Benutzer und weitere Faktoren. Die Verwendung der Mindestkonfiguration kann die Leistung beeinträchtigen.

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, Datenbank: siehe Sizing guidance

Komponente	Minimum
Studio	1 GB RAM, 100 MB Festplatte
Director	2 GB RAM, 200 MB Festplatte
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 Bereitstellung individuelle Anforderungen. Im Allgemeinen werden Citrix Virtual Apps-VMs auf der Basis der Hardware und nicht der Benutzerworkloads dimensioniert. (Eine Ausnahme ist RAM. Sie brauchen mehr RAM für Anwendungen, mehr verbrauchen.)

Weitere Informationen:

- Citrix Tech Zone enthält Anweisungen zur VDA-Dimensionierung.
- Unter Citrix Virtual Apps and Desktops Single Server Scalability wird erläutert, wie viele Benutzer oder VMs auf einem einzelnen physischen Host unterstützt werden können.

Microsoft Visual C++ 2017 Runtime

Installieren von Microsoft Visual C++ 2017 Runtime auf einer Maschine, auf der 2015 Runtime installiert ist, kann dazu führen, dass die 2015-Version automatisch entfernt wird. Diese Aktion 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 2019, Standard und Datacenter Edition und mit der Server Core-Option
- Windows Server 2016, Standard und Datacenter Edition und mit der Server Core-Option

- Windows Server 2012 R2, Standard und Datacenter Edition und Server Core für Windows Server 2012 R2

Anforderungen:

- Microsoft .NET Framework 4.7.1 wird automatisch installiert, wenn es (bzw. eine neuere Version) nicht bereits installiert ist.
- Windows PowerShell 3.0 oder höher
- Microsoft Visual C++ 2017 Runtime (32-Bit und 64-Bit)

Datenbank

Unterstützte Versionen von Microsoft SQL Server für die Datenbanken für Sitekonfiguration, Konfigurationsprotokollierung und Überwachung:

- SQL Server 2019, Express, Standard und Enterprise Edition.
- SQL Server 2017, Express, Standard und Enterprise Edition.
  - Neue Installationen: Standardmäßig wird SQL Server Express 2017 mit Cumulative Update 16 zusammen mit dem Controller installiert, wenn keine vorhandene unterstützte SQL Server-Installation erkannt wird.
  - Bei Upgrades werden vorhandene SQL Server Express-Versionen nicht aktualisiert.
- SQL Server 2016 SP1 bis SP3, Express, Standard und Enterprise Edition.
- SQL Server 2014 SP1 bis SP3, Express, Standard und Enterprise Edition.
- 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 SQL Server Express LocalDB 2017 mit CU 16 zur Verwendung mit dem lokalen Hostcache installiert. Diese Installation erfolgt separat von der standardmäßigen SQL Server Express-Installation für die Sitedatenbank. (Bei Controllerupgrades werden vorhandene Microsoft SQL Server Express LocalDB-Versionen nicht aktualisiert. Wenn Sie die LocalDB-Version aktualisieren möchten, folgen Sie den Anweisungen unter Datenbankaktionen.)

Weitere Informationen finden Sie in den folgenden Artikeln:

- Datenbank
- Der Knowledge Center-Artikel CTX114501 enthält die aktuellsten unterstützten Datenbanken.
- Leitfaden für die Datenbankgröße
- Lokaler Hostcache

Citrix Studio

Unterstützte Betriebssysteme:

- Windows Server 2019, Standard und Datacenter Edition
- Windows Server 2016, Standard und Datacenter Edition
- Windows Server 2012 R2, Standard und Datacenter Edition
- Windows 10

Anforderungen:

- Microsoft .NET Framework 4.7.1 wird automatisch installiert, wenn es (bzw. eine neuere Version) nicht bereits installiert ist.
- Microsoft Management Console 3.0 (in allen unterstützten Betriebssystemen enthalten)
- Windows PowerShell 3.0 oder höher

Citrix Director

Unterstützte Betriebssysteme:

- Windows Server 2019, Standard und Datacenter Edition und mit der Server Core-Option
- Windows Server 2016, Standard und Datacenter Edition und mit der Server Core-Option
- Windows Server 2012 R2, Standard und Datacenter Edition und Server Core für Windows Server 2012 R2

Anforderungen:

- Microsoft .NET Framework 4.7.1 wird automatisch installiert, wenn es (bzw. eine neuere Version) nicht bereits installiert ist.
- 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 Software nicht auf Ihrem Server installiert ist, werden Sie aufgefordert, das Windows Server-Installationsmedium einzulegen. Die Software wird dann für Sie 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 WMI-Plug-In für Citrix User Profile Manager auf dem VDA installiert sind (**Zusätzliche Komponenten** im Installationsassistenten). Der Citrix Profilverwaltungsdienst muss ausgeführt werden, 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. Verwenden Sie für den Zugriff auf Director die empfohlenen Webbrowsereinstellungen. 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 Einzelsitzungs-OS

Unterstützte Betriebssysteme:

- Windows 10 (nur x64), Mindestversion 1607
  - Informationen zur Unterstützung von Editionen finden Sie im Knowledge Center-Artikel CTX224843.
  - Informationen zu Citrix bekannten Problemen mit der Version 1709 finden Sie im Knowledge Center-Artikel CTX229052.

Anforderungen:

- Microsoft .NET Framework 4.7.1 wird automatisch installiert, wenn es (bzw. eine neuere Version) nicht bereits installiert ist.

- Microsoft Visual C++ 2017 Runtime (32-Bit und 64-Bit)

Remote-PC-Zugriff verwendet diesen VDA, den Sie auf physischen Büro-PCs installieren. Dieser VDA unterstützt den sicheren Start für Citrix Virtual Desktops-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, wird die Multimediabeschleunigung nicht installiert und funktioniert nicht. Entfernen Sie Media Foundation nicht nach der Installation der Citrix Software von der Maschine. Andernfalls können sich die Benutzer nicht an der Maschine anmelden. Bei den meisten Editionen von Windows-Einzelsitzungs-OS 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.

Informationen über den Linux VDA finden Sie in den Artikeln zu Linux Virtual Delivery Agent.

Zur Verwendung des Server-VDI-Features können Sie über die Befehlszeilenschnittstelle einen VDA für Windows-Einzelsitzungs-OS unter Windows Server 2019 oder Windows Server 2016 installieren. Weitere Informationen finden Sie im Artikel Server-VDI.

Informationen zum Installieren eines VDA auf einer Windows 7-Maschine finden Sie unter Ältere Betriebssysteme.

Virtual Delivery Agent (VDA) für Multisitzungs-OS

Unterstützte Betriebssysteme:

- Windows Server 2019, Standard und Datacenter Edition
- Windows Server 2016, Standard und Datacenter Edition
- Windows Server 2012 R2, Standard 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 4.7.1 wird automatisch installiert, wenn es (bzw. eine neuere Version) nicht bereits installiert ist.
- Microsoft Visual C++ 2017 Runtime (32-Bit und 64-Bit)

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, wird die Multimediabeschleunigung nicht

installiert und funktioniert nicht. 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 Server-Versionen wird das Media Foundation-Feature über den Server-Manager installiert. Weitere Informationen finden Sie unter Vorbereiten der Installation.

Wenn Media Foundation nicht auf dem VDA vorhanden ist, funktionieren diese Multimediafeatures nicht:

- Windows Media-Umleitung
- HTML5-Videoumleitung
- HDX RealTime-Webcamumleitung

Informationen über den Linux VDA finden Sie in den Artikeln zu Linux Virtual Delivery Agent.

Informationen zum Installieren eines VDAs auf einem nicht mehr unterstützten Windows-Betriebssystem finden Sie unter Ältere Betriebssysteme.

Hosts/Virtualisierungsressourcen

Die folgenden Host-/Virtualisierungsressourcen (alphabetisch aufgeführt) werden unterstützt. Wo zutreffend werden die folgenden *major.minor* Versionen unterstützt, einschließlich von Updates für diese Versionen. Der Knowledge Center-Artikel CTX131239 enthält aktuelle Versionsinformationen sowie Links zu bekannten Problemen.

Einige Features werden nicht auf allen Hostplattformen bzw. allen Plattformversionen 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.

- **Amazon Web Services (AWS)**
  - Sie können Anwendungen und Desktops auf unterstützten Windows-Betriebssystemen für einzelne oder mehrere Sitzungen (Einzel- oder Multisitzungs-OS) bereitstellen.
  - Citrix unterstützt Amazon Relational Database Service (RDS). Weitere Informationen finden Sie unter Citrix Ready Marketplace und Citrix und AWS.
- **Citrix Hypervisor (ehemals XenServer)**

  CTX131239 enthält aktuelle Versionshinweise sowie Links zu bekannten Problemen.

  Weitere Informationen finden Sie unter Citrix Hypervisor-Virtualisierungsumgebungen.
- **CloudPlatform** (veraltet)
- **Microsoft Azure Classic** (veraltet)

- **Microsoft Azure Resource Manager**

  Weitere Informationen finden in dem Artikel zu Microsoft Azure Resource Manager-Virtualisierungsumgebung

- **Microsoft 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.

- **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.

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

HDX

Audio

UDP-Audio für Multistream-ICA wird von der Citrix Workspace-App für Windows und der Citrix Workspace-App für Linux 13 unterstützt.

Die Echounterdrückung wird von der Citrix Workspace-App für Windows unterstützt.

Siehe Informationen zu Unterstützung und Anforderungen für HDX. Weitere Informationen zu HDX-Features und der Citrix Workspace-App finden Sie in der Featurematrix.

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 3D Pro

Der VDA für Windows-Einzelsitzungs-OS erkennt vorhandene GPU-Hardware zur Laufzeit.

Auf der physischen bzw. virtuellen Maschine, auf der die Anwendung gehostet wird, kann GPU-Passthrough oder Virtual GPU (vGPU) verwendet werden:

- GPU-Passthrough verfügbar mit: Citrix XenServer, Nutanix AHV, VMware vSphere und VMware ESX, dort wird es als vDGA (virtual Direct Graphics Acceleration) bezeichnet. GPU-Passthrough ist auch mit Microsoft Hyper-V in Windows Server 2016 verfügbar, wo es als diskrete Gerätezuweisung (DDA) bezeichnet wird.
- vGPU ist mit Citrix Hypervisor, Nutanix AHV und VMware vSphere verfügbar; siehe https://www.citrix.com/products/xenapp-xendesktop/hdx-3d-pro.html. HDX 3D Pro wird auch mit Cloud-Instanzen von Microsoft Azure NV und Amazon AWS EC2 G3 unterstützt.

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 und 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 Virtualization Solution).

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 eine maximale Auflösung 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.

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 2019
- Windows Server 2016
- Windows Server 2012 R2

Anforderungen:

- Microsoft Visual C++ 2017 Laufzeitbibliotheken (x86 und x64)
- Microsoft .NET Framework 4.7.1 (Mindestversion)

Für VDAs für Windows-Multisitzungs-OS 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

Es wird nur Citrix Lizenzserver 11.16 und höher unterstützt. Weitere Informationen finden Sie unter Lizenzierung.

Bei Verwendung von Citrix Provisioning (ehemals Provisioning Services) mit diesem Release gelten für Version 7.x der Lebenszyklus von XenApp 7.x/XenDesktop 7.x und der Lebenszyklus von Citrix Virtual Apps and Desktops. Weitere Informationen zur Versionskompatibilität finden Sie in der Produktmatrix.

Informationen zu unterstützten StoreFront-Versionen finden Sie unter StoreFront-Systemanforderungen.

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 Citrix Virtual Apps and Desktops-Kernkomponente installiert ist), muss auf der Maschine Visual Studio 2015 Runtime installiert sein. Informationen hierzu finden Sie in der Dokumentation von Microsoft.

Wenn Sie Domänen-Gruppenrichtlinienobjekte über die Gruppenrichtlinien-Verwaltungskonsole bearbeiten möchten, aktivieren Sie die Gruppenrichtlinienverwaltung im Windows Server-Manager auf allen Maschinen, die Delivery Controller enthalten.

Es werden mehrere Netzwerkkarten unterstützt.

Standardmäßig wird zusammen mit einem aktuellen VDA die Citrix Workspace-App für Windows installiert. Weitere Informationen finden Sie in der Dokumentation der Citrix Workspace-App für Windows.

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.

Gemischte DPI-Werte bei mehreren Monitoren: Die Verwendung unterschiedlicher DPI-Werte bei mehreren Monitoren wird in Citrix Virtual Apps and Desktops-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 Citrix Virtual Apps and Desktops ist nicht kompatibel mit AppDNA 7.8 und AppDNA 7.9. Citrix empfiehlt die Verwendung der aktuellen AppDNA-Version.

Technische Übersicht

June 27, 2024

Citrix Virtual Apps and Desktops ist eine Virtualisierungslösung, die IT die Steuerung von virtuellen Maschinen, Anwendungen, der Lizenzierung und Sicherheit ermöglicht und gleichzeitig Benutzern von überall Zugriff mit jedem Gerät bietet.

Citrix Virtual Apps and Desktops bietet folgende Möglichkeiten:

- 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.

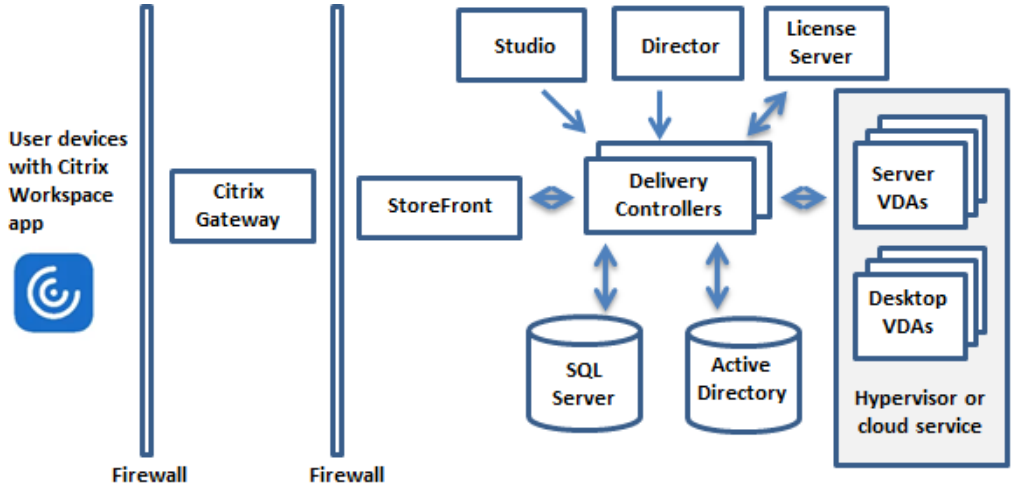
Citrix Virtual Apps and Desktops hat eine einheitliche Architektur: die FlexCast Management Architecture (FMA). Die Hauptfunktion von FMA umfasst die Ausführung mehrerer Versionen von Citrix Virtual Apps oder Citrix Virtual Desktops in einer Site und die Bereitstellung von integriertem Provisioning.

Informationen zu Änderungen an Produktnamen.

Hauptkomponenten

Dieser Artikel ist besonders für neue Anwender von Citrix Virtual Apps and Desktops geeignet. Wenn Sie eine XenApp-Farm bis Version 6.x oder eine XenDesktop-Site bis Version 5.6 haben, siehe auch Änderungen in Version 7.x.

Diese Abbildung unten zeigt die wichtigsten Komponenten in einer typischen Bereitstellung, die als “Site”bezeichnet wird.



Delivery Controller

Der Delivery Controller ist die zentrale Verwaltungskomponente einer 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 einen Hypervisor oder einen Clouddienst enthält, kommunizieren die Controller-Dienste mit diesem, um Anwendungen und Desktops zu verteilen, den Benutzerzugriff zu authentifizieren und zu verwalten, Verbindungen zwischen Benutzern und ihren 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 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 Maschine und Benutzergeräten. VDAs überprüfen außerdem, ob eine Citrix Lizenz für einen Benutzer bzw. eine Sitzung verfügbar ist, und wenden für die Sitzung konfigurierte 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-Einzelsitzungs-OS und für Windows-Multisitzungs-OS verfügbar. Mit VDAs für Windows-Multisitzungs-OS können mehrere Benutzer gleichzeitig eine Verbindung mit dem Server herstellen. Mit VDAs für Windows-Einzelsitzungs-OS kann jeweils nur ein Benutzer eine Verbindung zum Desktop herstellen. Linux VDAs sind ebenfalls verfügbar.

Citrix StoreFront

StoreFront authentifiziert Benutzer 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 Workspace-App

Die Citrix Workspace-App 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. Die Citrix Workspace-App bietet bedarfsgesteuerten Zugriff auf Windows-, Web- und SaaS-Anwendungen. Bei Geräten, auf denen die gerätespezifische Citrix Workspace-App-Software nicht installiert werden kann, ermöglicht die Citrix Workspace-App für HTML5 eine Verbindung über einen HTML5-kompatiblen Webbrowser.

Citrix Studio

Studio dient als Verwaltungskonsole zum Konfigurieren und Verwalten der Citrix Virtual Apps and Desktops-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 Citrix Virtual Apps- oder Citrix Virtual Desktops-Sites herstellen und diese überwachen.

In Director wird Folgendes angezeigt:

- Echtzeit-Sitzungsdaten vom Brokerdienst auf dem Controller, einschließlich Daten, die der Brokerdienst vom Brokeragent auf dem VDA erhält.
- Historische Daten der Site vom Überwachungsdienst auf dem Controller.

Director analysiert die vom Citrix Gateway-Gerät erfassten ICA-Leistungs- und Heuristikdaten und zeigt das Ergebnis für Administratoren an.

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. Eine Site muss über mindestens einen Lizenzserver zum Speichern und Verwalten von Lizenzdateien verfügen.

Hypervisor oder Clouddienst

Der Hypervisor oder Clouddienst hostet die virtuellen Maschinen der Site. Dies können virtuellen Maschinen sein, die Sie zum Hosten von Anwendungen und Desktops verwenden, und solche zum Hosten der Citrix Virtual Apps and Desktops-Komponenten. Ein Hypervisor wird auf einem Hostcomputer installiert, der nur zur Ausführung des Hypervisors und dem Hosten virtueller Maschinen bestimmt ist.

Citrix Virtual Apps and Desktops unterstützt diverse Hypervisors und Clouddienste.

Viele Bereitstellungen erfordern zwar einen Hypervisor, für die Bereitstellung von Remote-PC-Zugriff ist jedoch keiner erforderlich. Auch für die Bereitstellung von VMs mit Provisioning Services (PVS) ist kein Hypervisor erforderlich.

Weitere Informationen:

- Netzwerkports.
- Datenbanken.
- Windows-Dienste in Citrix Virtual Apps and Desktops-Komponenten: Konfigurieren von Benutzerrechten.
- Unterstützte Hypervisors und Clouddienste: Systemanforderungen.

Zusätzliche Komponenten

Citrix Virtual Apps and Desktops-Bereitstellungen können die folgenden, nicht in der Abbildung oben gezeigten zusätzlichen Komponenten enthalten. Weitere Informationen finden Sie in der Dokumentation dieser Komponenten.

Citrix Provisioning

Citrix Provisioning (zuvor "Provisioning Services") ist eine optionale Komponente, die in einigen Editionen verfügbar ist. Es bietet eine Alternative zu MCS für das Provisioning von virtuellen Maschinen. Während MCS Kopien eines Masterimages erstellt, streamt PVS das Masterimage zu den Benutzergeräten. PVS benötigt hierfür keinen Hypervisor, daher können Sie mit PVS physische Maschinen hosten. PVS kommuniziert mit dem Controller, um Benutzern Ressourcen bereitzustellen.

Citrix Gateway

Wenn Benutzer eine Verbindung von außerhalb der Unternehmensfirewall herstellen, können diese Verbindungen in Citrix Virtual Apps and Desktops mit Citrix Gateway (zuvor "Access Gateway"und "NetScaler Gateway") und TLS geschützt werden. Citrix Gateway bzw. das virtuelle VPX-Gerät ist ein SSL-VPN-Gerät, das in der DMZ bereitgestellt wird. Es bietet einen sicheren Einzelzugangspunkt durch die Unternehmensfirewall.

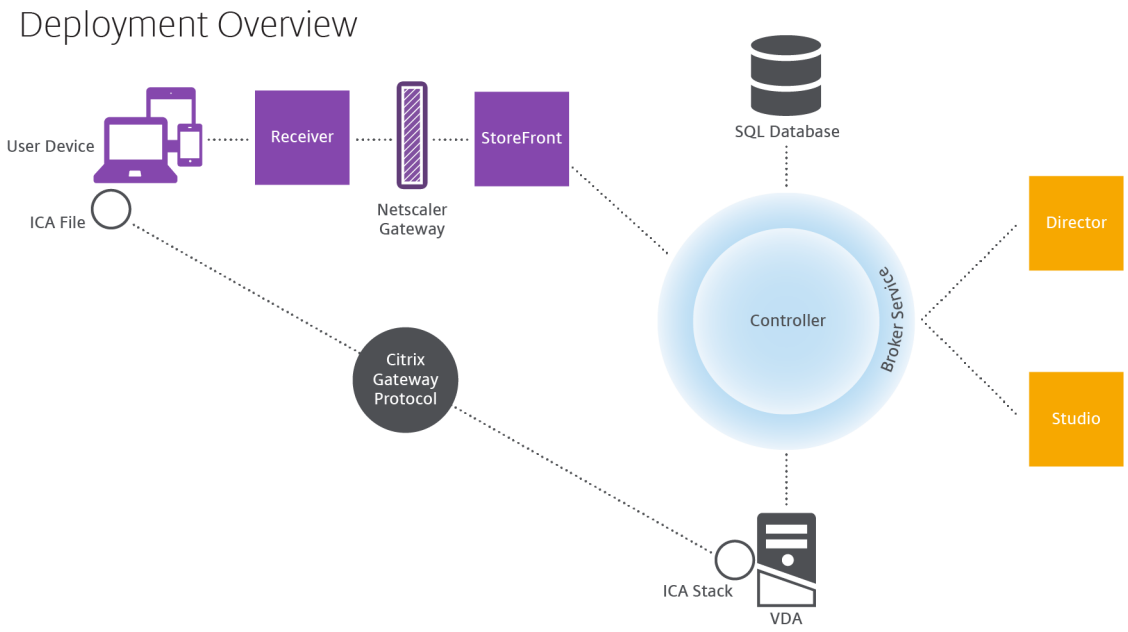
Citrix SD-WAN

Wenn Benutzern an Remotestandorten, wie in Zweigstellen, virtuelle Desktops bereitgestellt werden, kann mit Citrix SD-WAN die Leistung optimiert werden. Repeater erhöhen die Leistung in WANs. Mit Repeatern im Netzwerk erleben Benutzer in Zweigstellen eine LAN-ähnliche Leistung über das WAN.

Citrix SD-WAN kann bestimmten Teilen der Benutzererfahrung Priorität geben, damit sich beispielsweise die Benutzererfahrung in der Zweigstelle nicht verschlechtert, wenn eine große Datei oder ein großer Druckauftrag über das Netz gesendet wird. HDX WAN-Optimierung bietet Komprimierung mit Token sowie Datendeduplizierung, wodurch die Bandbreitenanforderungen drastisch 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.

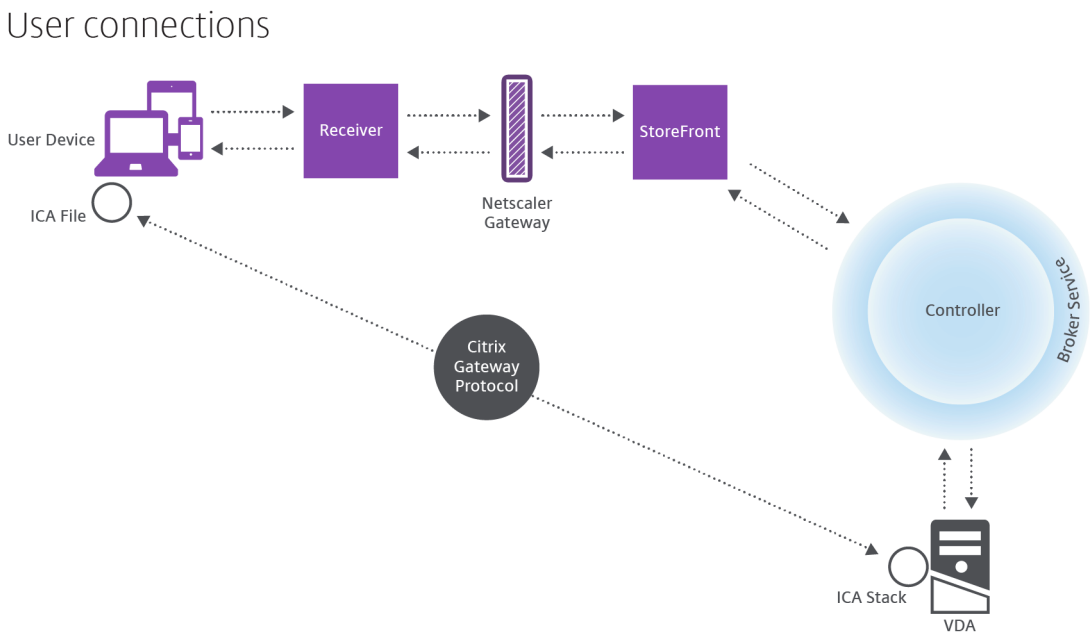
Benutzer greifen niemals direkt auf den Controller zu. Der VDA dient als Vermittler zwischen den Benutzern und dem Controller. Wenn sich Benutzer über StoreFront anmelden, werden ihre Anmeldeinformationen an den Brokerdienst auf dem Controller übermittelt. Der Brokerdienst ruft dann basierend auf den festgelegten Richtlinien Profile und verfügbare Ressourcen ab.

Behandlung von Benutzerverbindungen

Zum Starten einer Sitzung stellt der Benutzer eine Verbindung über die Citrix Workspace-App (auf dem Benutzergerät installiert) oder über eine StoreFront 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 der Citrix Workspace-App 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 Workspace-App-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 die Citrix Workspace-App zurück. Ein Satz erforderlicher Parameter wird in StoreFront gesammelt. Diese Parameter werden dann entweder als Teil der Protokollübermittlung zwischen der Citrix Workspace-App und StoreFront an die Citrix Workspace-App gesendet oder in eine ICA-Datei (Independent Computing Architecture) konvertiert und heruntergе-

laden. Wenn die Site ordnungsgemäß eingerichtet wurde, sind die Anmeldeinformationen während des gesamten Vorgangs verschlüsselt.

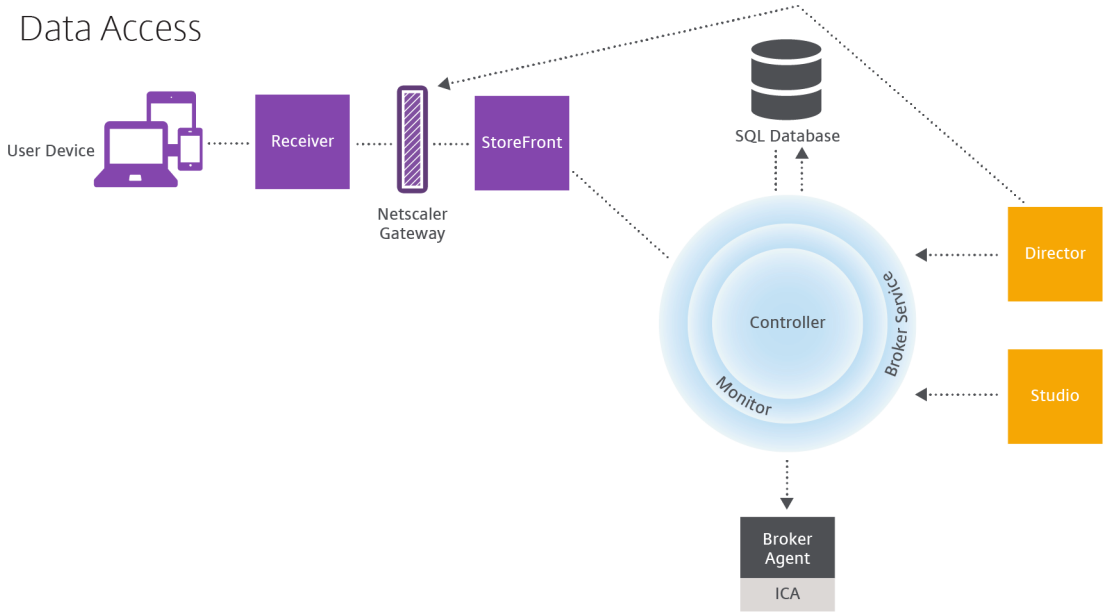
Die ICA-Datei wird auf das Benutzergerät kopiert und richtet eine direkte Verbindung zwischen dem Gerät und dem auf dem VDA ausgeführten ICA-Stack ein. Diese Verbindung umgeht die Verwaltungsinfrastruktur (Citrix Workspace-App, StoreFront und Controller).

Die Verbindung zwischen der Citrix Workspace-App 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 dann an die Standortdatenbank und beginnt mit der Protokollierung der Daten in der Überwachungsdatenbank.

Wie funktioniert der Datenzugriff

Jede Citrix Virtual Apps and Desktops-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 Daten 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 Citrix Gateway zugreifen und Informationen zu HDX-Daten abrufen.

Desktops und Anwendungen bereitstellen

Zur Einrichtung der Maschinen für die Bereitstellung von Anwendungen und Desktops verwenden Sie Maschinenkataloge. Anschließend erstellen Sie unter Verwendung der Maschinen in den Maschinenkatalogen Bereitstellungsgruppen, um festzulegen, welche Anwendungen und Desktops bereitgestellt werden sollen und welche Benutzer darauf zugreifen können. Optional können Sie dann Anwendungsgruppen erstellen, um Anwendungssammlungen zu verwalten.

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 (Citrix Provisioning 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:

- **Multisitzungs-OS:** Virtuelle oder physische Maschinen mit einem Betriebssystem für mehrere Sitzungen. Sie werden verwendet, um mit Citrix Virtual Apps veröffentlichte Anwendungen (serverbasierte, gehostete Anwendungen) und veröffentlichte Desktops (servergehostete Desktops) bereitstellen. Mehrere Benutzer können gleichzeitig eine Verbindung mit diesen Maschinen herstellen.
- **Einzelsitzungs-OS:** Virtuelle oder physische Maschinen mit einem Betriebssystem für eine Sitzung. Sie werden für die Bereitstellung von VDI-Desktops (personalisierbare Desktops mit

Einzelsitzungs-OS), von über VM gehosteten Anwendungen (Anwendungen von Einzelsitzungs-OS) und gehosteter physischer Desktops verwendet. Nur jeweils ein Benutzer kann eine Verbindung mit einem dieser Desktops herstellen.

- **Remote-PC-Zugriff:** ermöglicht Remotebenutzern den Zugriff auf ihre Büro-PCs über ein beliebiges Gerät mit der Citrix Workspace-App. Die Büro-PCs werden über die Citrix Virtual Desktops-Bereitstellung verwaltet und erfordern eine Positivliste mit Benutzergeräten.

Weitere Informationen finden Sie unter Citrix Virtual Apps and Desktops Image Management und 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.

Weitere Informationen

Diagramme für Citrix Virtual Apps and Desktops

Active Directory

November 2, 2022

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.

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 Controller 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.

> **Hinweis:**
>
> 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 oder bedingte 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. 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.

Konfigurieren Sie auf dem VDA Folgendes:
`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\SupportMultipleForest`

- Name: `SupportMultipleForest`

- Typ: REG_DWORD
- Wert: 0x00000001 (1)

Konfigurieren Sie auf allen Delivery Controllern Folgendes: HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer\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:

Suchen Sie für den VDA den Registrierungsschlüssel HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs

- Name: ListOfSIDs
- Typ: REG_SZ
- Daten: Sicherheits-ID (SID) der Controller (SIDs werden im Ergebnis des Cmdlets Get-BrokerController angezeigt.)

Wenn externe Vertrauensstellungen vorhanden sind, nehmen Sie die folgende Änderung auf dem VDA vor:

1. Suchen Sie die Datei Program Files\Citrix\Virtual Desktop Agent\brokeragent.exe.config.
2. Erstellen Sie ein Backup der Datei.
3. Öffnen Sie die Datei in einem Textbearbeitungsprogramm, z. B. Editor.
4. Suchen Sie 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
Extern	Nicht transitiv	Unidirektional oder bidirektional	Ja
Gesamtstruktur	Transitiv	Unidirektional oder bidirektional	Ja
Tastenkombination	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.

Datenbank

November 14, 2022

Citrix Virtual Apps- bzw. Citrix Virtual Desktops-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.

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 stets in der primären Zone enthalten sein. 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 VDA 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 dem seltenen Fall, dass die Kommunikation mit allen Controllern fehlschlägt. Es ist keine Alternative zu anderen Hochverfügbarkeitslösungen. Weitere Informationen finden Sie unter CTX 127564.

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 der Instanz 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 des Überwachungsdiensts 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). (Siehe Für die Einrichtung von Datenbanken erforderliche Berechtigungen.)

Sie können den Speicherort der Datenbank 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 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.
- Konfigurierte Features für hohe Verfügbarkeit (bei Bedarf).
- 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*	
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.

Skripts für bevorzugte Datenbankrechte

In Unternehmensumgebungen umfasst die Datenbankeinrichtung Skripts, die von verschiedenen Teams mit unterschiedlichen Rollen (Rechten) verwendet werden müssen: `securityadmin` oder `db_owner`.

Mit PowerShell können Sie nun die bevorzugten Datenbankrechte festlegen. (Das Feature ist in Studio nicht verfügbar, dort wird nur ein einzelnes Skript für alle Aufgaben unterstützt.)

Wenn Sie einen nicht standardmäßigen Wert angeben, werden separate Skripts erstellt. Ein Skript enthält Aufgaben, die die `securityadmin`-Rolle benötigen. Das andere Skript erfordert nur `db_owner`-Rechte und kann von einem Citrix Administrator ausgeführt werden, ohne einen Datenbankadministrator kontaktieren zu müssen.

In den `get-*DBSchema`-Cmdlets hat die Option `-DatabaseRights` die folgenden gültigen Werte:

- `SA`: Generiert ein Skript, das die Datenbanken und die Delivery Controller-Anmeldung erstellt. Diese Aufgaben erfordern `securityadmin`-Rechte.
- `DBO`: Generiert ein Skript, das die Benutzerrollen in der Datenbank erstellt, die Anmeldungen hinzufügt und dann die Datenbankschemas erstellt. Diese Aufgaben erfordern `db_owner`-Rechte.
- `Mixed`: (Standard) Alle Aufgaben in einem Skript, unabhängig von den erforderlichen Rechten.

Weitere Informationen finden Sie in der Hilfe zum Cmdlet.

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

- Datenbank-Dimensionierungstool:
- Dimensionierung der Sitedatenbank und Konfiguration von Verbindungszeichenfolgen bei Verwendung von SQL Server-Lösungen für hohe Verfügbarkeit.

Bereitstellungsmethoden

March 15, 2022

Citrix Virtual Apps and Desktops bietet verschiedene Bereitstellungsmethoden. Eine einzige Bereitstellungsmethode wird wahrscheinlich nicht alle Anforderungen erfüllen.

Einführung

Die Auswahl der geeigneten Methode zur Anwendungsbereitstellung verbessert Skalierbarkeit, Verwaltung und Benutzererfahrung.

- **Installierte Apps:** Solche Apps sind Teil des grundlegenden Desktopimages. Bei der Installation werden DLL-, EXE- und andere Dateien auf das Image-Laufwerk kopiert und Registrierungsänderungen vorgenommen. Weitere Informationen finden Sie unter Erstellen von Maschinenkatalogen.
- **Gestreamte Apps (Microsoft App-V):** Nach dem Erstellen eines Profils werden die Apps bei Bedarf auf den Desktops im Netzwerk bereitgestellt. App-Dateien und Registrierungseinstellungen werden in einem Container auf dem virtuellen Desktop abgelegt und vom Basisbetriebssystem sowie untereinander isoliert. Diese Isolation erleichtert das Beheben von Kompatibilitätsproblemen. Einzelheiten finden Sie unter App-V.
- **Layer-Apps (Citrix App Layering)**: Jeder Layer enthält eine App, einen Agent oder ein Betriebssystem. Durch die Integration eines Betriebssystemlayers, eines Plattformlayers (VDA, Citrix Provisioning Services-Agent) und vieler App-Layer kann ein Administrator problemlos neue, implementierbare Images erstellen. App Layering vereinfacht die Systempflege, da ein Betriebssystem, ein Agent und eine App auf einem einzelnen Layer ist. Wenn Sie den Layer aktualisieren, werden alle bereitgestellten Images aktualisiert, die diesen Layer enthalten. Einzelheiten finden Sie unter Citrix App Layering.
- **Gehostete Windows-App:** Eine Anwendung, die auf einem Citrix Virtual Apps-Host mit mehreren Benutzern installiert ist und als Anwendung und nicht als Desktop bereitgestellt wird. Benutzer greifen nahtlos über den VDI-Desktop oder das Endpunktgerät auf gehostete Windows-Apps zu, ohne dass sie bemerken, dass die App remote ausgeführt wird. Weitere Informationen finden Sie unter Erstellen von Bereitstellungsgruppen.
- **Lokale Apps:** auf dem Endpunktgerät bereitgestellte Apps. Die App-Schnittstelle wird in der gehosteten VDI-Sitzung des Benutzers angezeigt, obwohl die App auf dem Endpunkt ausgeführt wird. Einzelheiten finden Sie unter Lokaler App-Zugriff und URL-Umleitung.
- **Remote-PC-Zugriff:** Remote-PC-Zugriff ermöglicht Mitarbeitern den Remotezugriff auf ihre physischen PCs im Büro. Auf ihren Büro-PCs erhalten Benutzer Zugriff auf alle Apps, Daten und Ressourcen, die sie für ihre Arbeit benötigen. Mit Remote-PC-Zugriff ist das Einführen und Bere-

itstellen anderer Tools für die Telearbeit überflüssig. Einzelheiten finden Sie unter Remote-PC-Zugriff.

Als Desktops sollten Sie veröffentlichte Desktops oder VDI-Desktops verwenden.

In Citrix Virtual Apps veröffentlichte Apps und Desktops

Verwenden Sie Multisitzungs-OS-Maschinen zum Bereitstellen von mit Citrix Virtual Apps and Desktops veröffentlichten Apps und Desktops.

Anwendungsfall:

- Gewünscht wird eine kostengünstige, serverbasierte Bereitstellung, um die Kosten für die Bereitstellung von Anwendungen für zahlreiche Benutzer 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. Dies sorgt für eine konsistente, sichere und zuverlässige Benutzererfahrung.
- 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 Multisitzungs-OS-Maschine gespeichert.

- Maschinen werden über Maschinenkataloge verfügbar gemacht.
- Maschinen aus Maschinenkatalogen sind in Bereitstellungsgruppen organisiert, die Benutzergruppen dieselben Anwendungen bereitstellen.
- Multisitzungs-OS-Maschinen unterstützen Bereitstellungsgruppen, die Desktops, Anwendungen oder beides hosten.

Sitzungsverwaltung und -zuweisung:

- Auf Multisitzungs-OS-Maschinen werden mehrere Sitzungen auf einer einzelnen Maschine 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.

VM-gehostete Apps

Bereitstellen VM-gehosteter Anwendungen über Einzelsitzungs-OS-Maschinen

Anwendungsfall:

- Gewünscht wird eine clientbasierte Anwendungsbereitstellungslösung, die eine sichere, zentrale Verwaltung bietet und zahlreiche Benutzer pro Hostserver unterstützt. Benutzern sollen Anwendungen bereitstellt werden, die in High Definition im Seamlessmodus 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. Dies ermöglicht eine kosteneffektivere Anwendungsbereitstellung.
- 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 Maschinen mit Windows-Einzelsitzungs-OS 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 Benutzerdaten möglicherweise erhöht.

Benutzererfahrung:

- Die gleiche nahtlose Anwendungserfahrung wie mit gehosteten, freigegebenen Anwendungen auf Maschinen mit Windows-Multisitzungs-OS.

Verarbeiten, Hosten und Bereitstellen von Anwendungen:

- Wie bei Maschinen mit Windows-Multisitzungs-OS, außer dass es sich um virtuelle Maschinen mit Windows-Einzelsitzungs-OS handelt.

Sitzungsverwaltung und -zuweisung:

- Maschinen mit Windows-Einzelsitzungs-OS 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.

VDI-Desktops

Verwenden Sie Einzelsitzungs-OS-Maschinen zum Bereitstellen von VDI-Desktops mit Citrix Virtual Apps and Desktops.

VDI-Desktops werden auf virtuellen Maschinen gehostet und bieten jedem Benutzer ein Desktopbetriebssystem.

VDI-Desktops benötigen mehr Ressourcen als veröffentlichte Desktops, aber die auf ihnen installierten Anwendungen müssen keine serverbasierten Betriebssysteme unterstützen. Abhängig vom ausgewählten Typ des VDI-Desktops können Desktops außerdem einzelnen Benutzern zugewiesen werden. Dadurch können sie von Benutzern in hohem Maße personalisiert werden.

Beim Erstellen eines Maschinenkatalogs für VDI-Desktops erstellen Sie einen der folgenden Desktoptypen:

- **Zufälliger, nicht beständiger Desktop (gepoolter VDI-Desktop):** Jedes Mal, wenn sich ein Benutzer bei einem dieser Desktops anmeldet, wird ein Desktop aus einem Pool ausgewählt. Der Pool basiert auf einem einzelnen Masterimage. Alle Änderungen an dem Desktop gehen verloren, wenn die Maschine neu gestartet wird.
- **Statischer, nicht beständiger Desktop:** Während der ersten Anmeldung wird einem Benutzer ein Desktop aus einem Pool zugewiesen. (Jede Maschine im Pool basiert auf einem einzelnen Masterimage.) Anschließend wird dem Benutzer bei jeder weiteren Anmeldung derselbe Desktop zugewiesen. Alle Änderungen an dem Desktop gehen verloren, wenn die Maschine neu gestartet wird.
- **Statischer, permanenter Desktop:** Im Gegensatz zu anderen VDI-Desktoptypen können diese Desktops vollständig personalisiert werden. Während der ersten Anmeldung wird einem Benutzer ein Desktop aus einem Pool zugewiesen. Bei nachfolgenden Anmeldungen wird dem Benutzer derselbe Desktop wie beim ersten Mal zugewiesen. Alle Änderungen an dem Desktop bleiben erhalten, wenn die Maschine neu gestartet wird.

Netzwerkports

September 21, 2021

In den folgenden Tabellen sind die Standardnetzwerkports aufgeführt, die von 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 CTX101810.

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 Citrix Provisioning (zuvor "Provisioning Services"), finden Sie im aktuellen Artikel "Systemanforderungen"zu der jeweiligen Komponente.

In den Tabellen werden 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. Details zu diesen Zuweisungen finden Sie unter http://www.iana.org/assignments/port-numbers. Die Beschreibungen der IANA spiegeln jedoch nicht immer die heutige Verwendung wider.

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	Notizen
VDA	ICA/HDX	TCP, UDP	1494	EDT erfordert 1494 für UDP. Siehe Einstellungen der Richtlinie "ICA".

Komponente	Verwendung	Protokoll	Standardport, eingehend	Notizen
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 Workspace-App-Versionen
VDA	ICA/HDX über WebSocket	TCP	8008	Nur Citrix Workspace-App für HTML5 und Citrix Workspace-App 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	Notizen
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.

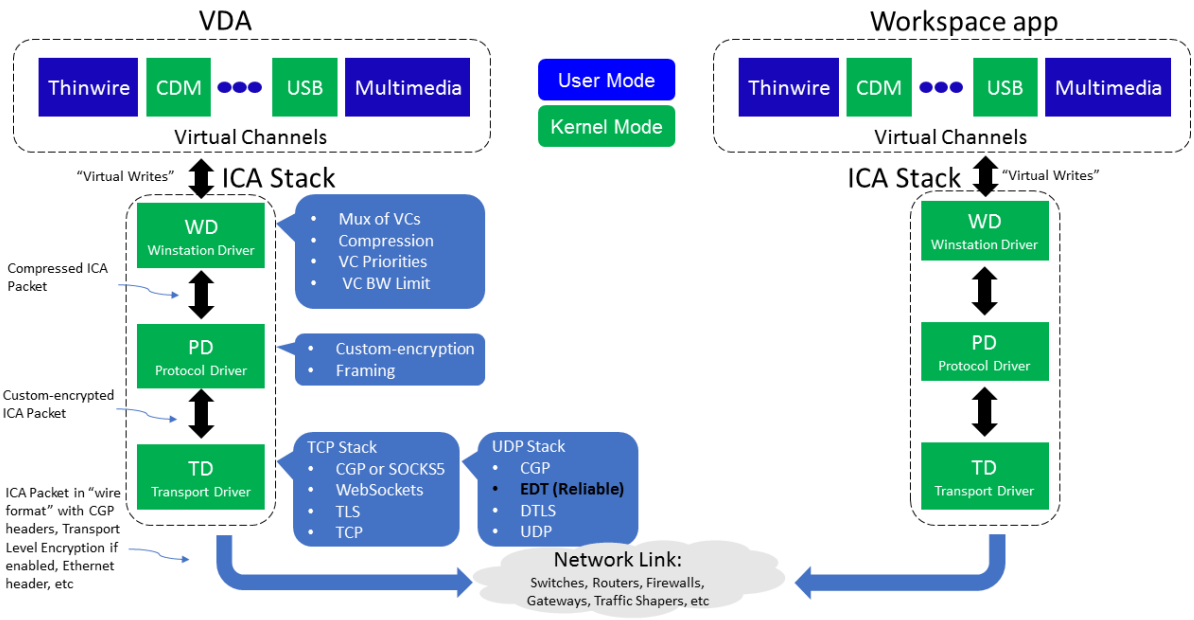
Komponente	Verwendung	Protokoll	Standardport, eingehend
Lizenzserver	Lizenzserver	TCP	27000
Lizenzserver	Lizenzserver für Citrix (Vendor Daemon)	TCP	7279
Lizenzserver	License Administration Console	TCP	8082
Lizenzserver	Web Services for Licensing	TCP	8083

HDX

April 19, 2024

> **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 bietet Benutzern zentralisierter Anwendungen und Desktops auf jedem Gerät und in jedem Netzwerk vielfältige Technologien für ein High Definition-Erlebnis.

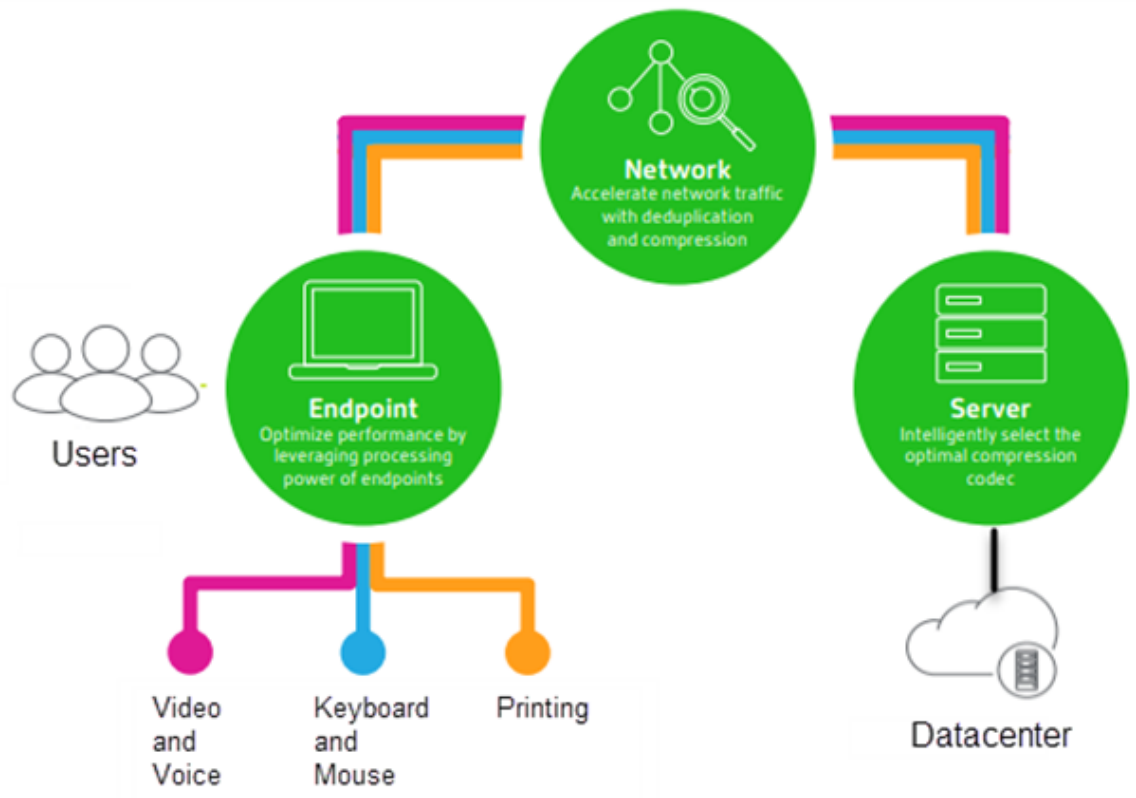


HDX basiert auf drei technischen Prinzipien:

- Intelligente Umleitung
- Adaptive Komprimierung
- Datendeduplizierung

Unter Anwendung in variablen Kombinationen optimieren sie die IT- und Benutzererfahrung, verringern den Bandbreitenverbrauch und erhöhen die Benutzerdichte pro Hostingserver.

- **Intelligente Umleitung:** Hierbei werden Bildschirmaktivität, Anwendungsbefehle, Endpunktgerät und Netzwerk-/Servermerkmale geprüft, um direkt zu bestimmen, wie und wo eine Anwendungs- oder Desktopaktivität gerendert werden soll. Das Rendering kann auf dem Endpunktgerät oder dem Hostingserver erfolgen.
- **Adaptive Komprimierung:** Durch die adaptive Komprimierung kann reichhaltiges Multimedia über schmale Netzwerkverbindungen bereitgestellt werden. HDX wertet zunächst mehrere Variablen aus, z. B. Art der Eingabe, Gerät und Anzeige (Text, Video, Sprache und Multimedia). Es wählt dann den optimalen Komprimierungs-Codec und das besten Verhältnis an CPU- und GPU-Nutzung aus. Es passt sich dann intelligent gemäß dem individuellen Benutzer und der Basis an. Die intelligente Anpassung erfolgt auf Benutzer- oder sogar Sitzungsbasis.



- **Datendeduplizierung:** Die Deduplizierung des Netzwerkverkehrs verringert die zwischen Client und Server gesendeten aggregierten Daten. Hierbei werden wiederholte Muster häufig verwendeter Daten (Bitmaps, Dokumente, Druckaufträge, gestreamte Medien usw.) genutzt. Durch die Zwischenspeicherung der Muster müssen nur die Änderungen über das Netzwerk übertragen werden und die doppelte Übertragung von Daten wird vermieden. HDX unterstützt auch das Multicasting von gestreamtem Multimedia, wenn eine Übertragung von der Quelle von mehreren Teilnehmern an einem Ort angezeigt wird (anstelle einer 1:1-Verbindung für jeden Benutzer).

Weitere Informationen finden Sie unter Boost productivity with a high-definition user workspace.

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 eingesetzt 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.

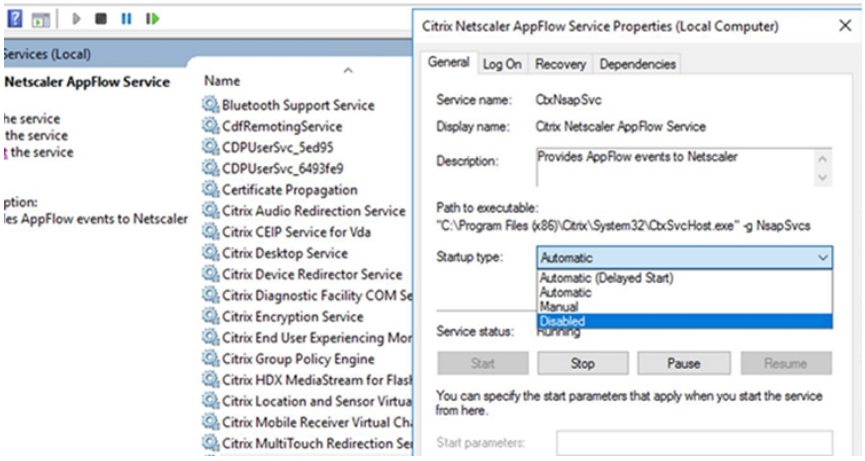
Sie können NetScaler zur Verwendung des virtuellen HDX Insight-Kanals aktivieren, um alle erforderlichen Datenpunkte unkomprimiert zu verschieben. Wenn Sie das Feature deaktivieren, entschlüsselt und dekomprimiert das NetScaler-Gerät den ICA-Datenverkehr über verschiedene virtuelle Kanäle hinweg. Die Verwendung des einzelnen virtuellen Kanals verringert die Komplexität, verbessert die Skalierbarkeit und ist kosteneffektiver.

Mindestanforderungen:

- Citrix Virtual Apps and Desktops 7 v1808
- XenApp und XenDesktop 7.17
- NetScaler Version 12.0 Build 57.x
- Citrix Workspace-App für Windows 1808
- Citrix Receiver für Windows 4.10
- Citrix Workspace-App für Mac 1808
- Citrix Receiver für Mac 12.8

Aktivieren oder Deaktivieren des virtuellen HDX Insight-Kanals

Um dieses Feature zu deaktivieren, deaktivieren Sie den Dienst “Citrix NetScaler Application Flow” . Legen Sie den Dienst zum Aktivieren auf “Automatisch”fest. In beiden Fällen wird empfohlen, die Servermaschine nach dem Ändern der Eigenschaft neu zu starten. Der Dienst ist standardmäßig aktiviert (automatisch).



Erleben von HDX-Funktionen mit Ihrem virtuellen Desktop

- Wenn Sie sehen möchten, wie die Browserinhaltsumleitung, eine von vier HDX-Multimediaumleitungstechno die Bereitstellung von HTML5- und WebRTC-Multimediainhalt beschleunigt:

  1. Laden Sie die Chrome-Browsererweiterung herunter und installieren Sie sie auf dem virtuellen Desktop.
  2. Um zu sehen, wie die Browserinhaltsumleitung die Bereitstellung von Multimediainhalten auf virtuellen Desktops beschleunigt, rufen Sie auf dem Desktop ein Video von einer Website mit HTML5-Videos auf (z. B. YouTube). Die Benutzer wissen nicht, wann die Browserinhaltsumleitung ausgeführt wird. Um zu sehen, ob die Browserinhaltsumleitung verwendet wird, ziehen Sie das Browserfenster schnell über den Bildschirm. Zwischen dem Viewport und Benutzeroberfläche macht sich eine Verzögerung bemerkbar. Sie können auch mit der rechten Maustaste auf die Webseite klicken und im Menü den Eintrag **Info über HDX-Browserumleitung** suchen.

- Um zu sehen, wie HDX HD-Audio bereitstellt führen Sie folgende Schritte aus:

  1. Konfigurieren Sie den Citrix Client für maximale Audioqualität; weitere Informationen hierzu finden Sie in der Citrix Workspace-App-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. http://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 Maschinen mit Windows-Multisitzungs-OS, Maschinen mit Windows-Einzelsitzungs-OS und Desktops mit Remote-PC-Zugriff zur Verfügung.
- Nachfolgend wird beschrieben, wie Sie die Benutzererfahrung optimieren, die Skalierbarkeit verbessern und 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.

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-Deckkraft 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.

Adaptiver HDX-Durchsatz

Der adaptive HDX-Durchsatz passt den Spitzendurchsatz einer ICA-Sitzung über die Ausgabepuffer intelligent an. Die Anzahl der Ausgabepuffer ist anfangs auf einen hohen Wert eingestellt. Der hohe Wert ermöglicht es insbesondere in Netzwerken mit hoher Latenz, Daten schneller und effizienter an den Client zu übertragen. Die bessere Interaktivität, schnellere Dateiübertragungen, flüssigere Videowiedergabe sowie höhere Framerate und Auflösung sorgen für eine bessere Benutzererfahrung.

Die Sitzungsinteraktivität wird ständig gemessen, um festzustellen, ob Datenströme innerhalb der ICA-Sitzung die Interaktivität beeinträchtigen. Ist dies der Fall, wird der Durchsatz verringert, um die Beeinträchtigungen durch den großen Datenstrom zu verringern und die Interaktivität wiederherzustellen.

> **Wichtig:**
>
> Der adaptive HDX-Durchsatz ändert die Einstellmethode der Ausgabepuffer, durch Übertragung des Mechanismus vom Client auf den VDA. Eine manuelle Konfiguration ist nicht erforderlich.

Dieses Feature erfordert Folgendes:

- VDA-Version 1811 oder höher
- Workspace-App für Windows 1811 oder höher

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 Citrix Virtual Apps and Desktops 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 Workspace-App-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 Hardware-verschlüsselungsfähigen Webcams verwendet HDX-Videokomprimierung die Hardware-Codierung 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 und zwei UDP-Streams sind zum Übertragen von ICA-Daten zwischen dem Benutzergerät und dem Server verfügbar.

- TCP-Streams: real time, interactive, background und bulk
- UDP-Streams: Voice und Framehawk-Display-Remoting

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 wird nur unterstützt, wenn mehrere Sitzungszuverlässigkeitsports oder CGP-Ports konfiguriert sind.

> **Warnung:**
>
> 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 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.

Ein- und Ausblenden der Remotesprachenleiste

Remotesprachenleiste ein- und ausblenden: Auf der Sprachenleiste wird die bevorzugte Eingabesprache von Anwendungssitzungen angezeigt. Wenn das Feature aktiviert ist (= Standardeinstellung), können Sie die Sprachenleiste in der Citrix Workspace-App für Windows über **Erweiterte Einstellungen > Sprachenleiste** ein- und ausblenden. Über eine Registrierungseinstellung auf dem VDA können Sie die Steuerung der Sprachenleiste auf dem Client deaktivieren. Wenn das Feature deaktiviert ist, wird die Client-UI-Einstellung nicht wirksam und der Status der Sprachenleiste wird über die für den Benutzer geltende Einstellung bestimmt. Weitere Informationen finden Sie unter Verbessern der Benutzererfahrung.

Deaktivieren der Clientsteuerung der Sprachenleiste über den VDA

1. Navigieren Sie im Registrierungseditor zu HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix
2. Erstellen Sie den DWORD-Wertschlüssel "SeamlessFlags"und legen Sie ihn auf "0x40000"fest.

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.

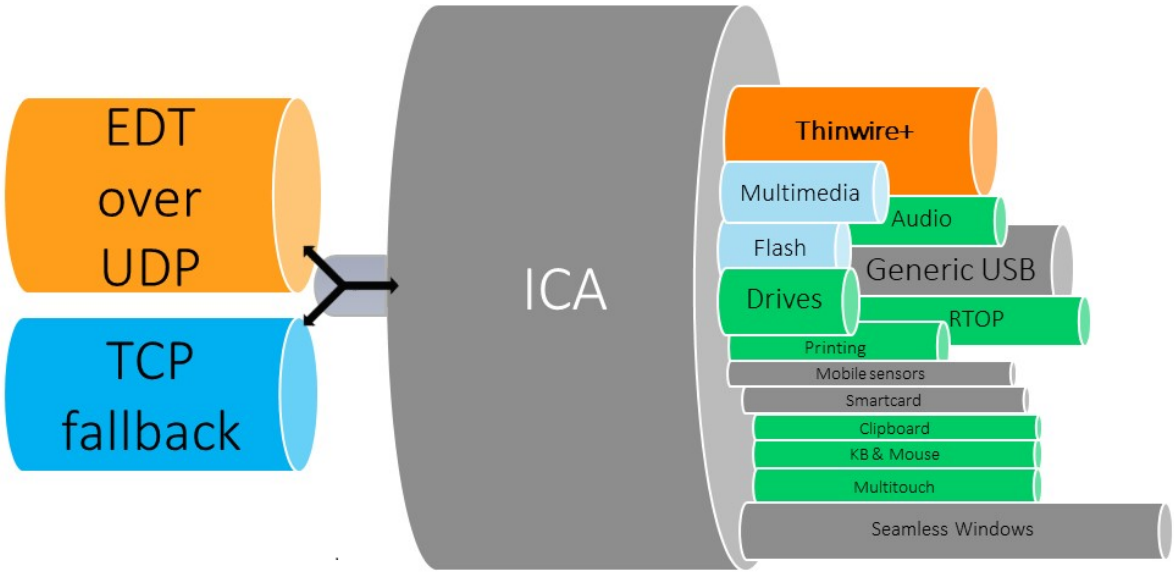
Adaptiver Transport

March 4, 2024

Adaptiver Transport ist ein Verfahren in Citrix Virtual Apps and Desktops, das die Möglichkeit bietet, Enlightened Data Transport (EDT) als Transportprotokoll für ICA-Verbindungen zu verwenden. Wenn EDT nicht verfügbar ist, wechselt der adaptive Transport zu TCP.

EDT ist ein Citrix-eigenes Transportprotokoll, das auf UDP (User Datagram Protocol) basiert. Es liefert eine überlegene Benutzererfahrung bei schwierigen Langstreckenverbindungen, ohne Abstriche bei

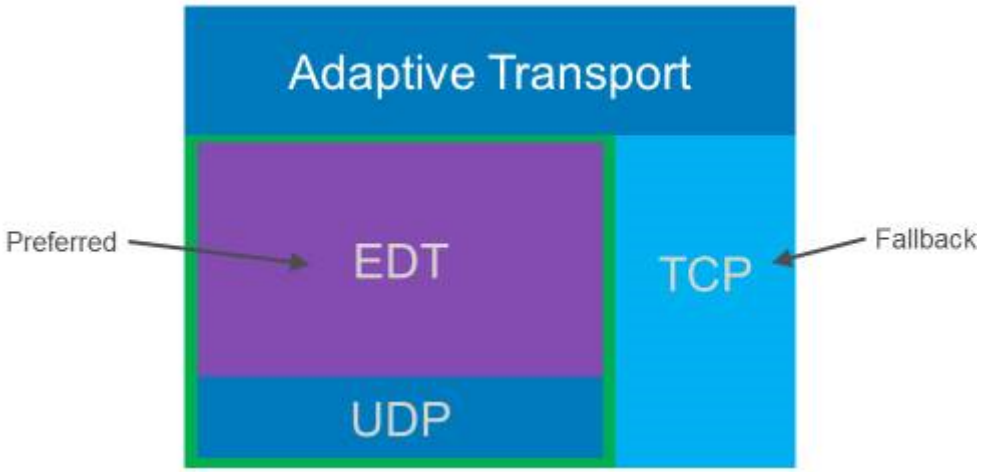
der Serverskalierbarkeit. EDT verbessert den Datendurchsatz für alle virtuellen ICA-Kanäle in instabilen Netzwerken und bietet so einen verlässlicheren Service.



Wenn der adaptive Transport auf **Bevorzugt** festgelegt ist, wird EDT als primäres Transportprotokoll und TCP als Fallback verwendet. Die Standardeinstellung für den adaptiven Transport ist **Bevorzugt**. Zu Testzwecken können Sie für den adaptiven Transport auch den **Diagnosemodus** wählen, der nur EDT zulässt und den Fallback auf TCP deaktiviert.

Bei Verwendung der Citrix Workspace-App für Windows, Mac und iOS werden EDT- und TCP-Verbindungen parallel bei der ersten Verbindung, bei einer Wiederverbindung mit Sitzungszuverlässigkeit und beim automatischen Wiederverbinden von Clients versucht. Dies verkürzt die Verbindungszeit, falls der zugrunde liegende UDP-Transport nicht verfügbar ist und stattdessen TCP verwendet werden muss. Wenn der adaptive Transport auf **Bevorzugt** festgelegt ist und die Verbindung über TCP hergestellt wird, versucht der adaptive Transport weiterhin alle fünf Minuten, zu EDT zu wechseln.

Bei Verwendung der Citrix Workspace-App für Linux und Android werden zuerst EDT-Verbindungen versucht. Wenn dieser Verbindungsaufbau fehlschlägt, versucht die Citrix Workspace-App nach dem Timeout der EDT-Anforderung, eine Verbindung über TCP herzustellen.



Systemanforderungen

Dies sind die Anforderungen für den Einsatz von adaptivem Transport und EDT:

- Steuerungsebene
  - Citrix Virtual Apps and Desktops Service
  - Citrix Virtual Apps and Desktops 1912 oder höher
- Virtual Delivery Agent
  - Version 1912 oder höher (2103 oder höher empfohlen)
  - Version 2012 ist die erforderliche Mindestversion für die Verwendung von EDT mit Citrix Gateway Service
- StoreFront
  - Version 3.12.x
  - Version 1912.0.x
- Citrix Workspace-App
  - Windows: Version 1912 oder höher (2105 oder höher empfohlen)
  - Linux: Version 1912 oder höher (2104 oder höher empfohlen)
  - Mac: Version 1912 oder höher (2108 oder höher empfohlen)
  - iOS: aktuell verfügbare Version im Apple App Store
  - Android: aktuell verfügbare Version in Google Play
- Citrix Gateway (ADC)
  - 13.0.52.24 oder höher
  - 12.1.56.22 oder höher

- Firewall (aus VDA-Perspektive)
  - UDP 1494 eingehend —bei deaktivierter Sitzungszuverlässigkeit
  - UDP 2598 eingehend —bei aktivierter Sitzungszuverlässigkeit
  - UDP 443 eingehend —bei aktiviertem VDA-SSL für die ICA-Verschlüsselung (DTLS)
  - UDP 443 ausgehend —bei Verwendung des Citrix Gateway Service. Weitere Informationen finden Sie in der Dokumentation zu Citrix Gateway Service.

Überlegungen

- Aktivieren Sie die Sitzungszuverlässigkeit, um die MTU-Discovery durch EDT sowie EDT mit Citrix Gateway und Citrix Gateway Service zu verwenden.
- Stellen Sie sicher, dass die EDT-MTU angemessen eingestellt ist, um eine Fragmentierung zu vermeiden. Andernfalls wird in einigen Fällen die Leistung beeinträchtigt oder Sitzungen können nicht gestartet werden. Weitere Informationen finden Sie unter MTU-Discovery durch EDT.
- Detaillierte Informationen zu Anforderungen und Überlegungen, die beim Einsatz von EDT mit dem Citrix Gateway Service zu berücksichtigen sind, finden Sie unter Unterstützung des adaptiven HDX-Transports mit EDT für Citrix Gateway Service.
- Einzelheiten zur Konfiguration von Citrix Gateway für EDT finden Sie unter Konfigurieren von Citrix Gateway zur Unterstützung von Enlightened Data Transport und HDX Insight.
- IPv6 wird derzeit nicht unterstützt.

Konfiguration

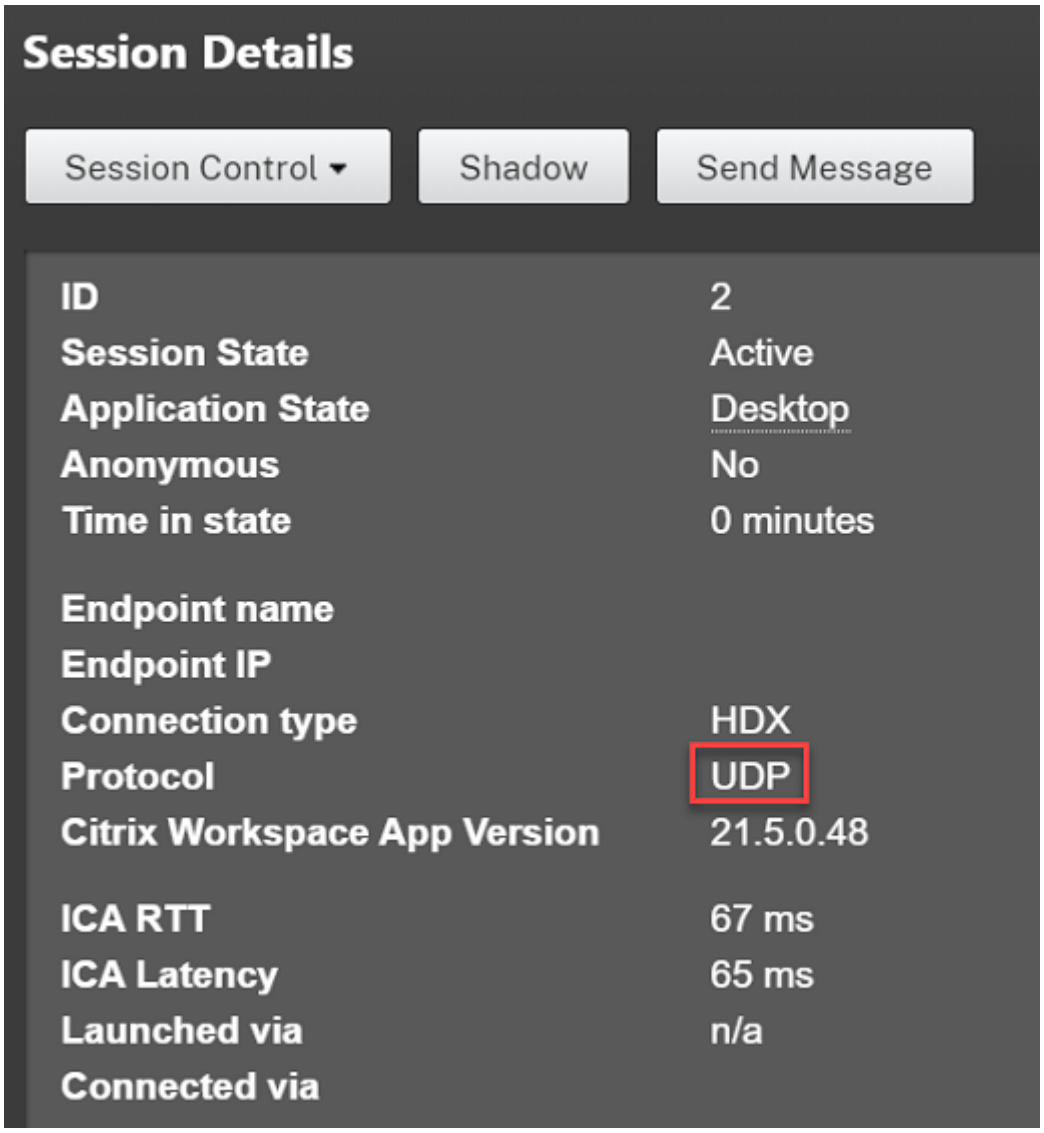
Der adaptive Transport ist standardmäßig aktiviert. Sie können die folgenden Optionen mit der Einstellung **Adaptiver HDX-Transport** in der Citrix-Richtlinie konfigurieren.

- **Bevorzugt**. Dies ist die Standardeinstellung. Der adaptive Transport ist aktiviert und verwendet EDT als bevorzugtes Transportprotokoll sowie TCP als Fallback.
- **Diagnosemodus:** Der adaptive Transport ist aktiviert und erzwingt den Einsatz von EDT. Der Fallback auf TCP ist deaktiviert. Diese Einstellung wird nur zum Testen und zur Fehlerbehebung empfohlen.
- **Aus**. Der adaptive Transport ist deaktiviert, und es wird nur TCP für den Transport verwendet.

Mit Director oder dem Befehlszeilenprogramm CtxSession.exe auf dem VDA können Sie bestätigen, dass EDT als Transportprotokoll für die Sitzung verwendet wird.

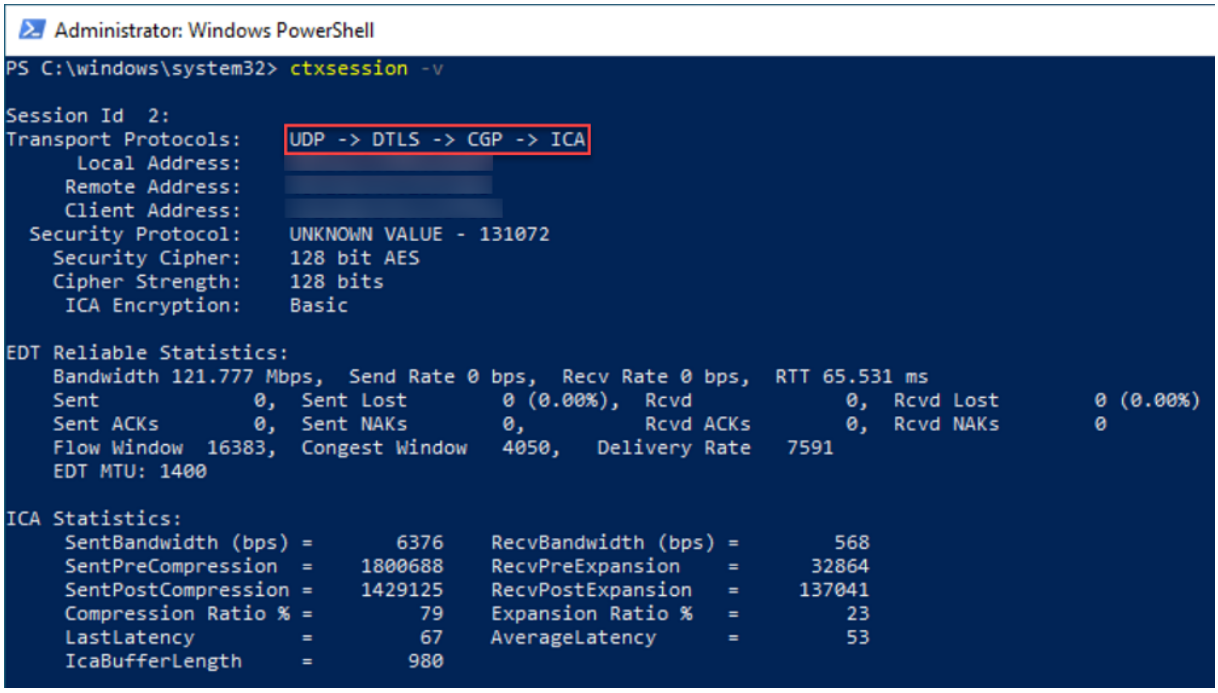
In Director suchen Sie die Sitzung und wählen dann **Details**. Wenn als **Verbindungstyp HDX** und als **Protokoll UDP** angezeigt ist, wird EDT als Transportprotokoll für die Sitzung verwendet. Wenn der

Verbindungstyp RDP ist, wird ICA nicht verwendet, und das **Protokoll** zeigt N/A an. Weitere Informationen finden Sie unter Überwachen von Sitzungen.



Um das Hilfsprogramm CtxSession.exe zu verwenden, starten Sie eine Eingabeaufforderung oder PowerShell in der Sitzung und führen `ctxsession.exe` aus. Zur Anzeige ausführlicher Statistiken führen Sie `ctxsession.exe -v` aus. Wenn EDT verwendet wird, wird eine der folgenden Optionen im Transportprotokoll angezeigt:

- **UDP > ICA** (Sitzungszuverlässigkeit deaktiviert)
- **UDP > CGP > ICA** (Sitzungszuverlässigkeit aktiviert)
- **UDP > DTLS > CGP > ICA** (ICA ist DTLS-verschlüsselt und Ende-zu-Ende)



MTU-Discovery durch EDT

Mit MTU-Discovery kann EDT beim Einrichten einer Sitzung automatisch die maximale Übertragungseinheit (MTU) ermitteln. Dadurch wird eine EDT-Paketfragmentierung verhindert, die zu einer Leistungsminderung oder einem Fehler beim Einrichten der Sitzung führen kann.

Anforderungen

- VDA-Mindestversion 1912 (2103 oder höher empfohlen)
- Citrix Workspace-App
  - Windows: Version 1912 oder höher (2105 oder höher empfohlen)
  - Mac: Version 2108 oder höher
  - Android: Version 21.5 oder höher
- Citrix ADC:
  - 13.0.52.24
  - 12.1.56.22
- Sitzungszuverlässigkeit muss aktiviert sein.

Bei Verwendung von Clientplattformen oder Versionen, die dieses Feature nicht unterstützen, finden Sie unter CTX231821 weitere Informationen zum Konfigurieren einer benutzerdefinierten EDT-MTU, die für Ihre Umgebung geeignet ist.

> **Wichtig:**
>
> Die MTU-Discovery wird nicht mit Multistream-ICA unterstützt.

Aktivieren oder Deaktivieren der MTU-Discovery durch EDT auf dem VDA

Legen Sie den folgenden Registrierungsschlüssel fest:

- Schlüssel: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd
- Wertname: MtuDiscovery
- Werttyp: DWORD
- Wertdaten: 00000001

Starten Sie den VDA neu und warten Sie, bis er registriert ist.

Zum Deaktivieren der MTU-Discovery durch EDT löschen Sie den Registrierungswert und starten Sie den VDA neu.

Diese Einstellung gilt für die ganze Maschine und wirkt sich auf alle von einem unterstützten Client verbundenen Sitzungen aus.

> **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.

Anforderungen

- Citrix Virtual Delivery Agent (VDA) 2003
- Citrix Workspace-App 2002 für Windows
- Sitzungszuverlässigkeit muss aktiviert sein. Weitere Informationen zur Sitzungszuverlässigkeit finden Sie unter Einstellungen der Richtlinie "Sitzungszuverlässigkeit".

Bekannte Probleme

Der adaptive Transport und EDT enthalten folgende Probleme:

- Die Paketfragmentierung kann die Leistung beeinträchtigen oder sogar zum Ausfall von Sitzungen führen. Sie können die EDT-MTU anpassen, um dies zu vermeiden. Verwenden Sie die MTU-Discovery oder die unter CTX231821 beschriebene Problemumgehung.

- Bei aktivierter MTU-Discovery wird möglicherweise ein grauer oder schwarzer Bildschirm angezeigt, wenn Sie eine Sitzung von einem Windows-Client aus starten. Aktualisieren Sie Ihre Workspace-App für Windows auf Version 2105 oder höher bzw. auf Version 1912 CU4 oder höher, um dieses Problem zu beheben.
- Auf Linux- und Android-Clients kann ein Fallback auf TCP fehlschlagen, wenn die Verbindung über Citrix Gateway oder Citrix Gateway Service hergestellt wird. Dies geschieht, wenn die EDT-Aushandlung zwischen Client und Gateway zwar erfolgreich ist, zwischen Gateway und VDA aber fehlschlägt. Führen Sie ein Upgrade auf die Workspace-App für Linux 2104 bzw. die Workspace-App für Android 21.5 oder höher durch, um dieses Problem zu beheben.
- Bei asymmetrischen Netzwerkpfaden kann die MTU-Discovery bei Verbindungen fehlschlagen, die nicht über Citrix Gateway oder Citrix Gateway Service laufen. Führen Sie ein Upgrade auf VDA Version 2103 oder höher durch, um dieses Problem zu beheben. [CVADHELP-16654]
- Bei Verwendung von Citrix Gateway oder Citrix Gateway Service können asymmetrische Netzwerkpfade dazu führen, dass die MTU-Discovery fehlschlägt. Dies liegt an einem Problem im Gateway, das dazu führt, dass das DF-Bit (don't fragment) im Header der EDT-Pakete nicht verteilt wird. Ein Fix für dieses Problem ist noch nicht verfügbar. [CGOP-18438]
- Die MTU-Discovery schlägt möglicherweise für Benutzer fehl, die sich über ein DS-Lite-Netzwerk verbinden. Einige Modems ignorieren das DF-Bit bei aktivierter Paketverarbeitung, sodass die MTU-Discovery eine Fragmentierung nicht erkennt. In dieser Situation sind folgende Optionen verfügbar:
  - Deaktivieren Sie die Paketverarbeitung auf dem Modem des Benutzers.
  - Deaktivieren Sie die MTU-Discovery und verwenden Sie eine fest codierte MTU wie unter CTX231821 beschrieben.
  - Deaktivieren Sie den adaptiven Transport, um die Verwendung von TCP für Sitzungen zu erzwingen. Wenn nur eine Untergruppe von Benutzern betroffen ist, können Sie sie möglicherweise auf der Clientseite deaktivieren, damit andere Benutzer EDT weiterhin verwenden können.

Problembehandlung

Zur Problembehandlung beim adaptiven Transport und EDT empfehlen wir Folgendes:

1. Überprüfen Sie sorgfältig die unter Anforderungen, Überlegungen und Bekannte Probleme aufgeführten Grundsätze.
2. Überprüfen Sie, ob vorhandene Citrix-Richtlinien in Studio oder im GPO die gewünschte Einstellung für den **adaptiven HDX-Transport** überschreiben.

3. Überprüfen Sie, ob vorhandene Einstellungen auf dem Client die gewünschte Einstellung für den adaptiven HDX-Transport überschreiben. Dies kann ein Voreinstellung im Gruppenrichtlinienobjekt, eine mit einer optionalen administrativen Vorlage der Workspace-App konfigurierte Einstellung oder eine manuelle Konfiguration der Einstellung **HDXoverUDP** in der Registrierung oder der Konfigurationsdatei des Clients sein.
4. Stellen Sie auf Maschinen mit Multisitzungs-VDA sicher, dass die UDP-Listener aktiv sind. Öffnen Sie eine Eingabeaufforderung in der VDA-Maschine und führen Sie `netstat -a -p udp` aus. Weitere Informationen finden Sie unter How to Confirm HDX Enlightened Data Transport Protocol.
5. Starten Sie intern eine direkte Sitzung (unter Umgehung des Citrix Gateway), und überprüfen Sie das verwendete Protokoll. Wenn die Sitzung EDT verwendet, ist der VDA in der Lage, EDT für externe Verbindungen über Citrix Gateway zu verwenden.
6. Wenn EDT für direkte interne Verbindungen funktioniert, jedoch nicht für Sitzungen, die über Citrix Gateway laufen:
   - Stellen Sie sicher, dass die Sitzungszuverlässigkeit aktiviert ist.
   - Stellen Sie sicher, dass DTLS im Gateway aktiviert ist.
7. Überprüfen Sie, ob die Firewallregeln in den Netzwerk-Firewalls und in den Firewalls, die auf den VDA-Maschinen ausgeführt werden, richtig konfiguriert sind.
8. Überprüfen Sie, ob die Verbindungen Ihrer Benutzer eine nicht standardmäßige MTU benötigen. Verbindungen mit einer effektiven MTU von weniger als 1500 Byte verursachen eine EDT-Paketfragmentierung, die sich auf die Leistung auswirken oder sogar den Sitzungsstart verhindern kann. Dieses Problem tritt häufig auf, wenn VPN, einige Wi-Fi-Zugangspunkte und Mobilfunknetze wie 4G und 5G verwendet werden. Informationen zur Behebung dieses Problems finden Sie im Abschnitt MTU-Discovery.

Interoperabilität mit Citrix SD-WAN

Die WAN-Optimierung (WANOP) mit Citrix SD-WAN ermöglicht eine sitzungsübergreifende tokenbasierte Datenkomprimierung (Deduplizierung), die auch das URL-basierte Zwischenspeichern von Videos umfasst und deutlich weniger Bandbreite benötigt. Die Reduzierung tritt auf, 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 Citrix Virtual Apps and Desktops-Servern.

Aktuell wird EDT nicht von SD-WAN WANOP unterstützt. Es ist jedoch nicht erforderlich, den adaptiven Transport zu deaktivieren, wenn SD-WAN WANOP verwendet wird. Wenn ein Benutzer eine Sitzung

startet, die über ein SD-WAN mit aktiviertem WANOP läuft, wird automatisch TCP als Transportprotokoll für die Sitzung verwendet. Nicht-WANOP-Sitzungen verwenden nach Möglichkeit weiterhin EDT.

Virtuelle ICA-Kanäle von Citrix

March 9, 2022

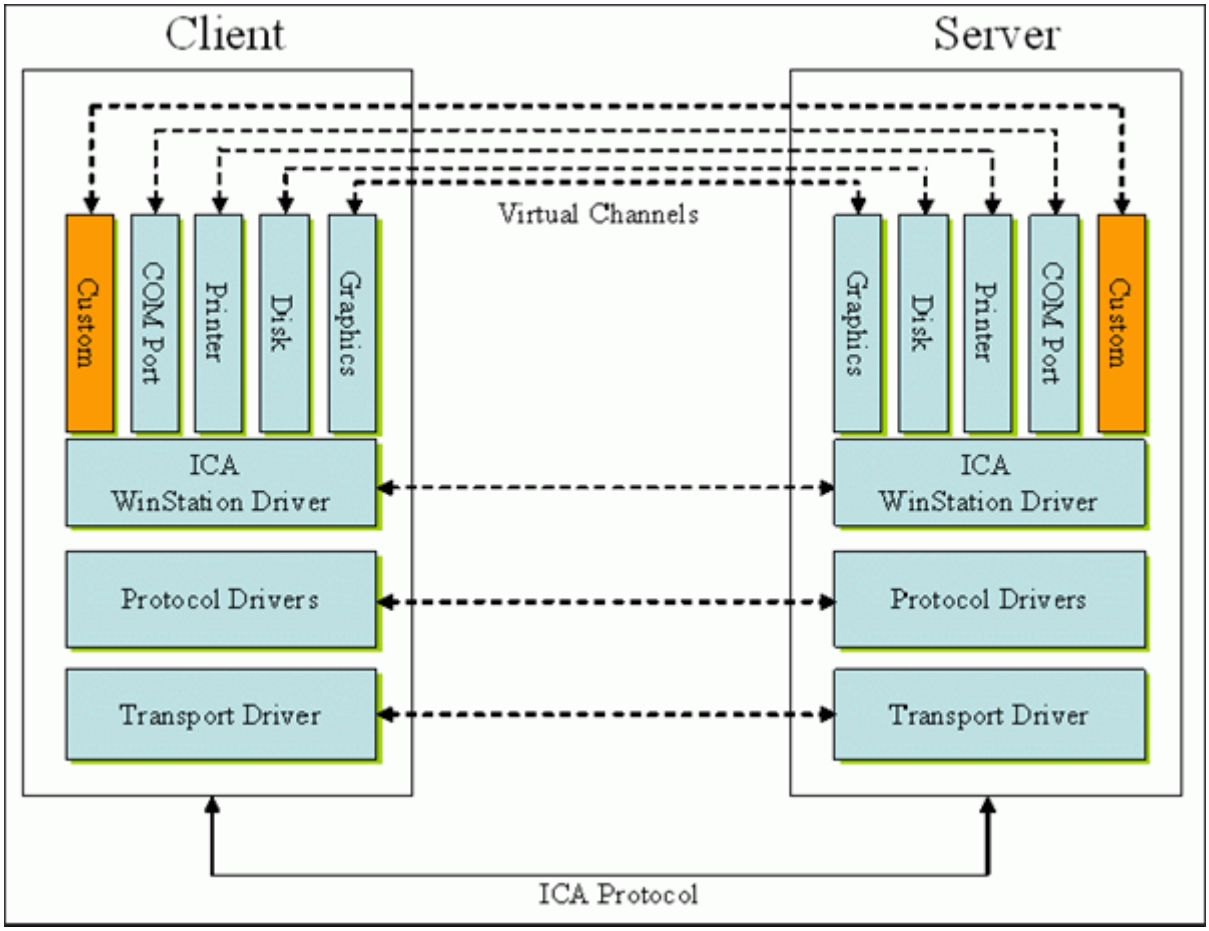
> **Warnung**
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen 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.

Was sind virtuelle ICA-Kanäle

Ein großer Teil der Funktionalität und Kommunikation zwischen der Citrix Workspace-App und den Citrix Virtual Apps and Desktops-Servern erfolgt über virtuelle Kanäle. Virtuelle Kanäle sind erforderlich für den Remotezugriff auf Citrix Virtual Apps and Desktops-Server. Virtuelle Kanäle werden für Folgendes verwendet:

- Audio
- COM-Ports
- Datenträger
- Grafik
- LPT-Ports
- Drucker
- Smartcards
- Benutzerdefinierte virtuelle Kanäle von Drittanbietern
- Video

Gelegentlich werden neue virtuelle Kanäle mit neuen Versionen der Citrix Virtual Apps and Desktops-Server und der Citrix Workspace-App veröffentlicht, um mehr Funktionalität zu bieten.



Ein virtueller Kanal besteht aus einem clientseitigen virtuellen Treiber, der mit einer serverseitigen Anwendung kommuniziert. Im Lieferumfang von Citrix Virtual Apps and Desktops sind mehrere virtuelle Kanäle enthalten. Diese sollen es Kunden und Drittanbietern ermöglichen, eigene virtuelle Kanäle mit einem der mitgelieferten Software Development Kits (SDKs) zu entwickeln.

Virtuelle Kanäle bieten eine sichere Möglichkeit, verschiedene Aufgaben zu erfüllen. Beispiele sind Anwendungen auf einem Citrix Virtual Apps-Server, die mit einem clientseitigen Gerät kommunizieren, oder Anwendungen, die mit der clientseitigen Umgebung kommunizieren.

Auf der Clientseite entsprechen virtuelle Kanäle virtuellen Treibern. Jeder virtuelle Treiber hat eine bestimmte Funktion. Einige sind für den Normalbetrieb erforderlich, während andere optional genutzt werden können. Virtuelle Treiber agieren auf der Protokollebene der Präsentationsschicht. Durch Multiplexing von Kanälen, die durch die Windows Station (WinStation)-Protokollebene bereitgestellt werden, können jederzeit mehrere Protokolle aktiv sein.

Die folgenden Funktionen sind im Registrierungswert "VirtualDriver"unter diesem Registrierungspfad enthalten:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\
Advanced\Modules\ICA 3.0
```


oder

`HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ICA 3.0` (für 64-Bit-Versionen)

- Thinwire3.0 (erforderlich)
- ClientDrive
- ClentPrinterQueue
- ClentPrinterPort
- Zwischenablage
- ClientComm
- ClientAudio
- LicenseHandler (erforderlich)
- TWI (erforderlich)
- SmartCard
- ICACTL (erforderlich)
- SSPI
- TwainRdr
- UserEXperience
- Vd3d

> **Hinweis:**
>
> Sie können spezielle Clientfunktionen deaktivieren, indem Sie einen oder mehrere dieser Werte aus dem Registrierungsschlüssel entfernen. Wenn Sie beispielsweise die Client-Zwischenablage entfernen möchten, entfernen Sie das Wort **Clipboard**.

Diese Liste enthält die virtuellen Client-Treiberdateien und ihre jeweiligen Funktionen. Citrix Virtual Apps und die Citrix Workspace-App für Windows verwenden diese Dateien. Sie sind als Dynamic Link Libraries (Benutzermodus) und nicht als Windows-Treiber (Kernelmodus) konzipiert, mit Ausnahme von Generischem USB, wie unter "Virtueller Kanal für Generisches USB"beschrieben.

- vd3dn.dll –Virtueller Kanal für Direct3D, verwendet für die Desktopgestaltungsumleitung
- vdcamN.dll –Bidirektionales Audio
- vdcdm30n.dll –Clientlaufwerkzuordnung
- vdcom30N.dll –Client-COM-Portzuordnung
- vdcpm30N.dll –Clientdruckerzuordnung
- vdctln.dll –ICA-Steuerungskanal
- vddvc0n.dll –Dynamischer virtueller Kanal
- vdeuemn.dll –End User Experience Monitoring
- vdgusbn.dll –Virtueller Kanal für Generisches USB
- vdkbhook.dll –Transparentes Schlüsselpassthrough
- vdlfpn.dll –Framehawk-Anzeigekanal mit Übertragung auf UDP-Basis

- vdmmn.dll –Multimedia-Unterstützung
- vdmrvc.dll –Virtueller Kanal für Mobile Receiver
- vdmtchn.dll –Multitouch-Unterstützung
- vdscardn.dll –Smartcard-Unterstützung
- vdsens.dll –Virtueller Kanal für Sensoren
- vdspl30n.dll –Client-UPD
- vdsspin.dll –Kerberos
- vdtuin.dll –Transparente Benutzeroberfläche
- vdtw30n.dll –Client-Thinwire
- vdtwin.dll –Seamless
- vdtwn.dll –Twain

Einige virtuelle Kanäle werden in andere Dateien kompiliert. Die Zwischenablagezuordnung ist beispielsweise in wfica32.exe verfügbar.

64-Bit-Kompatibilität

Die Citrix Workspace-App für Windows ist 64-Bit-kompatibel. Wie für die meisten Binärdateien, die für 32 Bit kompiliert sind, gibt es auch für diese Clientdateien 64-Bit-Äquivalente:

- brapi64.dll
- confmgr.dll
- ctxlogging.dll
- ctxmui.dll
- icaconf.exe
- icaconfs.dll
- icafile.dll
- pnipcn64.dll
- pnsson.dll
- ssoncom.exe
- ssonstub.dll
- vdkbhook64.dll

Virtueller Kanal für Generisches USB

Beim Implementieren eines virtuellen Kanals für Generisches USB werden zwei Kernelmodustreiber und der virtuelle Kanaltreiber vdgusbn.dll verwendet:

- ctxusbm.sys
- ctxusbr.sys

Funktionsweise virtueller ICA -Kanäle

Virtuelle Kanäle werden auf verschiedene Art geladen. Mit der Shell (WFShell für den Server und PicaShell für die Workstation) werden einige virtuelle Kanäle geladen. Einige virtuelle Kanäle werden als Windows-Dienste gehostet.

Beispiele virtueller Kanalmodule, die von der Shell geladen werden:

- EUEM
- TWAIN
- Zwischenablage
- Multimedia
- Seamless-Sitzungsfreigabe
- Zeitzone

Manche werden im Kernelmodus geladen. Beispiel sind:

- CtxDvcs.sys –Dynamischer virtueller Kanal
- Icausbb.sys –Generische USB-Umleitung
- Picadm.sys –Clientlaufwerkzuordnung
- Picaser.sys –COM-Portumleitung
- Picapar.sys –LPT-Portumleitung

Virtueller Kanal für Grafiken auf der Serverseite

Ab XenApp 7.0 und XenDesktop7.0 hostet `ctxgfx.exe` den virtuellen Grafikkanal für Sitzungen auf Arbeitsstations- und Terminalserverbasis. `Ctxgfx` hostet plattformspezifische Module, die mit dem entsprechenden Treiber interagieren (`Icardd.dll` für RDSH sowie `vdod.dll` und `vidd.dll` für Arbeitsstation).

Für XenDesktop 3D Pro-Bereitstellungen wird ein OEM-Grafiktreiber für den entsprechenden Grafikprozessor auf dem VDA installiert. `Ctxgfx` lädt spezielle Adaptermodule für die Interaktion mit dem OEM-Grafiktreiber.

Ausführen spezialisierter Kanäle in Windows-Diensten

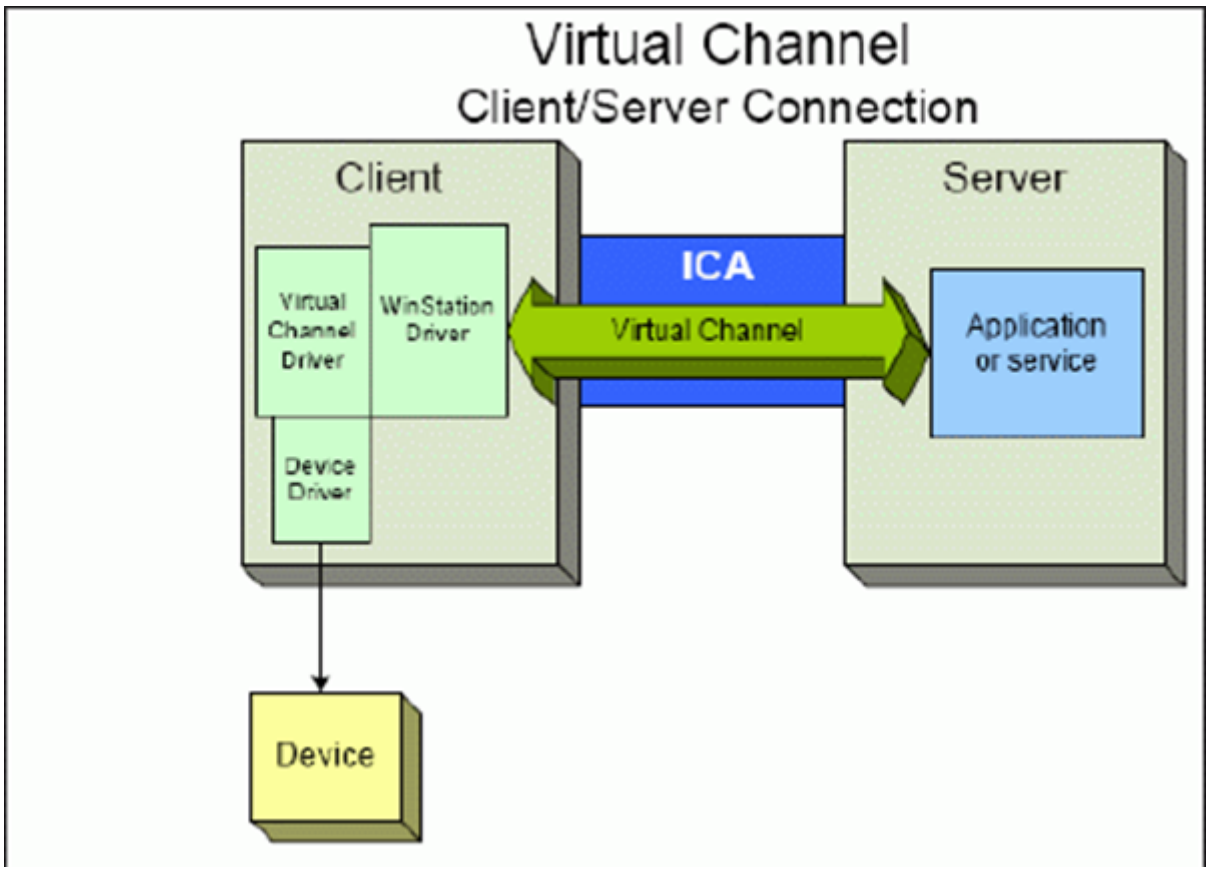
Auf Citrix Virtual Apps and Desktops-Servern werden verschiedene Kanäle als Windows-Dienste gehostet. Ein solches Hosting bietet eine Zuordnungssemantik vom Typ 1:n für mehrere Anwendungen in einer Sitzung und für mehrere Sitzungen auf dem Server. Beispiele für derartige Dienste:

- Citrix-Geräteumleitungsdienst
- Citrix-Dienst für dynamische virtuelle Kanäle

- Citrix-Dienst für End User Experience Monitoring
- Citrix-Dienst für virtuelle Standort- und Sensorkanäle
- Citrix-Multitouch-Umleitungsdienst
- Citrix-Druckmanagerdienst
- Citrix-Smartcarddienst
- Citrix-Audioumleitungsdienst (nur Citrix Virtual Desktops)

Der virtuelle Audiokanal in Citrix Virtual Apps wird über den Windows Audiodienst gehostet.

Auf der Serverseite werden alle virtuellen Client-Kanäle über den WinStation-Treiber Wdica.sys geleitet. Auf der Clientseite werden die virtuellen Client-Kanäle vom entsprechenden WinStation-Treiber abgefragt, der in wfica32.exe integriert ist. Dieses Bild veranschaulicht die Client-Server-Verbindung mit virtuellem Kanal.



Diese Übersicht enthält einen Client-Server-Datenaustausch über einen virtuellen Kanal.

1. Der Client stellt eine Verbindung mit dem Citrix Virtual Apps and Desktops-Server her. Der Client sendet Informationen zu den unterstützten virtuellen Kanälen an den Server.
2. Die serverseitige Anwendung wird gestartet, erhält ein Handle für den virtuellen Kanal und fragt optional weitere Informationen zum Kanal ab.

3. Der virtuelle Clienttreiber und die serverseitige Anwendung nutzen die folgenden zwei Methoden zur Datenübertragung:

    - Wenn Daten von der Serveranwendung an den Client zu senden sind, werden die Daten sofort übertragen. Wenn der Client die Daten empfängt, werden die über den virtuellen Kanal übertragenen Daten aus dem ICA-Datenstrom vom WinStation-Treiber demultiplext und sofort an den virtuellen Clienttreiber weitergeleitet.
    - Wenn Daten vom virtuellen Clienttreiber an den Server zu senden sind, werden sie bei der nächsten Datenabfrage durch den WinStation-Treiber übertragen. Wenn der Server die Daten empfängt, bleiben sie bis zur Auswertung durch die virtuelle Kanalanwendung in der Warteschlange. Es gibt keine Möglichkeit, die virtuelle Kanalanwendung des Servers über den Datenempfang zu informieren.

4. Nach Abschluss der virtuellen Kanalanwendung auf dem Server werden der virtuelle Kanal geschlossen und alle zugewiesenen Ressourcen freigegeben.

Erstellen eines eigenen virtuellen Kanals mit dem Virtual Channel SDK

Das Erstellen eines virtuellen Kanals mit dem Virtual Channel SDK erfordert fortgeschrittene Programmierkenntnisse. Verwenden Sie diese Methode, um einen größeren Kommunikationspfad zwischen Client und Server bereitzustellen. Dies gilt beispielsweise beim Implementieren eines Geräts auf dem Client (z. B. eines Scanners), der mit einem Prozess in der Sitzung verwendet werden soll.

> Hinweise:
>
> - Das Virtual Channel SDK erfordert, dass das WFAPI SDK die serverseitige Komponente des virtuellen Kanals schreibt.
> - Aufgrund der erhöhten Sicherheit für Citrix Virtual Apps and Desktops und die Citrix Workspace-App für Windows ist bei der Installation eines benutzerdefinierten virtuellen Kanals ein zusätzlicher Schritt erforderlich.

Erstellen eines eigenen virtuellen Kanals mit dem ICA Client Object SDK

Das Erstellen eines virtuellen Kanals mit dem ICA Client Object (ICO) ist einfacher als die Verwendung des Virtual Channel SDK. Zur Verwendung des ICO erstellen Sie mit dem **CreateChannels**-Verfahren ein benanntes Objekt in Ihrem Programm.

> Wichtig:
>
> Aufgrund der erhöhten Sicherheit für Citrix Receiver für Windows ab Version 10.00 (und Citrix

> Workspace-Apps für Windows) ist bei der Installation eines virtuellen ICO-Kanals ein zusätzlicher Schritt erforderlich.

Weitere Informationen finden Sie im Client Object API Specification Programmer's Guide.

Passthrough-Funktionalität virtueller Kanäle

Bei Verwendung der Citrix Workspace-App für Windows in einer ICA-Sitzung (auch Passthrough-Sitzung genannt) funktionieren die meisten von Citrix bereitgestellten virtuellen Kanäle unverändert. Berücksichtigen Sie jedoch Folgendes, wenn Sie den Client in zusätzlichen Hops verwenden.

Die folgenden Funktionen funktionieren auf die gleiche Weise in einzelnen Hops oder in mehreren Hops:

- Client-COM-Portzuordnung
- Clientlaufwerkszuordnung
- Clientdruckerzuordnung
- Client-UPD
- End User Experience Monitoring
- Generisches USB
- Kerberos
- Multimedia-Unterstützung
- Smartcard-Unterstützung
- Transparentes Schlüsselpassthrough
- TWAIN

Da Latenz und Faktoren wie Komprimierung, Dekomprimierung und Rendering jedoch bei jedem Hop auftreten, kann jeder zusätzliche Client-Hop die Leistung beeinträchtigen. Dies betrifft folgende Bereiche:

- Bidirektionales Audio
- Dateiübertragungen
- Generische USB-Umleitung
- Seamless
- Thinwire

> Wichtig:
>
> Standardmäßig sind die von einer Client-Instanz in einer Passthrough-Sitzung zugeordneten Clientlaufwerke auf die Clientlaufwerke des verbindenden Clients beschränkt.

Passthrough-Funktionalität virtueller Kanäle zwischen einer Citrix Virtual Desktop-Sitzung und einer Citrix Virtual App-Sitzung

Bei Verwendung der Citrix Workspace-App für Windows in einer ICA-Sitzung auf einem Citrix Virtual Desktops-Server (auch Passthrough-Sitzung genannt) funktionieren die meisten von Citrix bereitgestellten virtuellen Kanäle unverändert.

Auf dem Citrix Virtual Desktops-Server gibt es einen speziellen VDA-Hook, der **picaPassthruHook** ausführt. Durch diesen Hook läuft der Client wie auf einem CPS-Server und wird in den traditionellen Passthrough-Modus versetzt.

Wir unterstützen die folgenden traditionellen virtuellen Kanäle und ihre Funktionalität:

- Client
- Client-COM-Portzuordnung
- Clientlaufwerkszuordnung
- Clientdruckerzuordnung
- Generisches USB (leistungsbeschränkt)
- Multimedia-Unterstützung
- Smartcard-Unterstützung
- SSON
- Transparentes Schlüsselpassthrough

Sicherheit und virtuelle ICA-Kanäle

Bei der Planung, Entwicklung und Implementierung virtueller Kanäle ist eine sichere Nutzung von entscheidender Bedeutung. Dieses Dokument enthält mehrere Verweise auf spezielle Sicherheitsbereiche.

Bewährte Methoden

Öffnen Sie virtuelle Kanäle beim **Verbinden** und **Wiederverbinden**. Schließen Sie virtuelle Kanäle, wenn Sie sich abmelden und die **Verbindung trennen**.

Beachten Sie die folgenden Richtlinien, wenn Sie Skripts erstellen, die virtuelle Kanalfunktionen verwenden.

Benennen der virtuellen Kanäle:

Sie können maximal 32 virtuelle Kanäle erstellen. Siebzehn der 32 Kanäle sind für besondere Zwecke reserviert.

- Die Namen virtueller Kanäle dürfen nicht mehr als sieben Zeichen enthalten.

- Die ersten drei Zeichen sind für den Anbieternamen und die folgenden vier Zeichen für den Kanaltyp reserviert. **CTXAUD** stellt beispielsweise den virtuellen Audiokanal von Citrix dar.

Virtuelle Kanäle werden mit einem ASCII-Namen aus maximal sieben Zeichen bezeichnet. In einigen früheren Versionen des ICA-Protokolls wurden virtuelle Kanäle nummeriert. Die Nummern werden nun dynamisch auf der Basis des ASCII-Namens zugewiesen, da dies die Implementierung vereinfacht. Benutzer, die ihren virtuellen Kanalcode nur für den internen Gebrauch entwickeln, können einen beliebigen Namen aus sieben Zeichen verwenden, sofern kein Konflikt mit vorhandenen virtuellen Kanälen auftritt. Verwenden Sie nur Ziffern sowie Groß- und Kleinbuchstaben im ASCII-Format. Verwenden Sie die bestehende Namenskonvention, wenn Sie eigene virtuelle Kanäle hinzufügen. Es gibt mehrere vordefinierte Kanäle. Die vordefinierten Kanäle beginnen mit der OEM-Kennung CTX und sind nur von Citrix zu verwenden.

Double-Hop-Unterstützung:

Virtueller Kanal	Wird Double Hop unterstützt
Audio	Nein
Umleitung des Browserinhalts	Nein
CDM	Ja
CEIP	Nein
Zwischenablage	Ja
Continuum (MRVC)	Nein
Control VC	Ja
HTML5-Videoumleitung (v1)	Ja
Tastatur, Maus	Ja
MultiTouch	Nein
NSAPVC	Nein
Drucken	Ja
SensVC	Nein
Smartcard	Ja
TWAIN	Ja
USB VC	Ja
WAYCOM-Geräte -K2M mit USB-VC	Ja
Webcamvideokomprimierung	Ja

Virtueller Kanal	Wird Double Hop unterstützt
Windows Media-Umleitung	Ja

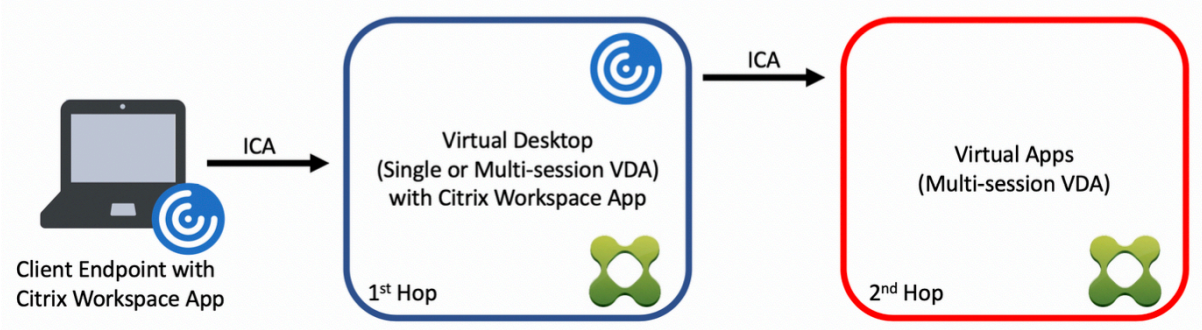
Siehe auch

- ICA Virtual Channel SDK
- Das Citrix Developer Network umfasst alle technischen Ressourcen und Diskussionen zur Verwendung von Citrix SDKs. Sie erhalten Zugriff auf SDKs, Beispielcode und Skripte, Erweiterungen und Plug-Ins sowie die SDK-Dokumentation. Foren zum Citrix Developer Network mit technischen Diskussionen zu den einzelnen Citrix SDKs sind ebenfalls enthalten.

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

May 10, 2023

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 Citrix Virtual Apps and Desktops die 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). Der Artikel Vorbereiten der Installation beschreibt die verfügbaren VDA-Installationsprogramme.

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.

Sie können auch weitere Citrix Komponenten in die Citrix Virtual Apps and Desktops-Bereitstellung integrieren.

- Citrix Provisioning ist eine optionale Komponente, mit der Maschinen durch das Streaming eines Masterimages auf die Zielgeräte bereitgestellt werden.
- Citrix Gateway ist eine sichere Anwendungszugriffslösung, die Administratoren durch Richtlinien auf Anwendungsebene und durch Aktionssteuerung ermöglicht, den Zugriff auf Anwendungen und Daten zu sichern.
- Citrix SD-WAN bietet eine Reihe von Geräten, die die WAN-Leistung optimieren.

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

May 24, 2024

Die Bereitstellung von Citrix Virtual Apps and Desktops 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 etwa Citrix Gateway. Eine Einführung finden Sie unter Integrieren von Citrix Virtual Apps and Desktops und Citrix Gateway.

Mit dem Produktinstallationsprogramm auf dem 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 Citrix Provisioning (zuvor "Provisioning Services") verwendet werden. Weitere Informationen finden Sie unter Installieren von VDAs mit Skripts.

Informationen zu Änderungen an Produktnamen.

Vor Installation zu lesende Informationen

- Technischer Überblick: Wenn Sie mit dem Produkt und den Komponenten nicht vertraut sind.
- 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 (nach dem Installieren der Kernkomponenten) konfigurieren. Richten Sie zuvor 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.
- Das Installieren einer unterstützten Komponente auf einem Server Core-Betriebssystem (z. B. einem Delivery Controller) muss über die Befehlszeile erfolgen. Da dieser Betriebssystemtyp keine grafische Oberfläche bietet, sollten Sie Studio und andere Tools andernorts installieren und sie dann auf den Controller-Server verweisen lassen.

Sie können einen Delivery Controller und einen VDA für Multisitzungs-OS 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 Multisitzungs-OS.

Stellen Sie sicher, dass für jedes Betriebssystem die neuesten Updates ausgeführt wurden. Die Installation eines Controllers oder eines VDAs unter 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 Maschinen mit Windows 10-Einzelsitzungs-OS 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.

Wenn Sie versuchen, einen Windows-VDA unter einem für diese Produktversion nicht unterstützten Betriebssystem zu installieren (bzw. ein VDA-Upgrade auszuführen) werden Sie durch eine Meldung zu einem Artikel geleitet, in dem Ihre Optionen beschrieben werden.

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 Citrix Virtual Apps and Desktops-Komponenten auf Domänencontrollern.
- 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

- Erkennt das Citrix Installationsprogramm beim Installieren oder Aktualisieren von Kernkomponenten (Delivery Controller, Studio, Lizenzserver, Director, StoreFront), dass ein Neustart für eine vorherige Windows-Installation aussteht, endet es mit dem Exitcode 9. Sie werden aufgefordert, die Maschine neu zu starten.

  Dies ist kein von Citrix erzwungener Neustart. Er ist auf andere Komponenten zurückzuführen, die zuvor auf der Maschine installiert wurden. Starten Sie in diesem Fall die Maschine neu und starten Sie dann erneut das Citrix Installationsprogramm.

  Wenn Sie die Befehlszeilenschnittstelle verwenden, können Sie die Prüfung auf einen ausstehenden Neustart mit der Option `/no_pending_reboot_check` verhindern.

- 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 Citrix 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 aktivieren, die Diagnosedaten zur Wartung und Problembehandlung erfassen. Informationen zu diesen Programmen finden Sie unter Citrix Insight Services.
- Google Analytics-Daten werden bei der Installation (oder dem Upgrade) von Studio automatisch erfasst und später hochgeladen. Nach der Installation von Studio können Sie diese Einstellung über den Registrierungsschlüssel `HKLM\Software\Citrix\DesktopStudio\GAEnabled` ändern. Der Wert 1 ermöglicht Sammeln und Upload, 0 deaktiviert Sammeln und Upload.
- Wenn eine VDA-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.

Bei der VDA-Installation

Die Citrix Workspace-App für Windows steht bei der Installation eines VDAs zur Verfügung, wird aber nicht standardmäßig installiert. Sie oder die Benutzer können die Citrix Workspace-App für Windows und anderen Citrix Workspace-App-Versionen von der Citrix Website herunterladen und installieren bzw. aktualisieren. Alternativ können Sie diese Citrix Workspace-Apps über den StoreFront-Server zur Verfügung stellen. Weitere Informationen finden Sie in der StoreFront-Dokumentation.

Der Druckspoolerdienst ist auf den unterstützten Windows-Servern standardmäßig aktiviert. Ist

dieser Dienst deaktiviert, können Sie keinen VDA für Windows-Multisitzungs-OS 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 Media Foundation nicht auf der Maschine mit dem VDA vorhanden ist, funktionieren folgende Multimediafeatures nicht:

- Windows Media-Umleitung
- HTML5-Videoumleitung
- HDX RealTime-Webcamumleitung

Wenn Sie VDA installieren, wird automatisch eine neue lokale Benutzergruppe namens Benutzer mit direktem Zugriff erstellt. Auf VDAs für Einzelsitzungs-OS gilt diese Gruppe nur für RDP-Verbindungen. Auf VDAs für Multisitzungs-OS 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.

VDA Supportability Tools

Alle VDA-Installationsprogramme enthalten ein Supportability-MSI mit Citrix Tools zum Überprüfen der VDA-Leistung (allgemeiner Zustand, Verbindungsqualität usw.). Die Installation des MSI können Sie auf der Seite **Zusätzliche Komponenten** der grafischen Oberfläche des VDA-Installationsprogramms aktivieren oder deaktivieren. Über die Befehlszeile können Sie die Installation mit der Option `/exclude "Citrix Supportability Tools"` ausschließen.

Standardmäßig wird die MSI des Unterstützungsprogramms in `c:\Program Files (x86)\Citrix\Supportability Tools\` installiert. Sie können den Pfad auf der Seite **Komponenten** der grafischen Oberfläche des VDA-Installationsprogramms oder mit der Befehlszeilenoption `/installdir` ändern. Ein geänderter Pfad gilt für alle installierten VDA-Komponenten und nicht nur für die Supportability Tools.

Aktuelle Tools im Supportability-MSI:

- Citrix Health Assistant: Informationen finden Sie unter CTX207624.
- VDA Cleanup Utility: Informationen finden Sie unter CTX209255.

Wenn Sie die Tools bei der VDA-Installation nicht installieren, finden Sie in dem CTX-Artikel einen Link zum aktuellen Downloadpaket.

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 Maschinen mit Windows-Multisitzungs-OS 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.

Nach jedem Neustart wird die VDA-Installation fortgesetzt. (Wenn Sie über die Befehlszeile installieren, können Sie dies mit der Option `/noresume` verhindern.)

> **Hinweis:**
>
> Beim Upgrade auf VDA-Version 7.17 (oder eine spätere unterstützte Version) tritt ein Neustart auf. Dies kann nicht vermieden werden.

Installationsprogramme

Komplettinstallationsprogramm

Mit dem im ISO-Image enthaltenen Komplettinstallationsprogramm:

- Kernkomponenten (Delivery Controller, Studio, Director, StoreFront und Lizenzserver) installieren, aktualisieren oder entfernen
- Windows-VDAs für Server- oder Desktopbetriebssysteme installieren oder aktualisieren
- UpsServer-Komponente des universellen Druckservers auf den Druckservern installieren
- Verbundauthentifizierungsdienst installieren
- Self-Service-Kennwortzurücksetzung installieren

Zum Bereitstellen eines Desktops von einem Multisitzungs-OS 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 vollständige 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. (Sie sind nicht auf dem Komplettinstallationsmedium verfügbar.)

VDAServerSetup.exe:

Installiert einen VDA für Multisitzungs-OS. Es unterstützt alle Optionen für VDAs für Multisitzungs-OS, die auch das Produktinstallationsprogramm bietet.

VDAWorkstationSetup.exe:

Installiert einen VDA für Einzelsitzungs-OS. Es unterstützt alle Optionen für VDAs für Einzelsitzungs-OS, die auch das Produktinstallationsprogramm bietet.

VDAWorkstationCoreSetup.exe:

Installiert einen VDA für Einzelsitzungs-OS, 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`.

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 Supportability Tools
- Citrix Files für Windows
- Citrix Files für Outlook.

`VDAWorkstationCoreSetup.exe` enthält und installiert keine Citrix Workspace-App für Windows.

`VDAWorkstationCoreSetup.exe` entspricht dem Komplettinstallationsprogramm bzw. VDA-WorkstationSetup zum Installieren eines Einzelsitzungs-OS-VDAs und eine der folgenden Optionen:

- Grafische Oberfläche: Auswahl der Option "Remote-PC-Zugriff"auf der Seite **Umgebung**.
- Befehlszeilenschnittstelle: Festlegen der Option `/remotepc`.
- Befehlszeilenschnittstelle: Angeben von `/components vda` und `/exclude "Citrix Personalization for App-V - VDA""Personal vDisk""Machine Identity Service""Citrix User Profile Manager""Citrix User Profile Manager WMI Plugin""Citrix Supportability Tools""Citrix Files for Windows"`.

Sie können die ausgelassenen Komponenten/Features später mit dem Produktinstallationsprogramm installieren. Diese Aktion installiert alle fehlende Komponenten.

Die Browserinhaltsumleitung-MSI wird vom Installationsprogramm `VDAWorkstationCoreSetup.exe` nicht automatisch installiert. (Alle anderen VDA-Installationsprogramme installieren diese MSI automatisch.) Um die Browserinhaltsumleitung zu aktivieren, installieren Sie nach der VDA-Installation `BCR_x64.msi` auf der Maschine. Die MSI-Datei befindet sich im vollständigen Produktinstallationsmedium im Ordner `x64 > Virtual Desktop Components`.

Citrix-Installationsrückgabecodes

Das Ergebnis der Komponenteninstallation wird im Installationsprotokoll in Form eines Citrix Rückgabecodes und nicht als Microsoft-Wert angegeben.

- 0 = Erfolg
- 1 = fehlgeschlagen
- 2 = Teilerfolg
- 3 = Teilerfolg und Neustart erforderlich
- 4 = fehlgeschlagen und Neustart erforderlich
- 5 = vom Benutzer abgebrochen
- 6 = Befehlszeilenargument fehlt
- 7 = neuere Version gefunden
- 8 = erfolgreicher Neustart erforderlich

- 9 = FileLock/Neustart
- 10 = abgebrochen
- 11 = Medien fehlgeschlagen
- 12 = Lizenz fehlgeschlagen
- 13 = Vorabprüfung fehlgeschlagen
- 14 = PendingRebootCheck abgebrochen
- -1 = Beenden

Wenn beispielsweise Tools wie Microsoft System Center Configuration Manager verwendet werden, kann eine skriptgesteuerte VDA-Installation als fehlgeschlagen erscheinen und das Installationsprotokoll enthält den Rückgabecode 3. Dies kann auftreten, wenn das VDA-Installationsprogramm auf einen von Ihnen auszulösenden Neustart wartet (z. B. nach Installation einer erforderlichen Remotedesktopdienste-Rolle auf einem Server). Eine VDA-Installation gilt erst dann als erfolgreich, wenn alle Voraussetzungen und ausgewählten Komponenten installiert wurden und die Maschine nach der Installation neu gestartet wurde.

Alternativ können Sie die Installation auch mit einem CMD-Script umschließen (welches Microsoft-Exitcodes ausgibt) oder die Erfolgscodes im Configuration Manager-Paket ändern.

Microsoft Azure Resource Manager-Virtualisierungsumgebungen

November 14, 2022

Folgen Sie diesen Anleitungen, wenn Sie mit Microsoft Azure Resource Manager virtuelle Maschinen in Ihrer Umgebung bereitstellen.

Sie sollten mit folgenden Elementen vertraut sein:

- Azure Active Directory: https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-create-new-tenant
- Einverständniserklärung: https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app
- Dienstprinzipal: https://docs.microsoft.com/en-us/azure/active-directory/develop/app-objects-and-service-principals

Einschränkungen

Berücksichtigen Sie beim Verwenden von Azure Resource Manager die folgende Einschränkung:

- Dieses Produkt unterstützt keine VDAs in einer Windows Virtual Desktop-Umgebung. Muss WVD unterstützt werden, verwenden Sie Citrix Virtual Apps and Desktops Service oder Citrix Virtual Apps and Desktops Standard für Azure.

Bedarfsgesteuertes Provisioning in Azure

Wenn Sie Maschinenkataloge mit Maschinenerstellungsdiensten (MCS) in Azure Resource Manager erstellen, bietet das bedarfsgesteuerte Provisioning in Azure folgende Vorteile:

- Geringere Speicherkosten
- Schnellere Katalogerstellung
- Schnellere Energievorgänge bei virtuellen Maschinen (VM)

Die Verfahren zum Erstellen von Hostverbindungen und MCS-Maschinenkatalogen in Studio sind beim bedarfsgesteuerten Provisioning die gleichen. Der Unterschied liegt in Art und Zeitpunkt der Ressourcenerstellung und -verwaltung in Azure und in der VM-Sichtbarkeit im Azure-Portal.

Wenn MCS einen Katalog erstellt hat, werden die VMs während des Provisioningvorgangs in Azure erstellt.

Beim bedarfsgesteuerten Provisioning in Azure werden VMs nur erstellt, wenn Citrix Virtual Apps and Desktops nach Abschluss des Provisionings eine Einschaltaktion initiiert. VM sind im Azure-Portal nur sichtbar, wenn sie ausgeführt werden. (In Studio sind VMs unabhängig vom Ausführungsstatus immer sichtbar.)

Wenn Sie einen MCS-Katalog erstellen, werden im Azure-Portal die Ressourcengruppen, Netzwerksicherheitsgruppe, Speicherkonten, Netzwerkschnittstellen, Basisimages und Identitätsdatenträger angezeigt. VMs werden erst dann im Azure-Portal angezeigt, wenn Citrix Virtual Apps and Desktops eine VM-Einschaltaktion startet. Der Status der VM ändert sich dann in Studio in **Ein**.

- Bei gepoolten Maschinen sind OS-Datenträger und Zurückschreibcache nur vorhanden, wenn die VM vorhanden ist. Durch gepoolte Maschinen kann viel Speicher eingespart werden, wenn Sie Ihre Maschinen routinemäßig herunterfahren (z. B. außerhalb der Arbeitszeiten).
- Bei dedizierten Maschinen wird der Betriebssystemdatenträger beim ersten Einschalten der VM erstellt. Es bleibt im Speicher, bis die Maschine gelöscht wird.

Das Initiieren einer Ausschaltaktion für eine VM führt dazu, dass Azure sie löscht. Die VM wird nicht mehr im Azure-Portal angezeigt. In Studio ändert sich der Status der VM in **Aus**.

Vor Einführung des bedarfsgesteuerten Provisionings erstellte Kataloge

VMs in Katalogen, die erstellt wurden, bevor Citrix Virtual Apps and Desktops das bedarfsgesteuerte Provisioning von Azure unterstützte (Mitte 2017), sind im Azure-Portal unabhängig von ihrem Aus-

führungsstatus sichtbar. Sie können diese VMs nicht in Maschinen mit bedarfsgesteuertem Provisioning konvertieren.

Um in den Genuss der Leistungsverbesserungen und verringerten Speicherkosten des bedarfsgesteuerten Provisionings zu kommen, erstellen Sie Kataloge mit MCS.

Azure Managed Disks

Azure Managed Disks ist ein flexibles Datenträgerspeichersystem, das Sie zusammen mit per MCS erstellten Maschinenkatalogen als Alternative zu herkömmlichen Speicherkonten verwenden können.

Das Managed Disks-Feature erleichtert die Erstellung und Verwaltung von Speicherkonten. Es bietet eine einfache und hochverfügbare Lösung zum Erstellen und Verwalten von Datenträgern. Sie können verwaltete Datenträger als Masterimage und als VM verwenden. Die Verwendung verwalteter Datenträger kann die Erstellung und Aktualisierung von Maschinenkatalogen beschleunigen. Weitere Informationen finden Sie unter Informationen zu verwalteten Datenträgern.

Maschinenkataloge verwenden standardmäßig verwaltete Datenträger. Sie können diese Standardeinstellung bei der Katalogerstellung außer Kraft setzen.

Verwenden verwalteter Datenträger

Bei der Erstellung eines Maschinenkatalogs in Studio werden auf der Seite **Masterimage** des Assistenten verwaltete Datenträger zusätzlich zu VMs und virtuellen Festplatten aufgelistet. Nicht alle Azure-Regionen unterstützen das Managed Disks-Feature. Verwaltete Datenträger werden in der Liste für alle Regionen angezeigt, die für die Hostverbindung des Katalogs sichtbar sind.

Die Zeit für die Katalogerstellung ist optimal, wenn Image und Katalog in derselben Region sind.

Das Managed Disks-Feature unterstützt derzeit nicht das Kopieren von Datenträgern zwischen Azure-Regionen. Wenn Sie ein Image in einer anderen Region auswählen, als der, in der der Katalog von MCS bereitgestellt wird, wird das Image in eine VHD in einem herkömmlichen Speicherkonto kopiert. Das Image wird im Katalogbereich angezeigt und dann wieder in einen verwalteten Datenträger konvertiert.

Auf der Seite **Speicher- und Lizenztypen** des Katalogerstellungsassistenten können Sie ein Kontrollkästchen zur Verwendung konventioneller Speicherkonten anstelle verwalteter Datenträger aktivieren. Sie können das Kontrollkästchen nicht aktivieren, wenn das Provisioning in einer Azure-Region erfolgt, die keine verwalteten Datenträger unterstützt.

Erstellen einer Verbindung mit Azure Resource Manager

Informationen zu den Assistenten zum Erstellen einer Verbindung finden Sie unter Verbindungen und Ressourcen. Die nachfolgenden Informationen gelten für Azure Resource Manager-Verbindungen.

Überlegungen:

- Dienstprinzipale müssen für das Abonnement die Teilnehmerrolle haben.
- Beim Erstellen der ersten Verbindung fordert Azure Sie auf, die erforderlichen Berechtigungen zu erteilen. Sie müssen sich für zukünftige Verbindungen neu authentifizieren, Ihre Zustimmung wird jedoch in Azure gespeichert und die Aufforderung nicht wieder angezeigt.
- Für die Authentifizierung verwendete Konten müssen Co-Administrator des Abonnements sein.
- Das für die Authentifizierung verwendete Konto muss Mitglied des Verzeichnisses des Abonnements sein. Es gibt zwei Arten von Konten, auf die Sie achten sollten: "Arbeitsplatz oder Schule"und "Persönliches Microsoft-Konto". Weitere Informationen hierzu finden Sie unter CTX219211.
- Sie können ein vorhandenes Microsoft-Konto verwenden, indem Sie es als Mitglied des Abonnementverzeichnisses hinzufügen. Es kann jedoch zu Komplikationen kommen, wenn dem Benutzer vorher Gastzugriff auf eine der Ressourcen des Verzeichnisses gewährt wurde. In dem Fall gibt es einen Platzhaltereintrag im Verzeichnis, der dem Konto nicht die erforderlichen Berechtigungen gewährt und es wird ein Fehler zurückgegeben.

  Um das Zugriffsproblem zu beheben, entfernen Sie die Ressourcen aus dem Verzeichnis und fügen Sie sie explizit wieder hinzu. Dabei ist jedoch Vorsicht geboten, denn dies hat unbeabsichtigte Auswirkungen auf andere Ressourcen, auf die das Konto zugreifen kann.
- Es gibt ein bekanntes Problem, bei dem bestimmte Konten, die eigentlich Mitglieder sind, als Verzeichnisgäste erkannt werden. Konten, die als Gäste erkannt wurden, treten in der Regel mit älteren, etablierten Verzeichniskonten auf. Fügen Sie als Workaround dem Verzeichnis jeweils ein Konto hinzu, das den richtigen Mitgliedschaftswert erhält.
- Ressourcengruppen sind Container für Ressourcen und enthalten Ressourcen aus ihrer eigenen und aus anderen Regionen. Ressourcengruppen können verwirrend sein, wenn Sie erwarten, dass die Ressourcen in der Region einer Ressourcengruppe angezeigt werden.
- Stellen Sie sicher, dass Ihr Netzwerk und Subnetz groß genug zum Hosten der benötigten Maschinenzahl ist. Die Netzwerkgröße erfordert etwas Planung, doch Microsoft kann Ihnen helfen, die richtigen Werte anzugeben und bietet Empfehlungen für die erforderliche Adressraumkapazität.

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**. Wählen Sie dann Ihre Azure Cloud-Umgebung aus.
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 er darf keine nicht alphanumerischen Zeichen 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 Citrix Virtual Apps and Desktops die aufgelisteten Berechtigungen zu erteilen. In Citrix Virtual Apps and Desktops 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. Nach der erfolgreichen Authentifizierung bei Azure werden die Schaltflächen **Neu erstellen** und **Vorhandene verwenden** durch **Verbunden** ersetzt 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.)
8. Ressourcen umfassen Region und Netzwerk.
    - Wählen Sie auf der Seite **Region** eine Region aus.
    - Geben Sie auf der Seite **Netzwerk** 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 er darf keine nicht alphanumerischen Zeichen 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 auswählen, die keine virtuellen Netzwerke hat, werden Sie zu dieser Seite zurückgeleitet. Wählen Sie eine Region mit virtuellen Netzwerken aus.

9. 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 im nachfolgenden Abschnitt aufgeführten PowerShell-Cmdlets.

Voraussetzungen:

- **$SubscriptionId:** Azure Resource Manager-`SubscriptionID` des Abonnements, für das Sie VDAs bereitstellen möchten.
- **$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:

1. Stellen Sie eine Verbindung mit Ihrem Azure Resource Manager-Abonnement her.

   ```
   Login-AzureRmAccount
   ```

2. Wählen Sie das Azure Resource Manager-Abonnement, in dem Sie den Dienstprinzipal erstellen möchten.

   ```
   Select-AzureRmSubscription -SubscriptionID $SubscriptionId
   ```

3. Erstellen Sie die Anwendung im AD-Mandanten.

   ```
   $AzureADApplication = New-AzureRmADApplication -DisplayName
   $ApplicationName -HomePage "https://localhost/$ApplicationName"-
   IdentifierUris https://$ApplicationName -Password $ApplicationPassword
   ```


4. Erstellen Sie einen Dienstprinzipal.

   ```
   New-AzureRmADServicePrincipal -ApplicationId $AzureADApplication.
   ApplicationId
   ```

5. Weisen Sie dem Dienstprinzipal eine Rolle zu.

   ```
   New-AzureRmRoleAssignment -RoleDefinitionName Contributor -
   ServicePrincipalName $AzureADApplication.ApplicationId –scope
   /subscriptions/$SubscriptionId
   ```

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 nur aus Leerzeichen bestehen oder nur aus nicht-alphanumerischen Zeichen.
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.)
5. Ressourcen umfassen Region und Netzwerk.

   - Wählen Sie auf der Seite **Region** eine Region aus.
   - Geben Sie auf der Seite **Netzwerk** 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 er darf keine nicht alphanumerischen Zeichen 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.

6. Schließen Sie den Assistenten ab.

Erstellen eines Maschinenkatalogs unter Verwendung eines Azure Resource Manager-Masterimages

Diese Informationen ergänzen die Anleitungen unter 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. Allgemeine 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 Anweisungen unter Erstellen von Maschinenkatalogen.
- Wählen Sie auf der Seite **Masterimage** eine Ressourcengruppe aus. Navigieren Sie 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** 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/premium-storage-performance
  - 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 reduziert die Kosten für das Ausführen von VMs in Azure auf die Grundgebühr für Computekapazität. Es verzichtet auf den Preis zusätzlicher Windows Server-Lizenzen aus der Azure-Galerie. Bringen Sie Ihre eigenen on-premises Windows Server-Images in Azure, um HUB zu verwenden. Images aus dem Azure-Katalog werden nicht unterstützt. Lokale Windows Client-Lizenzen werden derzeit nicht unterstützt.

Überprüfen Sie, ob die bereitgestellten virtuellen Maschinen erfolgreich HUB verwenden. Führen Sie den PowerShell Befehl `Get-AzureRmVM -ResourceGroup MyResourceGroup -Name MyVM` aus und überprüfen Sie, ob der Lizenztyp `Windows_Server` ist. Weitere Anweisungen finden Sie unter https://docs.microsoft.com/en-us/azure/virtual-machines/windows/hybrid-use-benefit-licensing/.

- 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.

- Mit MCS: Wählen Sie auf der Seite **Ressourcengruppen** aus, ob Sie neue Ressourcengruppen erstellen oder vorhandene verwenden.

  Wenn Sie neue Ressourcengruppen erstellen möchten, klicken Sie auf **Weiter**.

  Wenn Sie vorhandene Ressourcengruppen verwenden möchten, wählen Sie Gruppen in der Liste **Zum Bereitstellen verfügbare Ressourcengruppen** aus. Wählen Sie genügend Gruppen aus, um die Maschinen aufzunehmen, die Sie im Katalog erstellen. Studio zeigt eine Nachricht an, wenn Sie zu wenige auswählen. Wählen Sie ggf. mehr als die erforderliche Mindestanzahl aus, wenn Sie dem Katalog später weitere VMs hinzufügen möchten. Sie können einem Katalog nach dessen Erstellung keine weiteren Ressourcengruppen mehr hinzufügen.

  Weitere Informationen finden Sie unter Azure-Ressourcengruppen (#azure-resource-groups).

- Die Seiten **Netzwerkkarten**, **Computerkonten** und **Zusammenfassung** enthalten keine Azure-spezifischen Informationen. Folgen Sie den Anweisungen unter Erstellen von Maschinenkatalogen.

Schließen Sie den Assistenten ab.

Löschen von Maschinenkatalogen

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.

Azure-Ressourcengruppen

Azure Provisioning-Ressourcengruppen sind eine Methode des Provisionings von VMs, über die Benutzern Anwendungen und Desktops bereitgestellt werden. Fügen Sie vorhandene, leere Azure-Ressourcengruppen hinzu, wenn Sie in Studio einen MCS-Maschinenkatalog erstellen, oder lassen Sie neue Ressourcengruppen erstellen.

Informationen zu Azure-Ressourcengruppen finden Sie in der Dokumentation von Microsoft.

Anforderungen

- Jede Ressourcengruppe kann bis zu 240 VMs aufnehmen. Die Region, in der Sie den Katalog erstellen, muss ausreichend leere Ressourcengruppen enthalten. Wenn Sie beim Erstellen eines Maschinenkatalogs vorhandene Ressourcengruppen verwenden möchten, müssen Sie genügend Gruppen wählen, um die Anzahl der Maschinen im Katalog aufzunehmen. Wenn Sie beispielsweise im Assistenten zum Erstellen von Katalogen 500 Maschinen angeben, wählen Sie mindestens drei verfügbare Ressourcengruppen aus.

  Sie können einem Maschinenkatalog nach dessen Erstellung keine weiteren Ressourcengruppen mehr hinzufügen. Fügen Sie daher genügend Ressourcengruppen hinzu, damit auch für später hinzugefügte Maschinen noch Kapazität vorhanden ist.
- Erstellen Sie leere Ressourcengruppen in derselben Region wie die Hostverbindung.
- Wenn Sie Ressourcengruppen für jeden MCS-Katalog erstellen möchten, konfigurieren Sie den Azure-Dienstprinzipal, der der Hostverbindung zugeordnet ist. Dieser Prinzipal muss die Berechtigung zum Erstellen und Löschen von Ressourcengruppen haben. Wenn bestehende leere Ressourcengruppen verwendet werden sollen, muss der Azure-Dienstprinzipal, der der Hostverbindung zugeordnet ist, die Teilnehmerrolle für diese leeren Ressourcengruppen haben.
- Wenn Sie in Studio eine Hostverbindung mit der Option **Neu erstellen** erstellen, erhält der erstellte Dienstprinzipal die Teilnehmerrolle für den Abonnementbereich. Alternativ können Sie die Verbindung mit der Option **Vorhandene verwenden** erstellen, und einen bestehenden Abonnementbereichs-Dienstprinzipal angeben. Verwenden Sie die Option **Neu erstellen**, um den Dienstprinzipal in Studio zu erstellen. Der Prinzipal hat die erforderlichen Berechtigungen zum Erstellen und Löschen neuer Ressourcengruppen oder für das Provisioning in vorhandene leere Ressourcengruppen.
- Dienstprinzipale für eingeschränkte Bereiche müssen mit PowerShell erstellt werden. Bei Verwendung eines Dienstprinzipals mit eingeschränktem Gültigkeitsbereich müssen Sie außerdem mit PowerShell oder über das Azure-Portal leere Ressourcengruppen für jeden Katalog erstellen, in dem MCS VMs bereitstellen soll.

Wenn Sie für die Hostverbindung einen Dienstprinzipal mit eingeschränktem Gültigkeitsbereich verwenden und die Masterimage-Ressourcengruppe auf der Seite **Masterimage** des Katalogerstellungsassistenten nicht angezeigt wird, liegt dies wahrscheinlich daran, dass der Dienstprinzipal keine Berechtigung `Microsoft.Resources/subscriptions/resourceGroups/read` zum Auflisten der Masterimage-Ressourcengruppe hat. Schließen Sie den Assistenten, erteilen Sie dem Dienstprinzipal die Berechtigung (siehe Blogpost) und starten Sie den Assistenten neu. Es kann bis zu 10 Minuten dauern, bis das Update in Azure in Studio erscheint.

Informationen zu Azure-Dienstprinzipalen

Für das Provisioning von Maschinen in Azure Resource Manager, muss einem Plug-in Zugriff auf Ihr Azure-Abonnement gewährt werden. Diese Berechtigungen werden über einen Dienstprinzipal erteilt, dem Berechtigungen für die relevanten Azure-Ressourcen zugewiesen wurden. Ein Dienstprinzipal dient im Prinzip demselben Zweck wie ein Benutzerkonto. Er stellt die eine Azure Active Directory-Identität des Plug-Ins dar, die Anmeldeinformationen zur Authentifizierung und Berechtigungen für Azure-Ressourcen umfasst. Wie Benutzerkonten werden Dienstprinzipale über die rollenbasierten Zugriffssteuerung (RBAC) konfiguriert.

Abhängig von der Berechtigungsdefinition klassifizieren wir Dienstprinzipale als:

- Dienstprinzipale mit Abonnementgeltungsbereich oder als
- Dienstprinzipale mit eingeschränktem Gültigkeitsbereich

Dienstprinzipale mit Abonnementgeltungsbereich Dienstprinzipale mit Abonnementgeltungsbereich haben die Berechtigung *Mitwirkender* für alle Ressourcen im Abonnement, wodurch sie einfach zu erstellen und zu verwalten sind. Citrix Studio automatisiert das Erstellen von Dienstprinzipalen mit Abonnementgeltungsbereich. Sie können auch manuell in PowerShell erstellt werden. Mit diesen Prinzipalen kann das Azure Resource Manager-Plug-In Azure-Ressourcengruppen erstellen und die Ressourcenverwaltung vollständig automatisieren. Der Nachteil besteht darin, dass das Plug-In über Berechtigungen für Ressourcen im Abonnement verfügt, die nichts mit den Ressourcen zu tun haben, die das Plug-In verwaltet.

Mit der Rolle *Mitwirkender* kann das Plug-In alle Ressourcen im Abonnement erstellen, löschen, lesen und schreiben. Die Berechtigungen erstrecken sich nicht auf Objekte in Azure Active Directory, auch können Dienstprinzipale mit Abonnementgeltungsbereich anderen Benutzern oder Dienstprinzipalen keinen Zugriff auf Ressourcen gewähren.

Dienstprinzipale mit eingeschränktem Gültigkeitsbereich Dienstprinzipale mit eingeschränktem Gültigkeitsbereich ermöglichen dem Azure Resource Manager-Plug-In Zugriff auf einen von Ihnen

definierten Satz von Ressourcen. Azure erfordert Dienstprinzipale mit Abonnementgeltungsbereich zum Erstellen von Ressourcengruppen. Bei Verwendung von Dienstprinzipalen mit eingeschränktem Gültigkeitsbereich kann das Plug-In keine Ressourcengruppen erstellen. Zusätzlich zu den Dienstprinzipalen müssen Sie für jeden Katalog, für den Maschinen bereitgestellt werden sollen, einen Pool von Ressourcengruppen bereitstellen.

In Citrix Studio können weder Dienstprinzipale noch Kataloge mit eingeschränktem Gültigkeitsbereich erstellt werden. Beide Aufgaben müssen mit PowerShell ausgeführt werden. Sobald ein Katalog erstellt wurde, kann er jedoch wie jeder andere in Studio verwaltet werden. Dazu gehören auch das Hinzufügen und Löschen von Maschinen. Wenn Sie einen bestehenden Dienstprinzipal mit eingeschränktem Gültigkeitsbereich mit einem neuen Ressourcengruppenpool verwenden möchten, müssen Sie dem Dienstprinzipal mit PowerShell explizit Berechtigungen hinzufügen.

Ermitteln der Azure-Abonnement-Zugriffsanforderungen Die Techniken und Beispiele in den folgenden Abschnitten beziehen sich auf gängige Anforderungen und müssen je nach tatsächlicher Situation modifiziert werden.

Ziehen Sie in folgenden Fällen die Verwendung eines Dienstprinzipals mit Abonnementgeltungsbereich in Erwägung:

- Sie wünschen eine möglichst einfache Verwaltung.
- Sie möchten die Verwendung von PowerShell vermeiden und alles über Citrix Studio verwalten.
- Sie nutzen Ihr Azure-Abonnement dediziert für einen Citrix Virtual Apps and Desktops Service.
- Sie installieren Citrix Virtual Apps and Desktops für eine Machbarkeitsstudie.
- Die Administratoren von Citrix Virtual Apps and Desktops haben Zugriff als Mitwirkende zum Azure-Abonnementbereich.

Ziehen Sie in folgenden Fällen die Verwendung eines Dienstprinzipals mit eingeschränktem Gültigkeitsbereich in Erwägung:

- Ihr Azure-Abonnement wird für mehrere unabhängige Dienste verwendet.
- Die Azure-Administratoren haben unterschiedliche Abonnementberechtigungen abhängig von ihrer Rolle.
- Die Sicherheitsstandards Ihres Unternehmens erfordern eine detaillierte Zugriffssteuerung.
- Sie verfügen bereits über einen Prozess zum Erstellen von Dienstprinzipalen mit eingeschränktem Gültigkeitsbereich.

> **Tipp:**
>
> Sie können *untergeordnete* Abonnements erstellen, die als Teil Ihres primären Abonnements in

> Rechnung gestellt werden und auf das standardmäßige Azure Active Directory Ihres primären Abonnements verweisen. Durch diese Konfiguration haben Sie einen weiteren Mechanismus zur Steuerung des Zugriffs auf nicht verwandte Ressourcen.

Planen eines Dienstprinzipals mit eingeschränktem Gültigkeitsbereich Bevor Sie einen Katalog für einen Dienstprinzipal mit eingeschränktem Gültigkeitsbereich erstellen, ermitteln Sie die Zahl der erforderlichen Ressourcengruppen zum Hosten der anfänglichen und zukünftigen Anzahl virtueller Maschinen. Aufgrund einer Einschränkung in den Maschinenerstellungsdiensten können nach der Katalogerstellung keine Ressourcengruppen mehr hinzugefügt werden.

Bereitstellen eines Katalogs pro Ressourcengruppenpool Das Azure Resource Manager-Plug-In erstellt die erforderliche Infrastruktur in jeder Ressourcengruppe. Die Ressourcengruppe besteht aus Speicherkonten, Sicherheitsgruppen, Netzwerkschnittstellen, virtuellen Maschinen usw. Speicherkonten werden bei Bedarf erstellt, wenn Maschinen zum Katalog hinzugefügt werden. Die Größe eines Katalogs kann daher bis auf eine durch die Größe des Ressourcengruppenpools und Azure-Abonnementkontingente festgelegte Obergrenze wachsen. Speicherkonten werden erst wieder gelöscht, wenn der Katalog gelöscht wird. Da jede virtuelle Maschine gelöscht werden kann, kann es dazu kommen, dass leere Speicherkonten entstehen. Das kommt selten vor, da virtuelle Maschinen in der Regel per Zufallsprinzip über die verfügbaren Speicherkonten verteilt werden. Maschinen müssen mühsam ausgewählt werden, indem der Inhalt von Speicherkonten überprüft wird, um ein Speicherkonto absichtlich zu leeren.

Azure beschränkt die Anzahl der virtuellen Maschinen in einer Ressourcengruppe auf 800, doch das Azure Resource Manager-Plug-In verwendet eine andere Kennzahl. Ein standardmäßiger Azure-Datenträger hat ein Limit von 500 IOPS und ein Standardspeicherkonto hat ein IOPS-Limit von 20.000. Aus diesem Grund stellt das Plug-In maximal 40 Maschinen für ein Speicherkonto bereit. Dieses Limit gilt sowohl für Standard- als auch für Premiumspeicher. Außerdem erstellt das Plug-In maximal 19 Speicherkonten in einer Ressourcengruppe.

Die Grundformel für die Berechnung der Anzahl der Ressourcengruppen basierend auf der maximalen Anzahl von Maschinen ist somit:

Anzahl der Ressourcengruppen = Obergrenze (maximale Anzahl der Maschinen/(40 x 19))

Das Azure Resource Manager-Plug-In geht davon aus, dass es einen Ressourcengruppenpool exklusiv verwendet. Es gibt keine benutzererstellten Ressourcen in einer der angegebenen Ressourcengruppen.

Grundlagen der rollenbasierten Zugriffssteuerung (RBAC) in Azure.

Der Zugriff auf Azure-Ressourcen wird gewährt, indem einem Dienstprinzipal in einem bestimmten Bereich eine RBAC-Rolle zugewiesen wird. Der Bereich kann ein Abonnement, eine Ressourcengruppe oder eine Ressource sein. Ressourcen sind in einer Kapselungshierarchie angeordnet und die durch

die Rolle definierten Berechtigungen gelten für alle Ressourcen unterhalb des Bereichs, auf den sie angewendet wird. Eine auf ein Abonnement angewendete Rolle wird auf alle Ressourcen im Abonnement angewendet. Eine auf eine Ressourcengruppe angewendete Rolle wird auf alle Ressourcen in der Ressourcengruppe angewendet.

Bei der Azure-Ressourcenhierarchie können nur Dienstprinzipale mit Berechtigungen für den Abonnementbereich Ressourcengruppen erstellen. Das ist nicht ideal, da Anwendungen wie das Plug-In daran gehindert werden, Ressourcengruppen bei Bedarf für eine logische Gruppe zu erstellen und Ressourcen zu verwalten. Dies ist nur möglich, wenn sie haben ein hohes Maß an Berechtigungen für das ganze Abonnement haben.

Azure bietet viele integrierte Rollen und unterstützt auch die Definition benutzerdefinierter Rollen. Weitere Informationen zu benutzerdefinierten Rollen in der Azure-RBAC finden Sie unter Benutzerdefinierte Rollen für Azure-Ressourcen.

Erstellen eines Dienstprinzipals mit Abonnementgeltungsbereich In diesem Beispiel wird gezeigt, wie ein Dienstprinzipal mit Abonnementgeltungsbereich erstellt wird. Anhand der Informationen kann eine Azure-Verbindung in Citrix Studio erstellt werden. Sie können einen vorhandenen Dienstprinzipal verwenden oder eine Azure-Verbindung manuell in PowerShell erstellen.

```
param(
[string]$applicationName = "SubscriptionScopeSP",
[Parameter(Mandatory=$true)][string]$applicationPassword,
[Parameter(Mandatory=$true)][string]$subscriptionId
)

$application = New-AzureRmADApplication -DisplayName $applicationName -
    HomePage "https://localhost/$applicationName" `
-IdentifierUris "https://$applicationName" -Password
    $applicationPassword

New-AzureRmADServicePrincipal -ApplicationId $application.ApplicationId

# Wait for the service principal to become available
Start-Sleep -s 60

New-AzureRmRoleAssignment -RoleDefinitionName Contributor -
    ServicePrincipalName $application.ApplicationId `
-scope "/subscriptions/$subscriptionId"

Write-Host ("Application ID: " + $application.ApplicationId)
<!--NeedCopy-->
```

Erstellen eines Dienstprinzipals mit eingeschränktem Gültigkeitsbereich In diesem Abschnitt wird die Erstellung eines grundlegenden Dienstprinzipals mit eingeschränktem Gültigkeitsbereich mit Zuweisung von Berechtigungen im Ressourcengruppenbereich erläutert.

Das Azure Resource Manager-Plug-In benötigt Berechtigung für die folgenden Ressourcen:

1. Masterimage-VHD
2. Virtuelles Netzwerk für die Maschinen
3. Ressourcengruppen, in denen die Maschinen bereitgestellt werden sollen

Zur Vereinfachung des Skripts wird davon ausgegangen, dass der Zugriff der Rolle "Mitwirkender" im Ressourcengruppenbereich gewährt werden kann. Das Azure Resource Manager-Plug-In hat die Berechtigung der Rolle "Mitwirkender"für die Ressourcengruppe, in der die Image-VHD gespeichert ist, für die Ressourcengruppe, die das virtuelle Netzwerk enthält, und für den Ressourcengruppenpool, in dem die Maschinen bereitgestellt werden.

```
param(
[string]$applicationName = "BasicNarrowScopeSP",
[Parameter(Mandatory=$true)][string]$applicationPassword,
[Parameter(Mandatory=$true)][string]$subscriptionId,
[Parameter(Mandatory=$true)][string[]]$resourceGroups
)

$application = New-AzureRmADApplication -DisplayName $applicationName -
    HomePage "https://localhost/$applicationName" `
-IdentifierUris "https://$applicationName" -Password
    $applicationPassword

New-AzureRmADServicePrincipal -ApplicationId $application.ApplicationId

# Wait for the service principal to become available
Start-Sleep -s 60

New-AzureRmRoleAssignment -RoleDefinitionName Citrix-Network-Usage-
    Reader -ServicePrincipalName $application.ApplicationId `
-scope "/subscriptions/$subscriptionId/"

foreach ($rg in $resourceGroups)
{

  New-AzureRmRoleAssignment -RoleDefinitionName Contributor -
     ServicePrincipalName $application.ApplicationId `
  -scope "/subscriptions/$subscriptionId/resourcegroups/$rg"
 }


Write-Host ("Application ID: " + $application.ApplicationId)
<!--NeedCopy-->
```

Erstellen eines Dienstprinzipals mit eingeschränktem Gültigkeitsbereich über benutzerdefinierte Rollen Azure umfasst viele integrierte RBAC-Rollen. Citrix verwendet die Rolle "Mitwirkender"wie im vorherigen Abschnitt. Wie bereits erwähnt, hat das Azure Resource Manager-Plug-In dadurch

geringfügig mehr Berechtigungen als unbedingt erforderlich. Mit dem Verfahren in diesem Abschnitt wird eine benutzerdefinierte Rolle definiert und der Zugriff stärker eingeschränkt. Falls gewünscht, kann der Zugriff über weitere benutzerdefinierte Rollen und die direkte Anwendung von Rollen auf Image und Netzwerkressourcen blockiert werden.

> **Hinweis:**
>
> Die erforderlichen Berechtigungen können sich ändern.

Verwenden Sie die folgenden Berechtigungen zum Festlegen einer benutzerdefinierten Rolle für den Zugriff auf das virtuelle Netzwerk und das Masterimage im Ressourcengruppenbereich.

Masterimage-VHD.

Für die Katalogerstellung:

- Microsoft.Storage/storageAccounts/read
- Microsoft.Storage/storageAccounts/listKeys/action

Für zukünftige Citrix Studio-Unterstützung:

- Microsoft.Resources/subscriptions/resourceGroups/read

Virtuelles Netzwerk für die Maschinen:

- Microsoft.Network/virtualNetworks/read
- Microsoft.Network/virtualNetworks/subnets/join/action

Ressourcengruppen für bereitgestellte Maschinen.

Es ist möglich, eine weitere benutzerdefinierte Rolle mit den nachfolgenden Berechtigungen zu erstellen, doch der Einfachheit halber wird im Beispiel die Rolle "Mitwirkender"für die Ressourcengruppen mit den Maschinen verwendet. Diese Ressourcengruppen enthalten keine Ressourcen, die nicht vom Azure Resource Manager-Plug-In erstellt werden. Durch die Verwendung der Rolle "Mitwirkender"ist es eher unwahrscheinlich, dass Änderungen am Plug-In Änderungen am Dienstprinzipal erfordern:

- Microsoft.Compute/virtualMachines/*
- Microsoft.Network/networkInterfaces/*
- Microsoft.Network/networkSecurityGroups/*
- Microsoft.Resources/deployments/*
- Microsoft.Resources/subscriptions/resourceGroups/read
- Microsoft.Storage/storageAccounts/*

- Microsoft.Storage/storageAccounts/listKeys/action

Benutzerdefinierte Citrix Virtual Apps and Desktops-Zugriffsrollen.

Erstellen Sie eine benutzerdefinierte Rolle, indem Sie diese zuerst in der JSON definieren:

```
{

  "Name": "Citrix-Custom-Reader",
  "Description": "Grants access to Citrix XenDesktop images and virtual
      networks.",
  "Actions": [
    "Microsoft.Storage/storageAccounts/read",
    "Microsoft.Storage/storageAccounts/listKeys/action",
    "Microsoft.Network/virtualNetworks/read",
    "Microsoft.Network/virtualNetworks/subnets/join/action"
  ],
  "NotActions": [
  ],
  "AssignableScopes": [
    "/subscriptions/<YOUR-SUBSCRIPTION-ID>"
  ]
 }

<!--NeedCopy-->
```

Erstellen Sie die Rolle unter Verweis auf die **JSON-Definition**:

```
New-AzureRmRoleDefinition -InputFile citrix-custom-reader.json
<!--NeedCopy-->
```

Verwenden Sie die neue benutzerdefinierte Rolle beim Erstellen des Dienstprinzipals:

```
param(
[string]$applicationName = "NarrowScopeSP",
[Parameter(Mandatory=$true)][string]$applicationPassword,
[Parameter(Mandatory=$true)][string]$subscriptionId,
[Parameter(Mandatory=$true)][string[]]$machineResourceGroups,
[Parameter(Mandatory=$true)][string]$imageResourceGroup,
[Parameter(Mandatory=$true)][string]$networkResourceGroup
)

$application = New-AzureRmADApplication -DisplayName $applicationName -
    HomePage "https://localhost/$applicationName" `
-IdentifierUris "https://$applicationName" -Password
    $applicationPassword

New-AzureRmADServicePrincipal -ApplicationId $application.ApplicationId

# Wait for the service principal to become available
Start-Sleep -s 60

New-AzureRmRoleAssignment -RoleDefinitionName Citrix-Network-Usage-
    Reader -ServicePrincipalName $application.ApplicationId `
```



```
-scope "/subscriptions/$subscriptionId/"

foreach ($rg in $machineResourceGroups)
{

  New-AzureRmRoleAssignment -RoleDefinitionName Contributor -
     ServicePrincipalName $application.ApplicationId `
  -scope "/subscriptions/$subscriptionId/resourcegroups/$rg"
 }


New-AzureRmRoleAssignment -RoleDefinitionName Citrix-Custom-Reader -
    ServicePrincipalName $application.ApplicationId `
-scope "/subscriptions/$subscriptionId/resourcegroups/
    $imageResourceGroup"

New-AzureRmRoleAssignment -RoleDefinitionName Citrix-Custom-Reader -
    ServicePrincipalName $application.ApplicationId `
-scope "/subscriptions/$subscriptionId/resourcegroups/
    $networkResourceGroup"

Write-Host ("Application ID: " + $application.ApplicationId)
<!--NeedCopy-->
```

Erstellen von Citrix Virtual Apps and Desktops-Azure-Verbindungen.

Eine Azure-Verbindung für Citrix Virtual Apps and Desktops kann in Citrix Studio mit einem vorhandenen Dienstprinzipal erstellt werden. Die Verbindung kann auch über PowerShell erstellt werden.

Im Folgenden finden Sie ein Beispiel für das Erstellen einer Verbindung in PowerShell:

```
param(
[string]$connectionName = "AzureConnection",
[Parameter(Mandatory=$true)][string]$applicationId,
[Parameter(Mandatory=$true)][string]$applicationPassword,
[Parameter(Mandatory=$true)][string]$subscriptionId,
[Parameter(Mandatory=$true)][string]$subscriptionName,
[Parameter(Mandatory=$true)][string]$tenantId
)

Add-PsSnapin Citrix*

$customProperties = @"
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance">
 <Property xsi:type="StringProperty" Name="AuthenticationAuthority"
     Value="https://login.microsoftonline.com/"/>
 <Property xsi:type="StringProperty" Name="ManagementEndpoint" Value="
     https://management.azure.com/"/>
 <Property xsi:type="StringProperty" Name="StorageSuffix" Value="core.
     windows.net"/>
 <Property xsi:type="StringProperty" Name="TenantId" Value="$tenantId"
```



```
    />
 <Property xsi:type="StringProperty" Name="SubscriptionId" Value="
    $subscriptionId"/>
 <Property xsi:type="StringProperty" Name="SubscriptionName" Value="
    $subscriptionName"/>
</CustomProperties>
"@

$connection = New-Item -ConnectionType "Custom" -CustomProperties
    $customProperties -HypervisorAddress @("https://management.azure.com
    /") `
-Path @("XDHyp:\Connections$connectionName") -Persist -PluginId "
    AzureRmFactory" -Scope @() `
-SecurePassword (ConvertTo-SecureString -AsPlainText -Force
    $applicationPassword) -UserName $applicationId

New-BrokerHypervisorConnection -HypHypervisorConnectionUid $connection.
    HypervisorConnectionUid

<!--NeedCopy-->
```

An dieser Stelle fügen Sie der Verbindung Ressourcen mit Studio oder PowerShell hinzu.

Erstellen von Katalogen für Citrix Virtual Apps and Desktops.

Im folgenden Beispiel werden die Citrix PowerShell-Snap-Ins zum Erstellen eines Citrix Virtual Apps and Desktops-Katalogs verwendet.

Da das Azure Resource Manager-Plug-In mit einem Dienstprinzipal mit eingeschränktem Gültigkeitsbereich keine Ressourcengruppen erstellen kann, müssen Sie folgende Schritte ausführen:

1. Erstellen eines Ressourcengruppenpools
2. Erteilen der Dienstprinzipalberechtigungen für alle Ressourcengruppen im Pool
3. Auflisten jeder Ressourcengruppe im Pool in einer benutzerdefinierten Eigenschaft bei der Erstellung des Provisioningschemas

Die benutzerdefinierte Eigenschaft heißt **ResourceGroups**, der Wert ist eine durch Kommas getrennte Liste von Ressourcengruppennamen. Das Beispiel unten zeigt die Definition der benutzerdefinierten Eigenschaft.

> **Hinweis:**
>
> In der benutzerdefinierten Eigenschaft werden nur Ressourcengruppen aufgelistet, die für Maschinen bestimmt sind. Ressourcengruppen mit dem Image bzw. dem virtuellen Netzwerk werden nicht aufgelistet. Werden sie angegeben, versucht das Azure Resource Manager-Plug-In, Maschinen für diese Ressourcengruppen bereitzustellen, was zu einem unbeabsichtigtem Verhalten führen kann.

In dem Beispiel werden Maschinen in zwei Ressourcengruppen (xd-sales-1 und xd-sales-2) bereitgestellt:

```
Add-PsSnapin Citrix*

# The hosting unit name is the name of the Azure connection resources that should be used for this catalog
$hostingUnitName = "AzureHostingUnit"
$domain = "citrix.local"
$controllerAddress = ("ddc." + $domain)
$adminAddress = ($controllerAddress + ":80")
$catalogName = "catalog-name"
$network = "network-resource-group.resourcegroup\network-name"
$subnet = "subnet-name"
$serviceOffering = "Standard_A4"
$template = "image-resource-group.resourcegroup\imagestorage.storageaccount\images.container\image-name.vhd"

$customProperties = @" <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <Property xsi:type="StringProperty" Name="StorageAccountType" Value="Standard_LRS" />
    <Property xsi:type="StringProperty" Name="ResourceGroups" Value="xd-sales-1, xd-sales-2" />
</CustomProperties>
"@

$identityPool = New-AcctIdentityPool -AdminAddress $adminAddress -AllowUnicode -Domain $domain `
    -IdentityPoolName $catalogName -NamingScheme "vm-#" -NamingSchemeType "Numeric" -Scope @()

$brokerCatalog = New-BrokerCatalog -AdminAddress $adminAddress -AllocationType "Random" -IsRemotePC $False `
    -MinimumFunctionalLevel "L7_9" -Name $catalogName -PersistUserChanges "Discard" -ProvisioningType "MCS" -Scope @() `
    -SessionSupport "MultiSession"

Write-Host $brokerCatalog

$provScheme = New-ProvScheme -AdminAddress $adminAddress -CleanOnBoot -CustomProperties $customProperties `
    -HostingUnitName $hostingUnitName -IdentityPoolName $catalogName `
    -MasterImageVM "XDHyp:\HostingUnits$hostingUnitName\image.folder$template.vhd" `
    -NetworkMapping @{
 "0"="XDHyp:\HostingUnits$hostingUnitName\virtualprivatecloud.folder$network.virtualprivatecloud$subnet.network" }
  `
    -ProvisioningSchemeName $catalogName -Scope @() -SecurityGroup @() `
```



```
36      -ServiceOffering "XDHyp:\HostingUnits$hostingUnitName\
           serviceoffering.folder$serviceOffering.serviceoffering"
37
38  Write-Host $provScheme
39
40  Set-BrokerCatalog -AdminAddress $adminAddress -Name $catalogName -
       ProvisioningSchemeId $provScheme.ProvisioningSchemeUid
41
42  Add-ProvSchemeControllerAddress -AdminAddress $adminAddress.com -
       ControllerAddress $controllerAddress -ProvisioningSchemeName
       $catalogName
43  <!--NeedCopy-->
```

An dieser Stelle können Sie die Katalogseite in Citrix Studio aktualisieren und wie bei jedem anderen Katalog Maschinen hinzufügen und verwalten.

Konfigurieren von Ressourcengruppen für einen Maschinenkatalog in Studio

Auf der Seite **Ressourcengruppen** im Katalogerstellungsassistenten können Sie auswählen, ob neue Ressourcengruppen erstellt oder vorhandene verwendet werden sollen. Weitere Informationen finden Sie unter Erstellen eines Maschinenkatalogs unter Verwendung eines Azure Resource Manager-Masterimages.

Ressourcengruppen beim Löschen eines Maschinenkatalogs:

- Wenn Sie Citrix Virtual Apps and Desktops beim Erstellen eines Maschinenkatalogs Ressourcengruppen erstellen lassen und den Katalog später löschen, werden auch die Ressourcengruppen und alle darin enthaltenen Ressourcen gelöscht.
- Wenn Sie beim Erstellen eines Maschinenkatalogs bestehende Ressourcengruppen verwenden und den Katalog später löschen, werden alle in den Ressourcengruppen enthaltenen Ressourcen gelöscht, die Ressourcengruppen selbst bleiben jedoch erhalten.

Überlegungen, Einschränkungen und Problembehandlung

Wenn Sie bestehende Ressourcengruppen verwenden, wird die Liste verfügbarer Ressourcengruppen auf der Seite “Ressourcengruppen”im Katalogerstellungsassistenten nicht automatisch aktualisiert. Wenn Sie bei geöffneter Assistentenseite Berechtigungen für Ressourcengruppen in Azure erstellen oder hinzufügen, werden die Änderungen daher nicht in der Liste des Assistenten angezeigt. Zur Anzeige der Änderungen gehen Sie entweder zurück zur Seite **Maschinenverwaltung**, wo Sie die der Hostverbindung zugeordneten Ressourcen erneut auswählen, oder schließen Sie den Assistenten und starten Sie ihn neu. Es kann bis zu 10 Minuten dauern, bis in Azure gemachte Änderungen in Studio erscheinen.

Ressourcengruppen sollten nur in je einem Maschinenkatalog verwendet werden. Dies wird jedoch nicht erzwungen. Beispiel: Sie wählen beim Erstellen eines Katalogs 10 Ressourcengruppen aus, erstellen jedoch nur eine Maschine in dem Katalog. Neun der ausgewählten Ressourcengruppen bleiben leer, nachdem der Katalog erstellt wurde. Sie planen, die Gruppen später evtl. zum Erweitern der Kapazität zu verwenden, und behalten die Verknüpfung mit dem Katalog bei. Sie können einem Katalog nach dessen Erstellung keine weiteren Ressourcengruppen mehr hinzufügen. Daher ist es eine gute Idee, eventuelles künftiges Wachstum einzuplanen. Wenn nun ein anderer Katalog erstellt wird, werden die neun Ressourcengruppen in der Liste der verfügbaren Gruppen angezeigt. In Citrix Virtual Apps and Desktops wird derzeit nicht nachverfolgt, welche Ressourcengruppen welchen Katalogen zugeordnet sind. Es liegt an Ihnen, das zu überwachen.

Wenn der Dienstprinzipal Ihrer Verbindung auf leere Ressourcengruppen in verschiedenen Regionen zugreifen kann, werden die Gruppen aus allen Regionen in der Liste der verfügbaren Gruppen angezeigt. Achten Sie darauf, Ressourcengruppen der Region auszuwählen, in welcher der Maschinenkatalog erstellt wird.

Problembehandlung:

- Ressourcengruppen werden nicht in der Liste auf der Seite "Ressourcengruppen"des Katalogerstellungsassistenten angezeigt.

  Der Dienstprinzipal muss die erforderlichen Berechtigungen für die Ressourcengruppen verfügen, die in der Liste angezeigt werden sollen. Siehe den Abschnitt "Anforderungen"oben.

- Beim Hinzufügen von Maschinen zu einem zuvor erstellten Maschinenkatalog werden nicht alle Maschinen bereitgestellt.

  Nach Erstellen eines Katalog dürfen Sie beim späteren Hinzufügen weiterer Maschinen die Maschinenkapazität der ursprünglich für den Katalog ausgewählten Ressourcengruppen (240 pro Gruppe) nicht überschreiten. Sie können einem Katalog nach dessen Erstellung keine weiteren Ressourcengruppen mehr hinzufügen. Wenn Sie versuchen, mehr Maschinen hinzuzufügen als die vorhandenen Ressourcengruppen aufnehmen können, schlägt das Provisioning fehl.

  Beispiel: Sie erstellen einen Maschinenkatalog mit 300 VMs und 2 Ressourcengruppen. Die Ressourcengruppen können bis zu 480 VMs (2 x 240) aufnehmen. Wenn Sie später versuchen, dem Katalog 200 VMs hinzuzufügen, übersteigt dies die Kapazität der Ressourcengruppen (300 bestehende VMs + 200 neue = 500, doch die Ressourcengruppen können maximal 480 aufnehmen).

Weitere Informationen

- Verbindungen und Ressourcen
- Maschinenkataloge erstellen

- CTX219211: Set up a Microsoft Azure Active Directory account
- CTX219243: Grant XenApp and XenDesktop access to your Azure subscription
- CTX219271: Deploy hybrid cloud using site-to-site VPN

Microsoft System Center Virtual Machine Manager-Virtualisierungsumgebungen

February 6, 2020

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 unter Systemanforderungen aufgeführten VMM-Versionen.

Verwenden Sie Citrix Provisioning (zuvor "Provisioning Services") und Maschinenerstellungsdienste zum Bereitstellen folgender Elemente:

- Desktop- oder Serverbetriebssystem-VM der ersten Generation
- VM der zweiten Generation mit Windows Server 2012 R2, Windows Server 2019, Windows Server 2016 und Windows 10 (mit oder ohne sicheren Start)

Installieren und Konfigurieren eines Hypervisors

> **Wichtig:**
>
> Alle Delivery Controller müssen in derselben Gesamtstruktur sein wie die VMM-Server.

1. Installieren Sie Microsoft Hyper-V Server und VMM auf Ihren Servern.
2. 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.
3. 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.

Die direkte Installation eines Controllers auf einem Server, auf dem Hyper-V ausgeführt wird, wird nicht unterstützt.

Erstellen einer Master-VM

1. Installieren Sie einen VDA auf der Master-VM und wählen Sie die Option zur Desktopoptimierung aus. Dies verbessert die Leistung.
2. Erstellen Sie einen Snapshot der Master-VM, um diesen als Sicherungskopie zu verwenden.

Erstellen virtueller Desktops

Bei Verwendung von MCS zum Erstellen von VM beim Erstellen einer Site oder einer Verbindung:

1. Wählen Sie den Typ des Microsoft-Virtualisierungshosts aus.
2. Geben Sie die Adresse als vollqualifizierten Domänennamen des Hostservers ein.
3. Geben Sie die Anmeldeinformationen für das zuvor erstellte Administratorkonto ein, das Berechtigungen zum Erstellen von VM enthält.
4. Wählen unter **Hostdetails** den Cluster oder eigenständigen Host aus, der beim Erstellen der neuen VM verwendet werden soll.

   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
<!--NeedCopy-->
```

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

- **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:

  Upload der Identitätsdisk durch die HCL auf die Hyper-V-Maschine über die Administratorfreigabe.

  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).

Die HCL löscht die Datei aus der Administratorfreigabe.

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.

  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.

  Die HCL liest den Datenträger aus der Administratorfreigabe der Hyper-V-Maschine in den Speicher.

  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.

Citrix Hypervisor-Virtualisierungsumgebungen

April 19, 2024

Erstellen einer Verbindung zu Citrix Hypervisor

Beim Erstellen einer Verbindung zu Citrix Hypervisor (früher XenServer) müssen Sie die Anmeldeinformationen eines VM-Hauptadministrators oder eines höherrangigen Benutzers eingeben.

Citrix empfiehlt, HTTPS zum Sicheren der Kommunikation mit Citrix Hypervisor zu verwenden. Um HTTPS zu verwenden, müssen Sie das standardmäßig mit Citrix Hypervisor installierte SSL-Zertifikat ersetzen (siehe CTX128656).

Sie können hohe Verfügbarkeit konfigurieren, wenn dies auf Citrix Hypervisor aktiviert ist. Citrix empfiehlt, dass Sie alle Server im Pool (über Server mit hoher Verfügbarkeit bearbeiten) auswählen, um die Kommunikation mit dem Citrix Hypervisor-Server zu ermöglichen, wenn der Poolmaster ausfällt.

Sie können einen GPU-Typ und eine GPU-Gruppe oder Passthrough auswählen, wenn Citrix Hypervisor vGPU unterstützt. Es wird angezeigt, ob die Auswahl dedizierte GPU-Ressourcen umfasst.

Wenn Sie auf Citrix Hypervisor-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.)

Verwenden von IntelliCache für Citrix Hypervisor-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 differenzierender Datenträgern 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 verwenden zu können, müssen Sie ihn sowohl in diesem Produkt als auch in Citrix Hypervisor aktivieren.

- Bei der Installation von Citrix Hypervisor wählen Sie **Enable thin provisioning (Optimized storage for Citrix Virtual Desktops)**. 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 zu Citrix Hypervisor.

- In Citrix Virtual Apps and Desktops ist IntelliCache standardmäßig deaktiviert. Sie können die Einstellung nur beim Erstellen einer Citrix Hypervisor-Verbindung ändern, IntelliCache kann später nicht deaktiviert werden. Wenn Sie eine Citrix Hypervisor-Verbindung hinzufügen:
  - Wählen Sie als Speichertyp **Freigegeben** aus.
  - Aktivieren Sie das Kontrollkästchen **IntelliCache verwenden**.

Erforderliche Citrix Hypervisor-Berechtigungen

Die Citrix Hypervisor-Berechtigungen sind rollenbasiert (RBAC).

Weitere Informationen finden Sie unter Rollenbasierte Zugriffskontrolle.

Die Rollenhierarchie lautet in der Reihenfolge steigender Berechtigungen: Schreibgeschützt → VM-Operator → VM-Hauptadministrator → Pooloperator → Pooladministrator.

Im folgenden Abschnitt wird die Mindestrolle zusammengefasst, die für jede Bereitstellungsaufgabe erforderlich ist.

Hostverbindung erstellen

Aufgabe	Erforderliche Mindestrolle
Hostverbindung unter Verwendung der von XenServer abgerufenen Informationen hinzufügen	Schreibgeschützt
Benutzer und ihre zugewiesene Rolle anzeigen	Schreibgeschützt

Energieverwaltung virtueller Maschinen

Aufgabe	Erforderliche Mindestrolle
VMs ein- oder ausschalten	VM-Operator

Erstellen, Aktualisieren oder Löschen von VMs

Aufgabe	Erforderliche Mindestrolle
VMs zu bestehenden Snapshot-Zeitplänen hinzufügen oder daraus entfernen	VM-Hauptadministrator
Snapshot-Zeitpläne hinzufügen, ändern und löschen	Pooloperator
Masterimage veröffentlichen	Pooloperator (Switch-Port-Sperre erforderlich)
Maschinenkatalog erstellen	Pooloperator: Switch-Port-Sperre erforderlich
VMs hinzufügen oder entfernen (keine GPU-fähigen VMs)	VM-Administrator
VMs hinzufügen oder entfernen (GPU-fähige VMs)	Pooloperator
Virtuelle Datenträger oder CD-Geräte hinzufügen, entfernen oder konfigurieren	VM-Administrator
Tags verwalten	VM-Operator

Weitere Informationen zu RBAC-Rollen und -Berechtigungen finden Sie unter RBAC-Rollen und -Berechtigungen.

Informationen zum Sperren von Switch-Ports finden Sie unter Switch-Port-Sperre verwenden.

Erstellen eines Maschinenkatalogs über eine Citrix Hypervisor-Verbindung

GPU-fähige Maschinen benötigen 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 Citrix VM 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.

Weitere Informationen

- Verbindungen und Ressourcen
- Maschinenkataloge erstellen

Microsoft System Center Configuration Manager-Umgebungen

September 21, 2021

Bei Sites, in denen der Zugriff auf Anwendungen und Desktops mit Microsoft System Center Configuration Manager (Configuration Manager) verwaltet wird, kann diese Verwendung über folgende Optionen auf Citrix Virtual Apps and Desktops ausgeweitet werden:

- Installieren von VDAs mit SCCM.
- **Configuration Manager Wake Proxy-Feature:** Für das Wake-On-LAN-Feature für den Remote-PC-Zugriff wird Configuration Manager benötigt. Weitere Informationen finden Sie unter Remote-PC-Zugriff - Wake-On-LAN.
- **Citrix Virtual Apps and Desktops-Eigenschaften:** Diese Eigenschaften ermöglichen das Identifizieren von Citrix Virtual Desktops für die Verwaltung durch Configuration Manager. (In einigen Versionen verwendet Configuration Manager den früheren Namen von Citrix Virtual Apps and Desktops: XenApp und XenDesktop.)

Eigenschaften

Eigenschaften stehen Microsoft System Center Configuration Manager für die Verwaltung virtueller Desktops zur Verfügung.

Boolesche Eigenschaften in Configuration Manager werden möglicherweise als `1` oder `0` statt "True" oder "False"angezeigt.

Die Eigenschaften sind für die Klasse `Citrix_virtualDesktopInfo` im Namespace `Root\Citrix\DesktopInformation` verfügbar. 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` (legt `IsAssigned` auf `True` fest)

Eigenschaft	Beschreibung
`BrokerSiteName`	Site. Gibt den gleichen Wert zurück wie `HostIdentifier`
`DesktopCatalogName`	Dem Desktop zugewiesener Maschinenkatalog
`DesktopGroupName`	Dem Desktop zugewiesene Bereitstellungsgruppe
`HostIdentifier`	Site. Gibt den gleichen Wert zurück wie `BrokerSiteName`
`IsAssigned`	`True` = Desktop wird einem Benutzer zugewiesen; `False` = zufälliger Desktop
`IsMasterImage`	Ermöglicht Entscheidungen bezüglich der Umgebung. Beispielsweise könnten Sie Anwendungen auf dem Image 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 Image 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. Dieser Speicherort ist für Benutzer nicht zugänglich.
`PersonalvDiskDriveLetter`	Bei einem Desktop mit einer persönlichen vDisk ist dies der Laufwerksbuchstabe, den Sie der persönlichen vDisk zuweisen.
`BrokerSiteName`, `DesktopCatalogName`, `DesktopGroupName`, `HostIdentifier`	Werden festgelegt, wenn der Desktop beim Controller registriert wird. Sie sind Null bei einem nicht vollständig registrierten Desktop.

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 enthalten die Namen möglicherweise Leerzeichen oder weichen vom Eigenschaftsnamen geringfügig ab. Zum Beispiel könnte `BrokerSiteName` als `Broker Site Name` erscheinen.

- 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.

VMware-Virtualisierungsumgebungen

June 27, 2024

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/s/article/2101567). Wenn Sie das Feature deaktivieren, funktioniert MCS nicht richtig.

Erforderliche Privilegien

Erstellen Sie ein VMware-Benutzerkonto und mindestens eine VMware-Rolle mit einigen oder allen Berechtigungen, die in diesem Artikel aufgeführt sind. Berücksichtigen Sie bei der Rollenerstellung die erforderliche Granularität für die Benutzerberechtigungen zum jederzeitigen Anfordern der verschiedenen Citrix DaaS-Vorgänge. Zum Gewähren spezifischer Berechtigungen für jeden Zeitpunkt weisen Sie dem Benutzer die entsprechende Rolle mindestens auf Datencenterebene zu, wobei die Option **An untergeordnete Elemente weitergeben** aktiviert ist.

Die folgenden Tabellen zeigen die Zuordnungen zwischen Citrix Virtual Apps and Desktops-Vorgängen und die erforderlichen VMware-Mindestberechtigungen.

> **Hinweis:**
>
> Der Anzeigename der Berechtigungsliste, insbesondere für *User Interface*, ist in einigen vSphere-Versionen unterschiedlich. In vSphere 6.7 lautet die Berechtigung für *User Interface* beispielsweise **Change Memory** und **Change Settings** und nicht **Settings** und **Memory**, wie hier in den erforderlichen Berechtigungen beschrieben.

Verbindungen und Ressourcen hinzufügen

SDK	Benutzeroberfläche
System.Anonymous, System.Read und System.View	Automatisch hinzugefügt. Kann die integrierte Lesezugriff-Rolle verwenden.

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
Datastore.Browse	Datastore > Browse datastore

Bereitstellen von Maschinen (Maschinenerstellungsdienste)

Für das Provisioning von Maschinen mit MCS sind die folgenden Berechtigungen erforderlich:

SDK	Benutzeroberfläche
Datastore.AllocateSpace	Datastore > Allocate Space
Datastore.Browse	Datastore > Browse datastore
Datastore.FileManagement	Datastore > Low level file operations

SDK	Benutzeroberfläche
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
Virtual machine.Config > Add or remove device	Virtual machine > Configuration > Add or remove device
VirtualMachine.Config.AdvancedConfig	Virtual machine > Configuration > Advanced
VirtualMachine.Config.RemoveDisk	Virtual machine > Configuration > Remove disk
VirtualMachine.Config.CPUCount	Virtual machine > Configuration > Change CPU count
VirtualMachine.Config.Memory	Virtual machine > Configuration > Change memory
VirtualMachine.Config.Settings	Virtual machine > Configuration > Change settings
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
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, vSphere 5.1, Update 1, and vSphere 6.x, Update 1: Virtual machine > State > Create snapshot; vSphere 5.5: Virtual machine > Snapshot management > Create snapshot

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

Speicherprofil (vSAN)

Zum Anzeigen, Erstellen oder Löschen von Speicherrichtlinien bei der Katalogerstellung in einem vSAN-Datenspeicher sind die folgenden Berechtigungen obligatorisch:

SDK	Benutzeroberfläche
StorageProfile.Update	PROFILE-DRIVEN STORAGE > Profile-driven storage update. vSphere 8: VM storage policies > Update VM storage policies
StorageProfile.View	PROFILE-DRIVEN STORAGE > Profile-driven storage view. vSphere 8: VM storage policies > View VM storage policies

Tags und benutzerdefinierte Attribute

Mithilfe von Tags und benutzerdefinierten Attributen können Sie Metadaten an die im vSphere-Bestand erstellten VMs anhängen und das Suchen und Filtern dieser Objekte vereinfachen. Zum Erstellen, Bearbeiten, Zuweisen und Löschen von Tags oder Kategorien sind die folgenden Berechtigungen erforderlich:

SDK	Benutzeroberfläche
InventoryService.Tagging.CreateTag	vSphere Tagging > Create vSphere Tag
InventoryService.Tagging.CreateCategory	vSphere Tagging > Create vSphere Tag Category
InventoryService.Tagging.EditTag	vSphere Tagging > Edit vSphere Tag
InventoryService.Tagging.EditCategory	vSphere Tagging > Edit vSphere Tag Category
InventoryService.Tagging.DeleteTag	vSphere Tagging > Delete vSphere Tag
InventoryService.Tagging.DeleteCategory	vSphere Tagging > Delete vSphere Tag Category
InventoryService.Tagging.AttachTag	vSphere Tagging > Assign or Unassign vSphere Tag
InventoryService.Tagging.ObjectAttachable	vSphere Tagging > Assign or Unassign vSphere Tag on Object
Global.ManageCustomFields	Global > Manage custom attributes
Global.SetCustomField	Global > Set custom attribute

> **Hinweis:**
>
> Wenn MCS einen Maschinenkatalog erstellt, weist es den Ziel-VMs Namens-Tags zu. Anhand der Tags wird das Masterimage von mit MCS erstellten VMs unterschieden und verhindert, dass letztere für die Imageerstellung verwendet werden. Sie können den Unterschied anhand des Attributs `XdProvisioned` in vCenter identifizieren. Das Attribut ist **True**, wenn MCS VMs erstellt.

Kryptographische Verfahren

Berechtigungen für kryptografische Verfahren legen fest, welcher Benutzer welche Art von kryptografischem Verfahren an welchem Objekttyp ausführen kann. vSphere Native Key Provider verwendet die `Cryptographer.*`-Berechtigungen. Die folgenden Mindestberechtigungen sind für kryptographische Verfahren erforderlich:

SDK	Benutzeroberfläche
Cryptographer.Access	Privileges > All Privileges > Cryptographic operations > Direct Access
Cryptographer.AddDisk	Privileges > All Privileges > Cryptographic operations > Add disk
Cryptographer.Clone	Privileges > All Privileges > Cryptographic operations > Clone
Cryptographer.Encrypt	Privileges > All Privileges > Cryptographic operations > Encrypt
Cryptographer.EncryptNew	Privileges > All Privileges > Cryptographic operations > Encrypt new
Cryptographer.Decrypt	Privileges > All Privileges > Cryptographic operations > Decrypt
Cryptographer.Migrate	Privileges > All Privileges > Cryptographic operations > Migrate
Cryptographer.ReadKeyServersInfo	Privileges > All Privileges > Cryptographic operations > Read KMS information

Bereitstellen von Maschinen (Citrix Provisioning)

Um VMs über die Citrix Provisioning-Konsole mit dem Citrix Virtual Apps and Desktops-Setupassistenten und dem Assistenten zum Exportieren von Geräten bereitzustellen, sind diese Berechtigungen zum Klonen und Bereitstellen einer Vorlage erforderlich. Legen Sie die Berechtigungen fest, während

Sie eine Hostingverbindung herstellen. Sie benötigen 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
VApp.Export	vApp > Export

> **Hinweis:**
>
> `VApp.Export` ist für die Erstellung von MCS-Maschinenkatalogen mithilfe von Maschinenprofilen erforderlich.

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

SDK	Benutzeroberfläche
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

Zertifikat beschaffen und importieren

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 Delivery Controller hinzu.

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/etc/ hinzu. Dieser Schritt ist nur erforderlich, wenn der FQDN des Computers, auf dem vCenter Server ausgeführt wird, nicht bereits im Domänennamensystem vorhanden ist.
2. Rufen Sie das vCenter-Zertifikat mit einer der folgenden drei Methoden ab:

   Führen Sie auf dem vCenter-Server folgende Schritte aus:

   a) Kopieren Sie die Datei rui.crt vom vCenter-Server zu einem Speicherort, auf den Ihre Delivery Controller zugreifen können.

b) 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.

a) Öffnen Sie einen Webbrowser und stellen Sie eine sichere Webverbindung mit dem vCenter-Server her (z. B. https://server1.domain1.com)).
b) Akzeptieren Sie die Sicherheitswarnungen.
c) Klicken Sie auf die Adressleiste, in der der Zertifikatfehler angezeigt wird.
d) Zeigen Sie das Zertifikat an und klicken Sie auf die Registerkarte "Details".
e) Wählen Sie **Copy to file and export in .CER format** und geben Sie bei entsprechender Aufforderung einen Namen an.
f) Speichern Sie das exportierte Zertifikat.
g) Navigieren Sie auf den Speicherort des exportierten Zertifikats und öffnen Sie die CER-Datei.

Importieren Sie direkt über Internet Explorer unter Ausführung als Administrator.

- Öffnen Sie einen Webbrowser und stellen Sie eine sichere Webverbindung mit dem vCenter-Server her (z. B. https://server1.domain1.com)).
- Akzeptieren Sie die Sicherheitswarnungen.
- Klicken Sie auf die Adressleiste, in der der Zertifikatfehler angezeigt wird.
- Zeigen Sie das Zertifikat an.

3. Importieren Sie das Zertifikat auf jedem Controller in den Zertifikatspeicher.

a) Klicken Sie auf **Zertifikat installieren**, wählen Sie **Lokaler Computer** und klicken Sie dann auf **Weiter**.
b) Wählen Sie **Alle Zertifikate in folgendem Speicher speichern** und klicken Sie dann auf **Durchsuchen**. Wählen Sie **Vertrauenswürdige Personen** und klicken Sie auf **OK**. Klicken Sie auf **Weiter** und dann auf **Fertigstellen**.

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 Citrix Virtual Apps and Desktops 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

October 6, 2022

Folgen Sie diesen Anleitungen, wenn Sie mit Nutanix Acropolis virtuelle Maschinen in Ihrer Citrix Virtual Apps and Desktops-Bereitstellung bereitstellen. Der Setupvorgang umfasst die folgenden Aufgaben:

- Installieren und Registrieren des Nutanix-Plug-Ins in der Citrix Virtual Apps and Desktops-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 heruntergeladen werden kann.

Vorbereiten der Installation des Nutanix MCS-Plug-Ins für den Citrix Cloud Connector

Für die Integration von Nutanix Acropolis im Delivery Controller von Citrix Virtual Apps and Desktops gelten folgende Voraussetzungen:

- Benutzer, die das AHV MCS-Plug-In für das Citrix Cloud Connector-Installationsprogramm ausführen, müssen über Administratorrechte für die Citrix Cloud Connector-VM verfügen.
- Registrieren Sie die Citrix Cloud Connector-VM bei einem Ressourcenstandort im Citrix Cloud-Mandanten.
- Installieren Sie das AHV MCS-Plug-In für den Citrix Cloud Connector auf allen Cloud Connectors, die beim Citrix Cloud-Mandanten registriert sind. Führen Sie diese Installation auch dann durch, wenn die Connectors einen Ressourcenstandort ohne AHV bereitstellen.

Installieren und Registrieren des Nutanix-Plug-Ins

Nach der Installation der Citrix Virtual Apps and Desktops-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 `C:\\Program Files\\Common Files\\Citrix\\HCLPlugins\\RegisterPlugins.exe –PluginsRoot "C:\\Program Files\\Common Files\\Citrix\\HCLPlugins\\CitrixMachineCreation\\v1.0.0.0"` aus.
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
<!--NeedCopy-->
```


Erstellen einer Verbindung mit Nutanix

Vollständige Informationen zu allen Seiten in den Assistenten zum Erstellen einer Verbindung finden Sie unter 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 Katalog verwendet. Erstellen Sie erst Images und Snapshots in Nutanix, bevor Sie den Katalog 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 Erstellen von Maschinenkatalogen.

Wählen Sie auf der Seite **Container**, die nur für Nutanix gilt, den Container aus, in dem die Datenträger 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 Citrix Virtual Apps and Desktops 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 Erstellen von Maschinenkatalogen.

Microsoft Azure-Virtualisierungsumgebungen

June 27, 2024

> **HINWEIS:**
>
> Dieser Artikel enthält Informationen zu Azure (Classic). Informationen zu Azure Resource Manager finden Sie unter Virtualisierungsumgebungen mit Microsoft Azure Resource Manager.

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="\*address\*"
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 von Verbindungseinstellungen.

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.

- VM- und Cloudgrößen für Azure: https://docs.microsoft.com/en-us/azure/cloud-services/cloud-services-sizes-specs
- Preise virtueller Maschinen: http://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 http://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 1000 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://docs.microsoft.com/en-us/azure/azure-resource-manager/management/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

March 15, 2022

Die Kernkomponenten des Installationsmediums sind der Citrix Delivery Controller, Citrix Studio, Citrix Director und Citrix Lizenzserver.

(In Versionen vor 1912 LTSR CU1 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.)

Lesen Sie vor der Installation den vorliegenden Artikel sowie Vorbereiten der Installation.

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

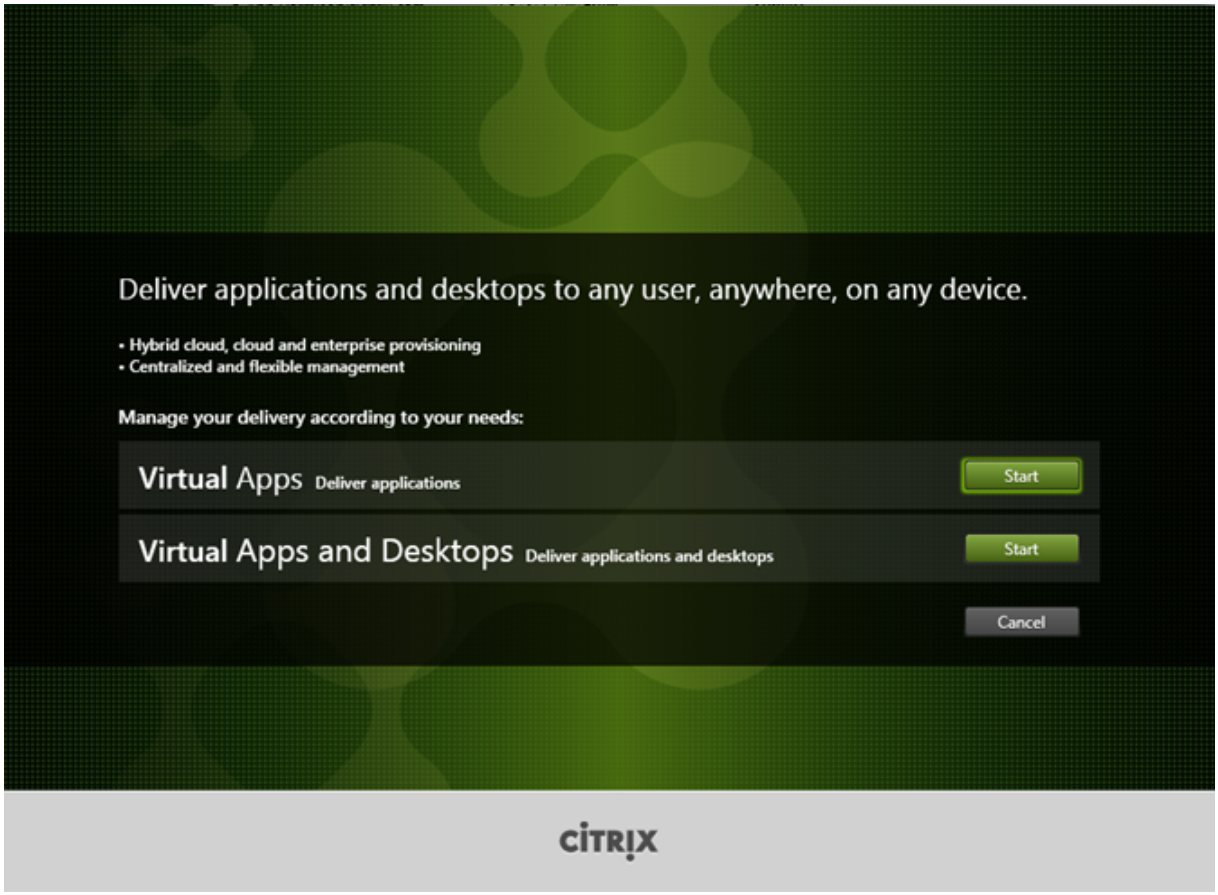
Rufen Sie unter Angabe Ihrer Citrix Anmeldeinformationen die Citrix Virtual Apps and Desktops-Downloadseite auf. Laden Sie die ISO-Datei für das Produkt herunter.

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

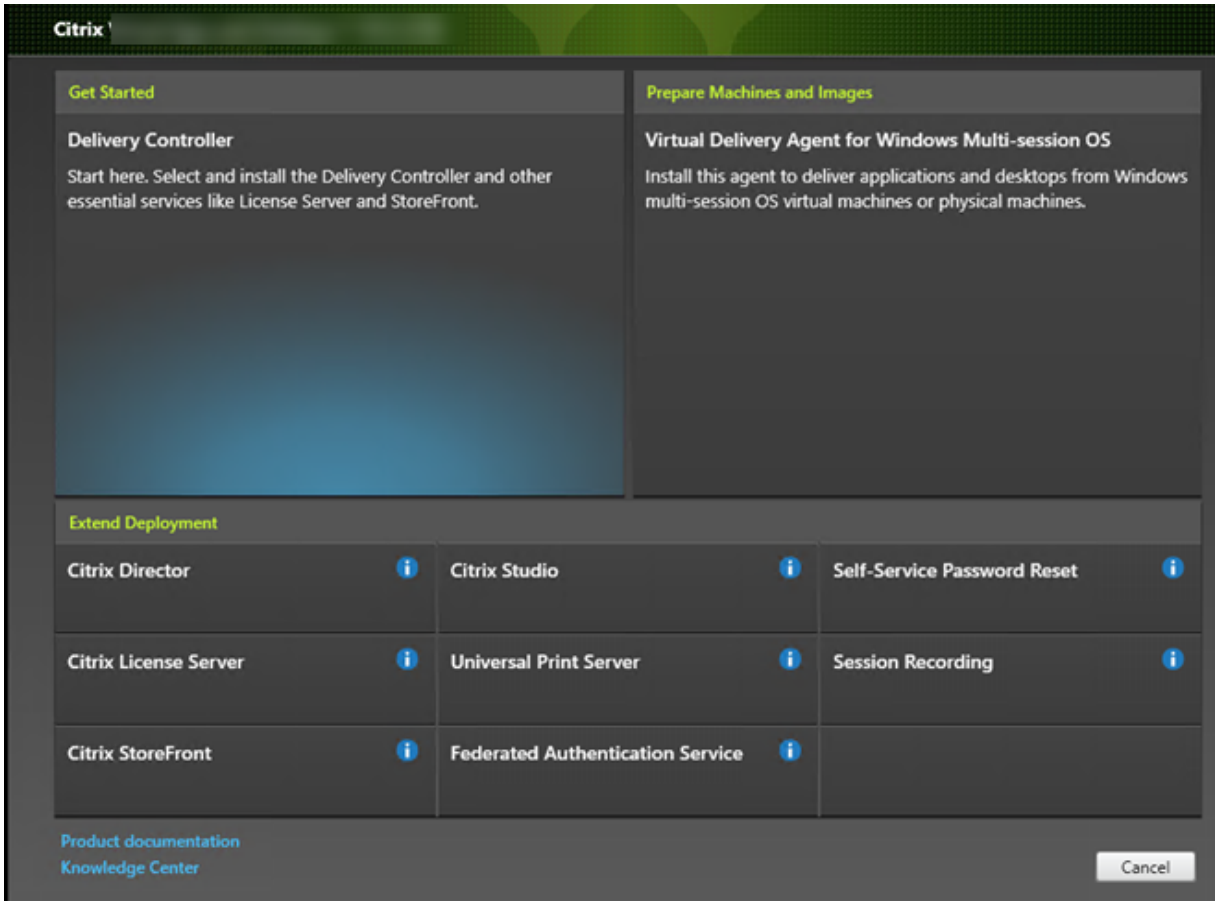


Klicken Sie auf **Start** neben dem zu installierenden Produkt: Virtual Apps oder Virtual Apps and Desktops.

(Wenn auf der Maschine bereits Citrix Virtual Apps and Desktops-Komponenten installiert sind, wird diese Seite nicht angezeigt.)

Befehlszeilenoption: /xenapp zur Installation von Citrix Virtual Apps; Citrix Virtual Apps and Desktops wird installiert, wenn die Option ausgelassen wird.

Schritt 3. Auswählen der zu installierenden Komponente

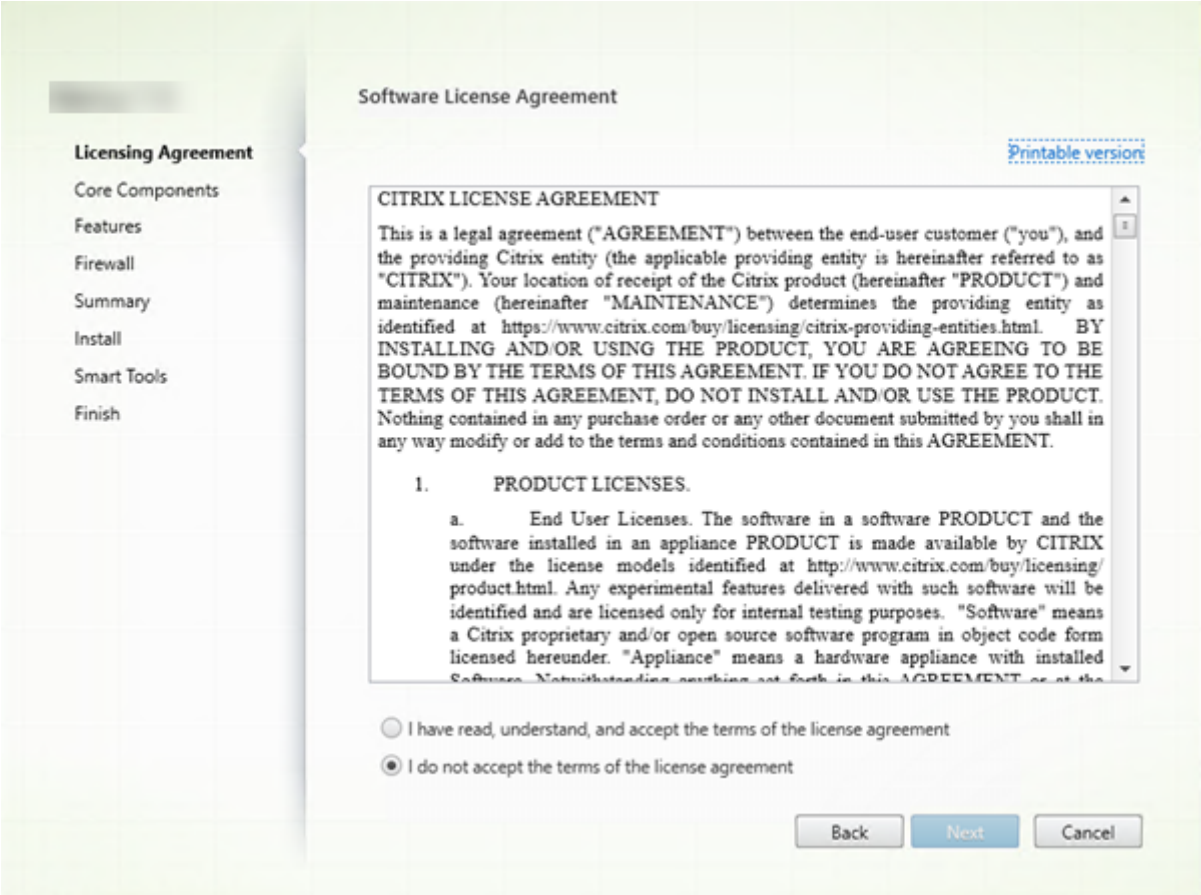


Wenn Sie ganz zu Beginn der Installation stehen, wählen Sie **Delivery Controller**. (Später wählen Sie die spezifischen Komponenten aus, die Sie auf dieser Maschine installieren.)

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.

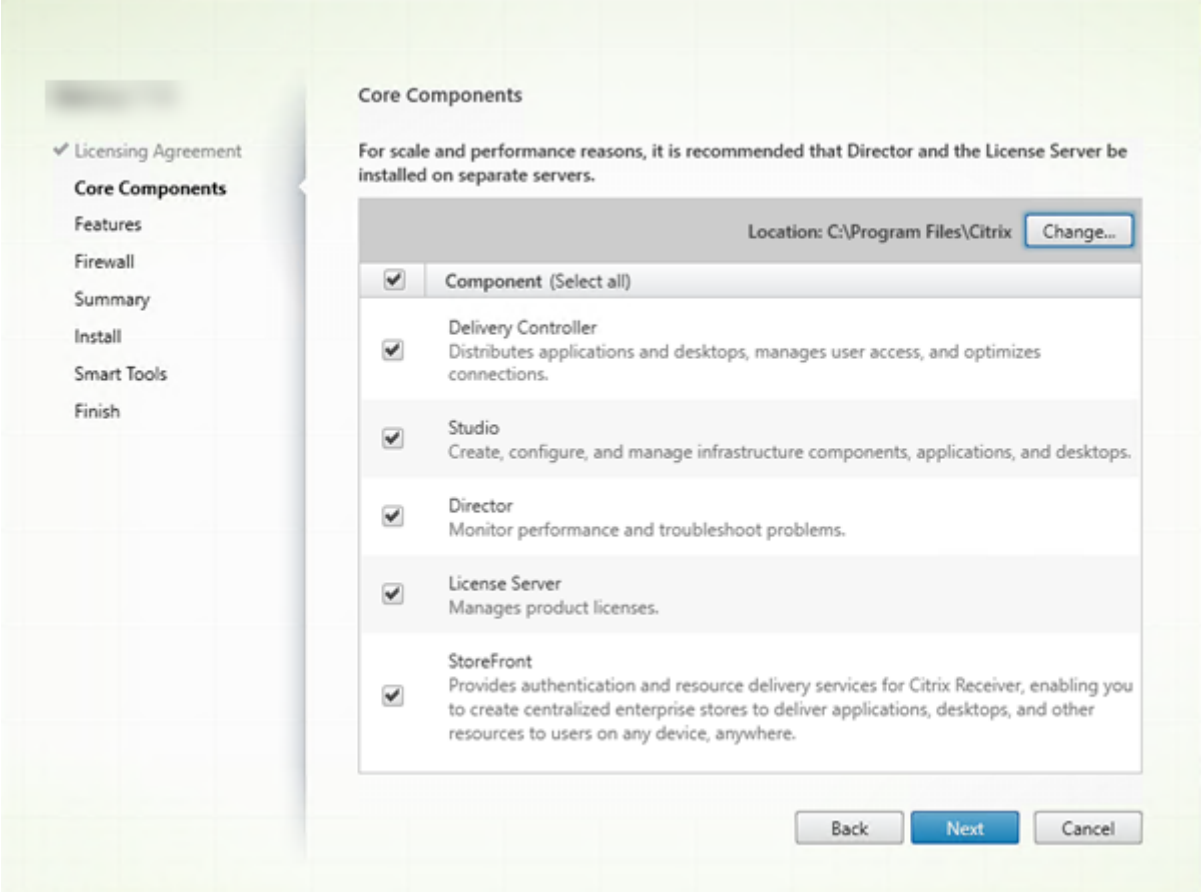
Befehlszeilenoption: `/components`

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**.

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. 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`

Hardwareprüfung

Wenn Sie einen Delivery Controller installieren oder aktualisieren, wird die Hardware überprüft. Das Installationsprogramm benachrichtigt Sie, wenn die Maschine weniger als die empfohlene RAM-Größe hat (5 GB), was sich auf die Stabilität der Site auswirken kann. (Weitere Informationen finden Sie unter Hardwareanforderungen.)

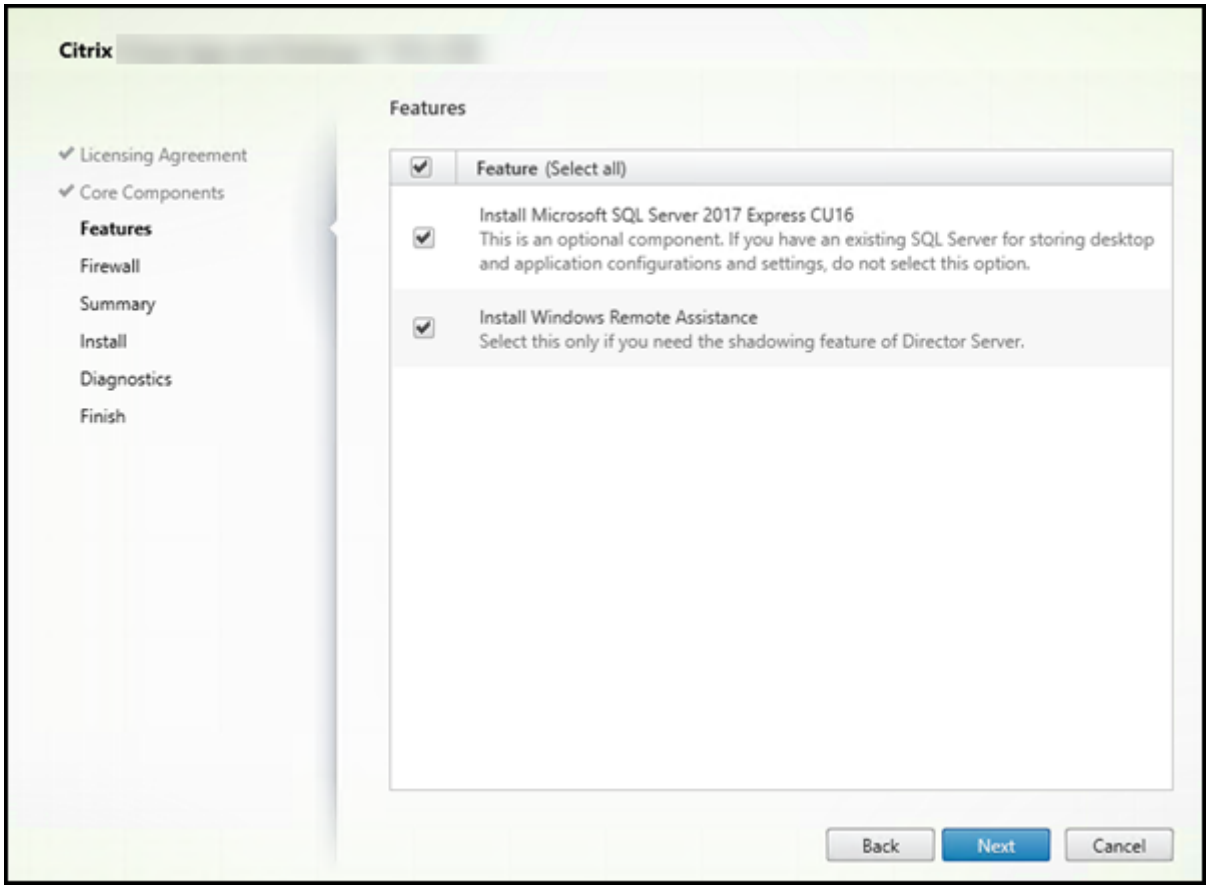
Grafische Oberfläche: Ein Dialogfeld wird angezeigt.

- Empfohlen: Klicken Sie auf **Abbrechen**, um die Installation abzubrechen. Installieren Sie mehr RAM auf der Maschine und starten Sie die Installation erneut.
- Sie können auch auf **Weiter** klicken, um mit der Installation fortzufahren. Die Site kann dann Stabilitätsprobleme haben.

Befehlszeilenschnittstelle: Die Installation bzw. das Upgrade endet. Die Installationsprotokolle enthalten eine Meldung über den Befund und die verfügbaren Optionen.

- Empfohlen: Installieren Sie mehr RAM und führen Sie den Befehl erneut aus.
- Alternativ können Sie den Befehl erneut mit der Option /`ignore_hw_check_failure` zum Ignorieren der Warnung ausführen. Die Site kann dann Stabilitätsprobleme haben.

Schritt 6. Aktivieren oder Deaktivieren von Features



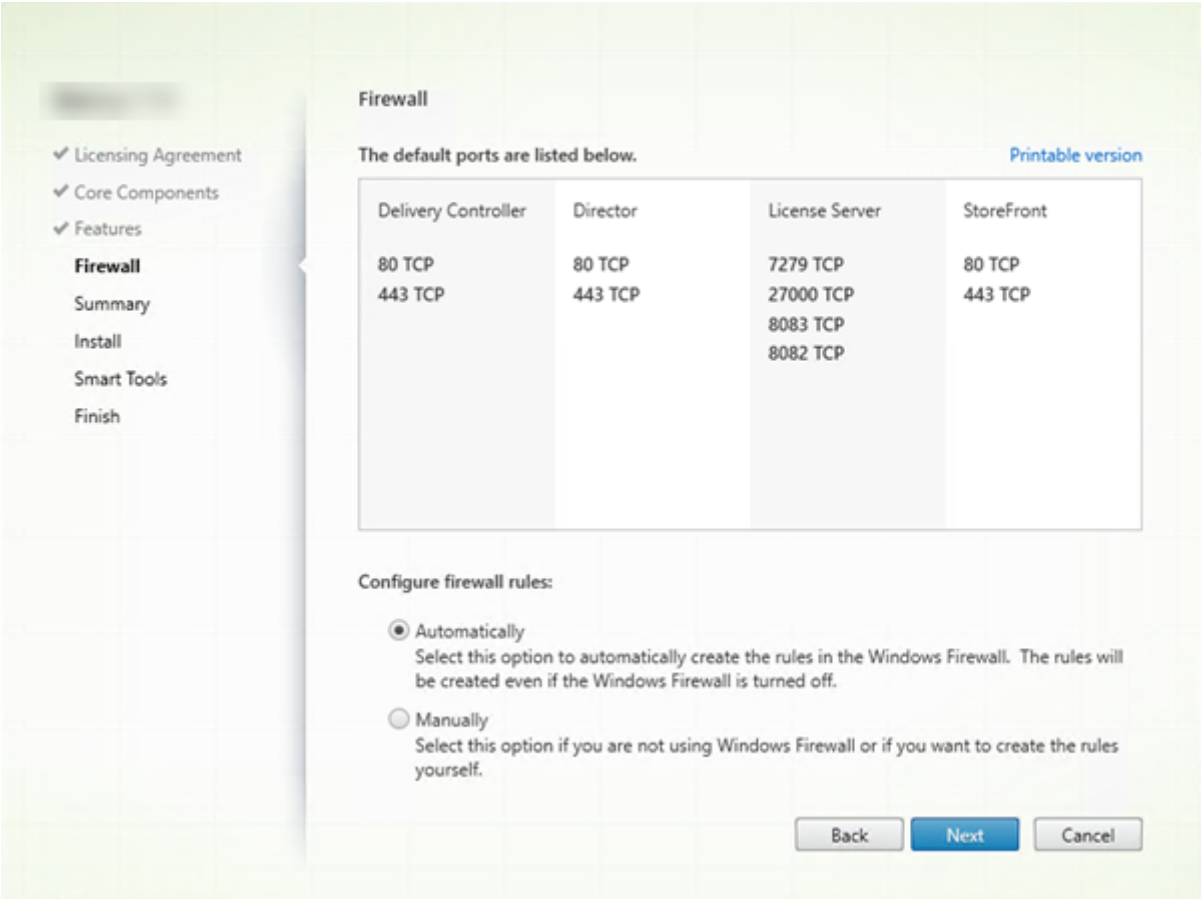
Auf der Seite **Features**:

- Wählen Sie aus, ob Microsoft SQL Server Express zur Verwendung als Sitedatenbank installiert werden soll. Diese Option ist standardmäßig aktiviert. Weitere Informationen zu den Datenbanken von Citrix Virtual Apps and Desktops finden Sie 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. Öffnen von Windows-Firewallports



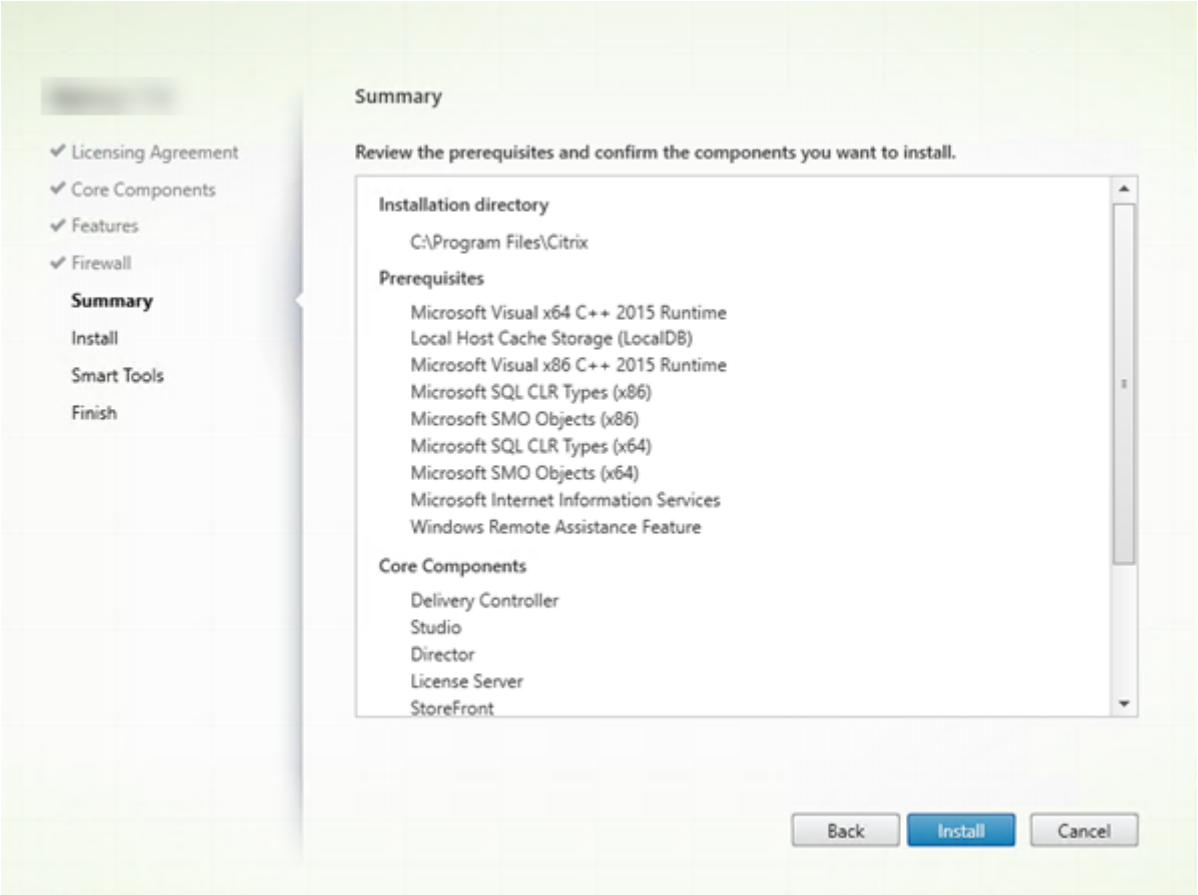
Standardmäßig werden die Ports auf der Seite **Firewall** automatisch geöffnet, wenn der Windows-Firewalldienst ausgeführt wird, selbst wenn die Firewall nicht aktiviert ist. Die Standardeinstellung ist für die meisten Bereitstellungen geeignet. Weitere Informationen zu Ports finden Sie unter Netzwerkports.

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`

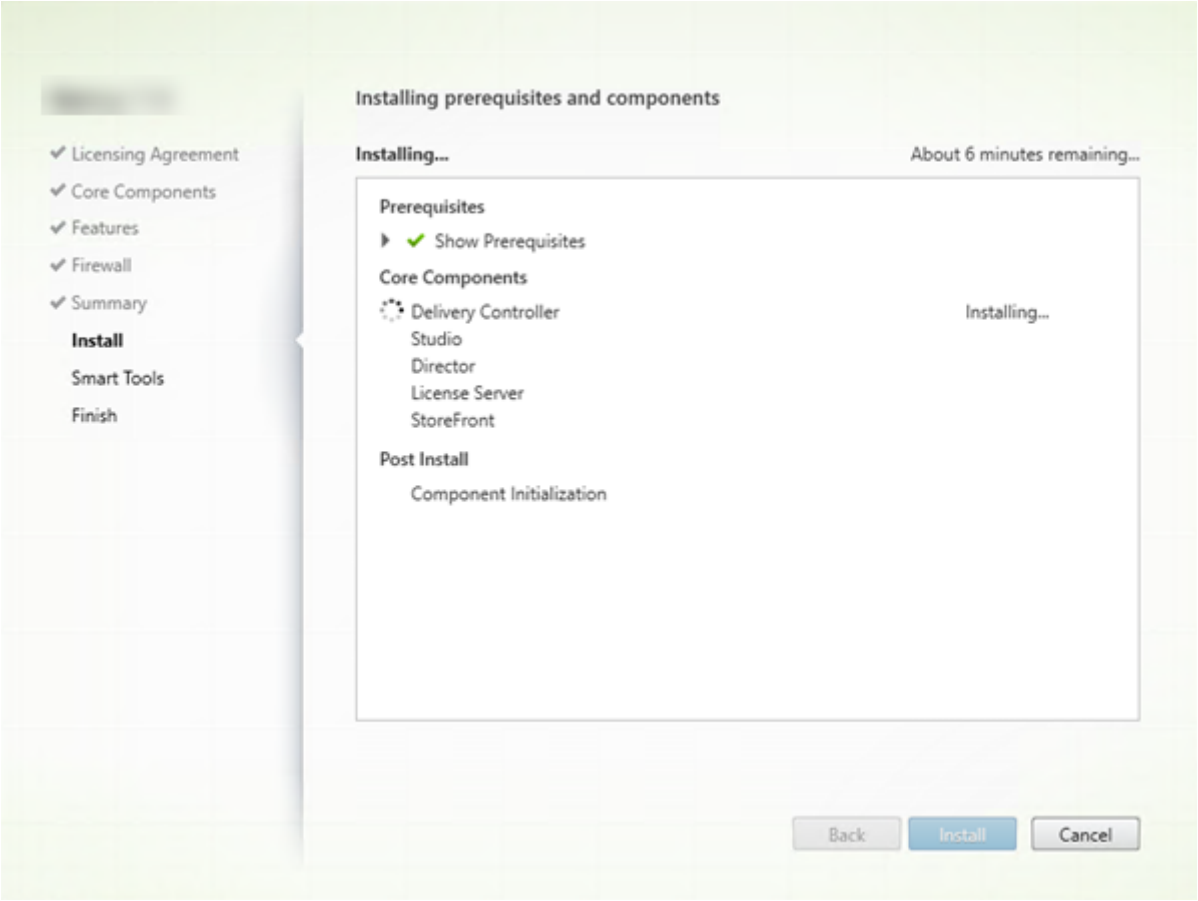
Schritt 8. Überprüfen der Voraussetzungen und Bestätigen der Installation



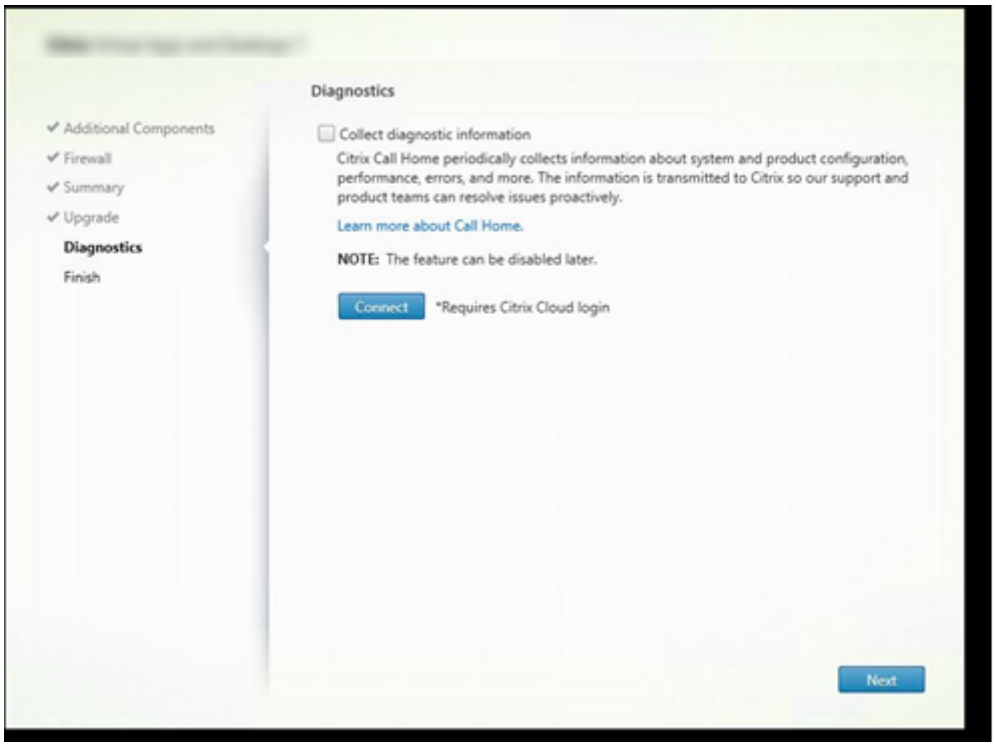
Auf der Seite **Zusammenfassung** wird aufgelistet, was installiert wird. Sie können mit der Schaltfläche Zurück zu vorherigen Seiten zurückkehren und Ihre Auswahl ändern.

Wenn Sie fertig sind, klicken Sie auf **Installieren**.

Der Fortschritt der Installation wird angezeigt.



Schritt 9. Diagnose



Geben Sie auf der Seite **Diagnose** an, ob Sie bei Citrix Call Home teilnehmen möchten.

Diese Seite wird angezeigt, wenn Sie einen Delivery Controller über die grafische Benutzeroberfläche installieren. Wenn Sie StoreFront (jedoch keinen Controller) installieren, zeigt der Assistent diese Seite an. Wenn Sie andere Kernkomponenten als StoreFront und Controller installieren, wird diese Seite nicht angezeigt.

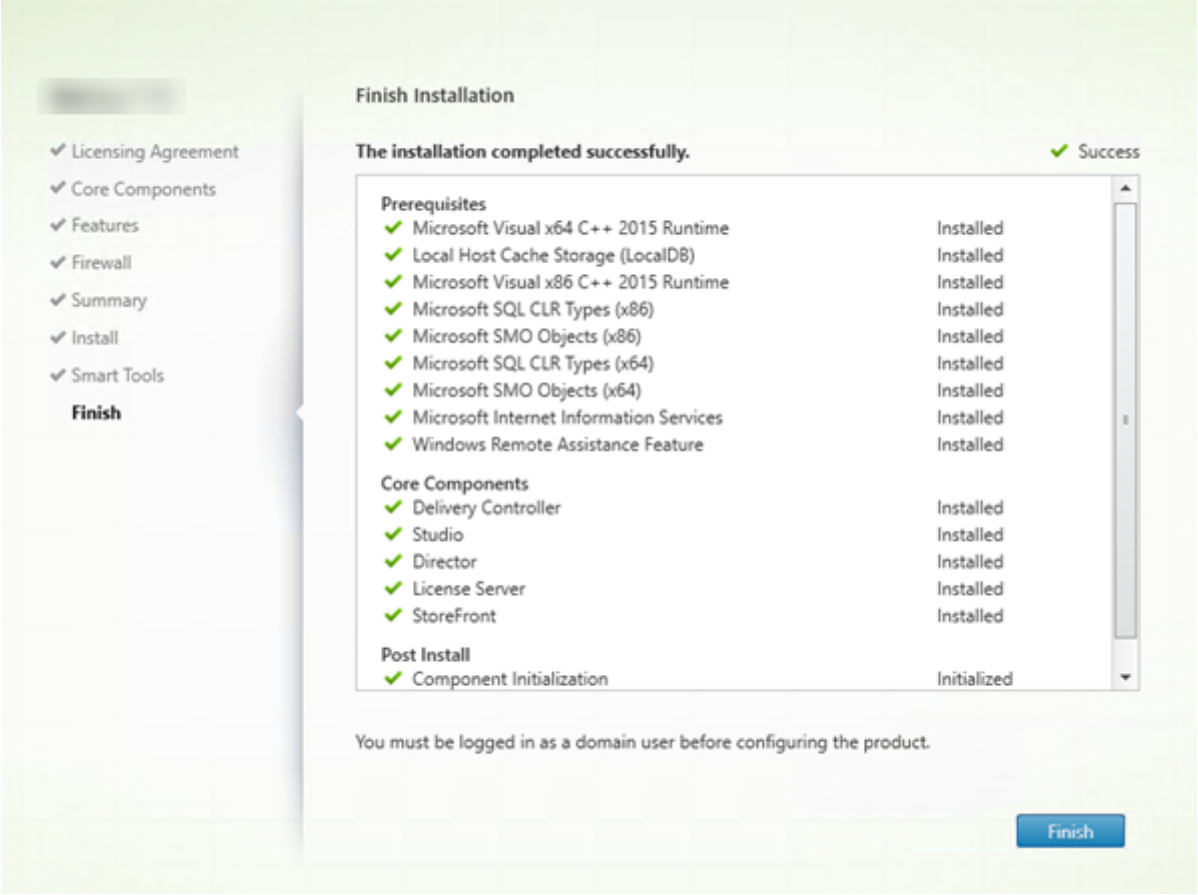
Während eines Upgrades wird diese Seite nicht angezeigt, wenn Call Home bereits aktiviert ist oder wenn das Installationsprogramm einen Fehler im Zusammenhang mit dem Citrix Telemetriedienst findet.

Wenn Sie teilnehmen möchten (Standardeinstellung), klicken Sie auf **Verbinden**. Geben Sie nach Aufforderung die Anmeldeinformationen Ihres Citrix-Kontos ein. (Sie können die Registrierungsauswahl nach der Installation ändern.)

Wenn Ihre Anmeldeinformationen überprüft sind (bzw. wenn Sie nicht teilnehmen), klicken Sie auf **Weiter**.

Weitere Informationen finden Sie unter Call Home.

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. Standardmäßig sind auf der Seite **Firewall** die TCP-Ports 7229 und 8080 in der Firewall geöffnet, wenn der Windows-Firewalldienst ausgeführt wird, selbst wenn die Firewall nicht aktiviert ist. Sie können die Standardaktion deaktivieren, wenn Sie die Ports manuell öffnen möchten.

  Anweisungen zum Installieren dieser Komponente über die Befehlszeile finden Sie unter Installieren über die Befehlszeile.
- Verbundauthentifizierungsdienst.
- Self-Service-Kennwortzurücksetzung.
- Sitzungsaufzeichnung.

VDAs installieren

November 14, 2022

> **Wichtig:**
>
> Bei Updates von VDAs mit persönlicher vDisk (PvD) lesen Sie die Informationen unter Upgrade von VDAs auf 1912 oder höher.

Es gibt zwei VDA-Typen für Windows-Maschinen: VDAs für Einzelsitzungs-OS und VDAs für Multisitzungs-OS. Informationen zu VDAs für Linux-Maschinen finden Sie in der Dokumentation zu Linux Virtual Delivery Agent.

Vor dem Start einer Installation lesen Sie Vorbereiten der Installation, und führen Sie alle notwendigen Vorbereitungsschritte aus.

Vor der Installation von VDAs müssen Sie die Kernkomponenten installieren. Sie können auch die Site erstellen, bevor Sie die VDAs installieren.

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.

Schritt 1. Produktsoftware herunterlade und Assistent starten

Produktinstallationsprogramm verwenden:

1. Wenn Sie die Produkt-ISO-Datei noch nicht heruntergeladen haben:

    - Rufen Sie unter Angabe Ihrer Citrix Anmeldeinformationen die Citrix Virtual Apps and Desktops-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.

2. 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:

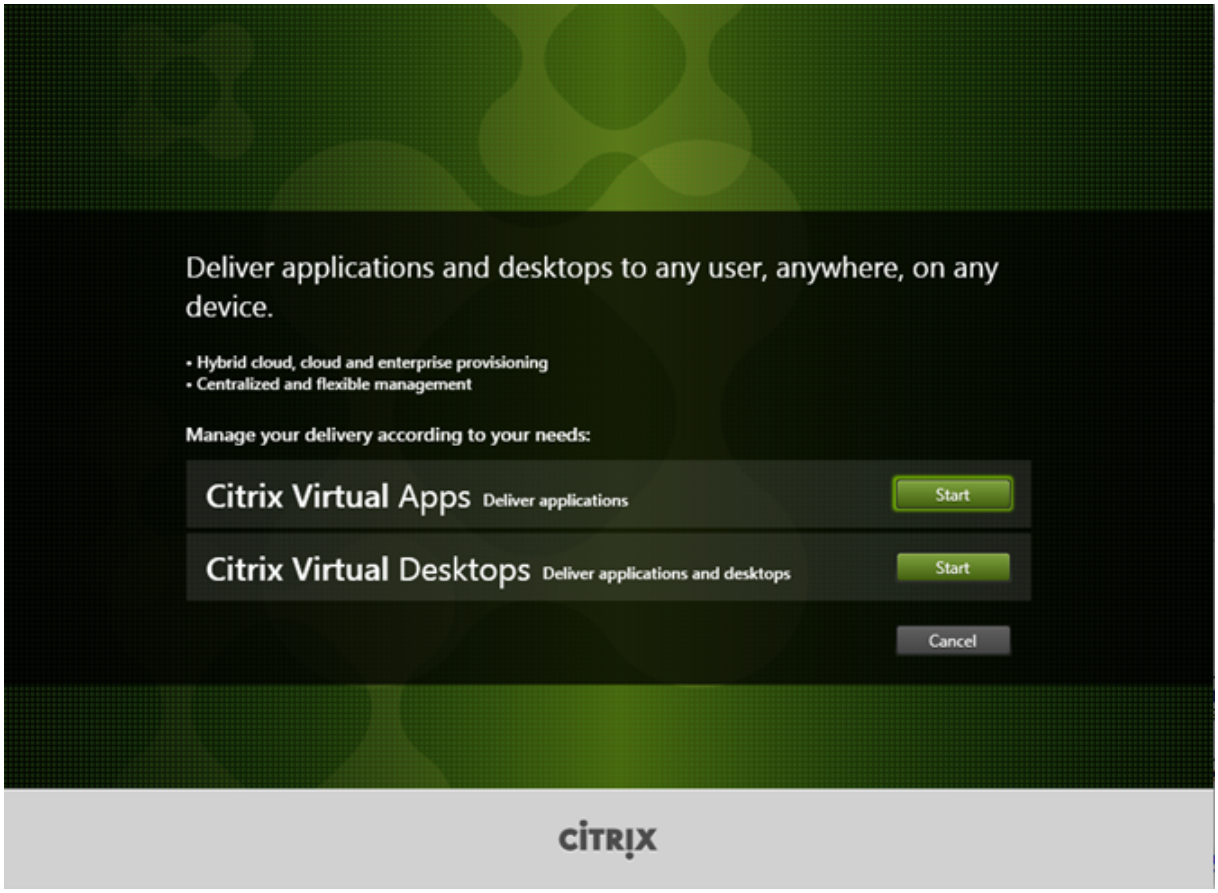
1. Rufen Sie unter Angabe Ihrer Citrix Anmeldeinformationen die Citrix Virtual Apps and Desktops-Downloadseite auf. Laden Sie das benötigte Paket:

    - VDAServerSetup.exe: VDA für Multisitzungs-OS *Version*
    - VDAWorkstationSetup.exe: VDA für Einzelsitzungs-OS *Version*
    - VDAWorkstationCoreSetup.exe: Kernkomponenten-VDA für Einzelsitzungs-OS *Version*

2. Klicken Sie mit der rechten Maustaste auf das Paket und wählen Sie **Als Administrator ausführen**.

    Der Installationsassistent wird gestartet.

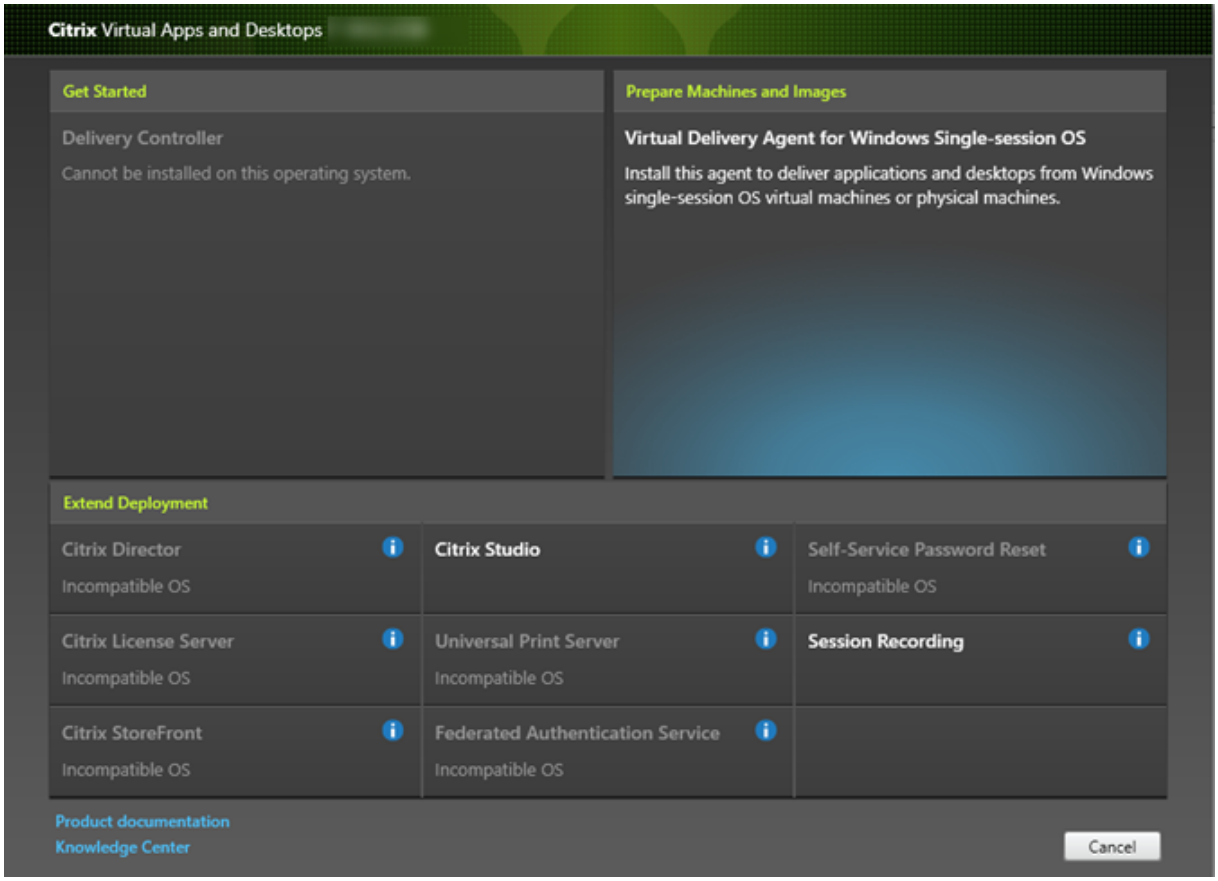
Schritt 2. Zu installierendes Produkt auswählen



Klicken Sie auf **Start** neben dem zu installierenden Produkt: Citrix Virtual Apps oder Citrix Virtual Desktops. (Wenn auf der Maschine bereits eine Citrix Virtual Apps- oder Citrix Virtual Desktops-Komponente installiert ist, wird diese Seite nicht angezeigt.)

Befehlszeilenoption: /xenapp zum Installieren von Citrix Virtual Apps. Wenn diese Option ausgelassen wird, wird Citrix Virtual Desktops installiert.

Schritt 3. VDA auswählen

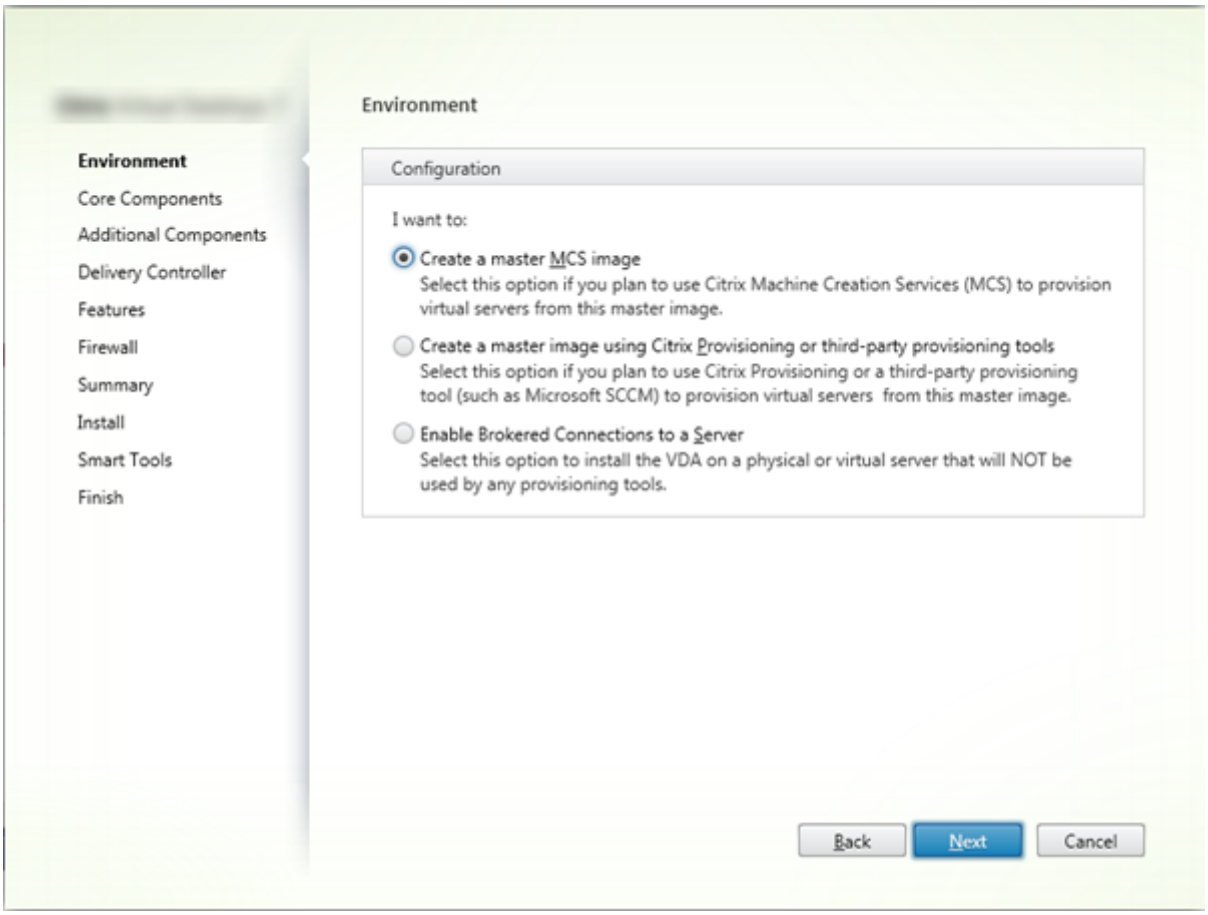


Wählen Sie den Eintrag **Virtual Delivery Agent**. Das Installationsprogramm weiß, ob ein VDA unter einem Einzel- oder Multisitzungs-OS ausgeführt wird, und bietet daher nur einen VDA des richtigen Typs an.

Wenn das Installationsprogramm beispielsweise auf einer Windows Server 2016-Maschine ausgeführt wird, wird der VDA für Windows-Multisitzungs-OS angeboten. Der VDA für Einzelsitzungs-OS ist nicht verfügbar.

Wenn Sie versuchen, einen Windows-VDA unter einem für diese Citrix Virtual Apps and Desktops-Version nicht unterstützten Betriebssystem zu installieren (bzw. ein VDA-Upgrade auszuführen) werden Sie durch eine Meldung zu Informationen über Ihre Optionen geleitet.

Schritt 4. Art der VDA-Verwendung angeben



Geben Sie auf der Seite **Umgebung** an, wie Sie den VDA verwenden werden und ob Sie die Maschine als Masterimage für das Provisioning von zusätzlichen Maschinen verwenden möchten.
Je nach gewählter Option werden dann Citrix Bereitstellungstools installiert (falls notwendig) und die Standardwerte auf der Seite "Zusätzliche Komponenten"im VDA-Installationsprogramm festgelegt.
Bei der Installation eines VDAs werden mehrere MSIs (Provisioning- und andere) automatisch installiert. Die einzige Möglichkeit, ihre Installation zu verhindern, ist die Befehlszeileninstallation mit der Option `/exclude`. Weitere Informationen finden Sie unter Installieren an der Befehlszeile.

Wählen Sie eine der folgenden Optionen:

- **MCS-Masterimage erstellen:** Wählen Sie diese Option, um einen VDA auf einem VM-Masterimage zu installieren, wenn Sie Maschinenerstellungsdienste zur Bereitstellung von VMs verwenden möchten. Mit dieser Option wird der Maschinenidentitätsdienst installiert, der TargetOSOptimizer.exe enthält. Dies ist die Standardoption. Befehlszeilenoption: `/mastermcsimage` oder `/masterimage`
- **Erstellen Sie ein Masterimage mit Citrix Provisioning oder Bereitstellungsprogrammen von Drittanbietern:** Wählen Sie diese Option, um einen VDA auf einem VM-Master-Image zu installieren, wenn Sie entweder Citrix Provisioning oder eine Drittanbieteranwendung (z. B.

Microsoft System Center Configuration Manager) für das Provisioning von VMs verwenden möchten. Befehlszeilenoption: `/masterpvsimage`

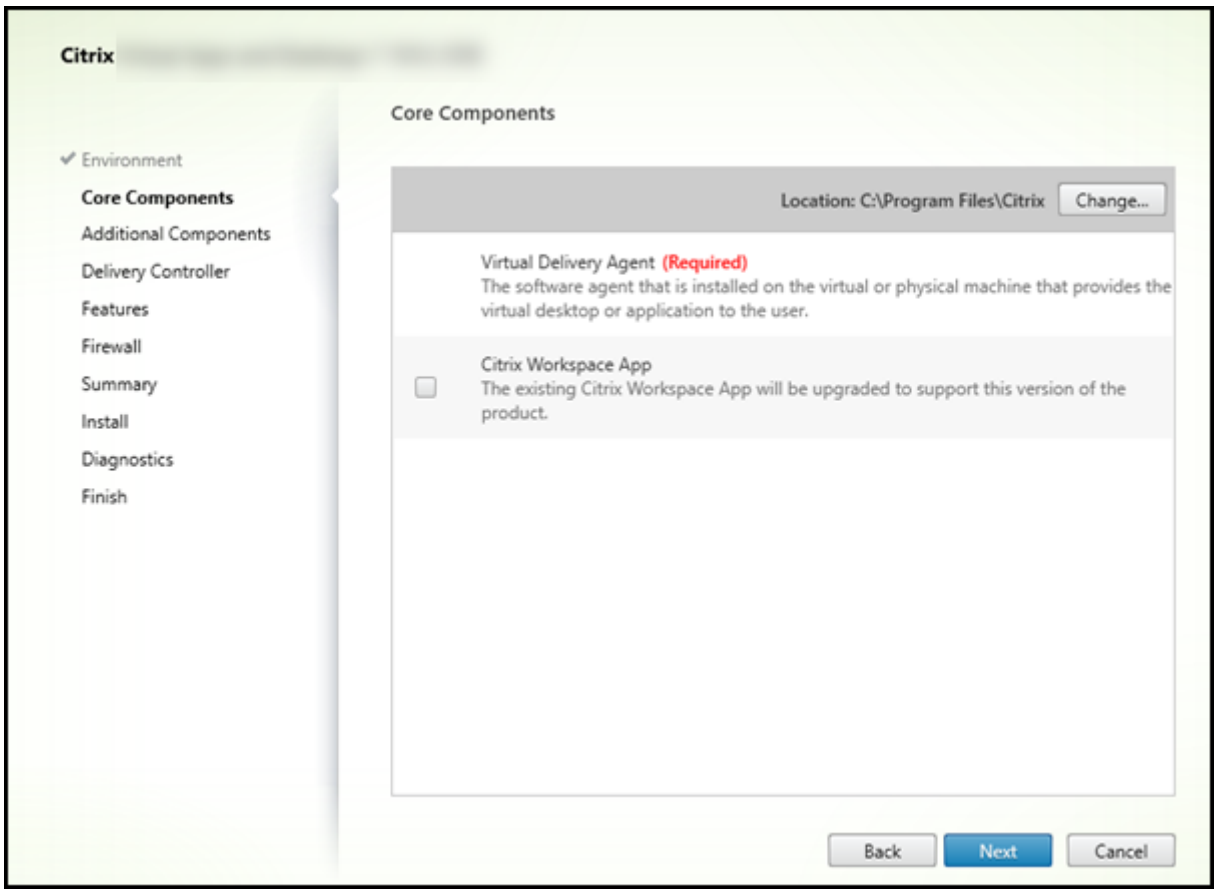
- (Wird nur auf Maschinen mit Multisitzungs-OS angezeigt) **Vermittelte Verbindungen zu einem Server aktivieren:** Wählen Sie diese Option, um einen VDA auf einer physischen oder virtuellen Maschine zu installieren, die nicht als Masterimage für das Provisioning von anderen Maschinen verwendet werden soll. Befehlszeilenoption: `/remotepc`
- (Wird nur auf Maschinen mit Einzelsitzungs-OS angezeigt.) **Remote-PC-Zugriff aktivieren:** Wählen Sie diese Option, um einen VDA auf einer physischen Maschine zur Verwendung mit Remote-PC-Zugriff zu installieren. Befehlszeilenoption: `/remotepc`

Klicken Sie auf **Weiter**.

Die Seite wird in folgenden Fällen nicht angezeigt:

- Bei VDA-Upgrades
- Bei Verwendung des Installationsprogramms `VDAWorkstationCoreSetup.exe`

Schritt 5. Auswählen der Komponenten und des Speicherorts für die Installation



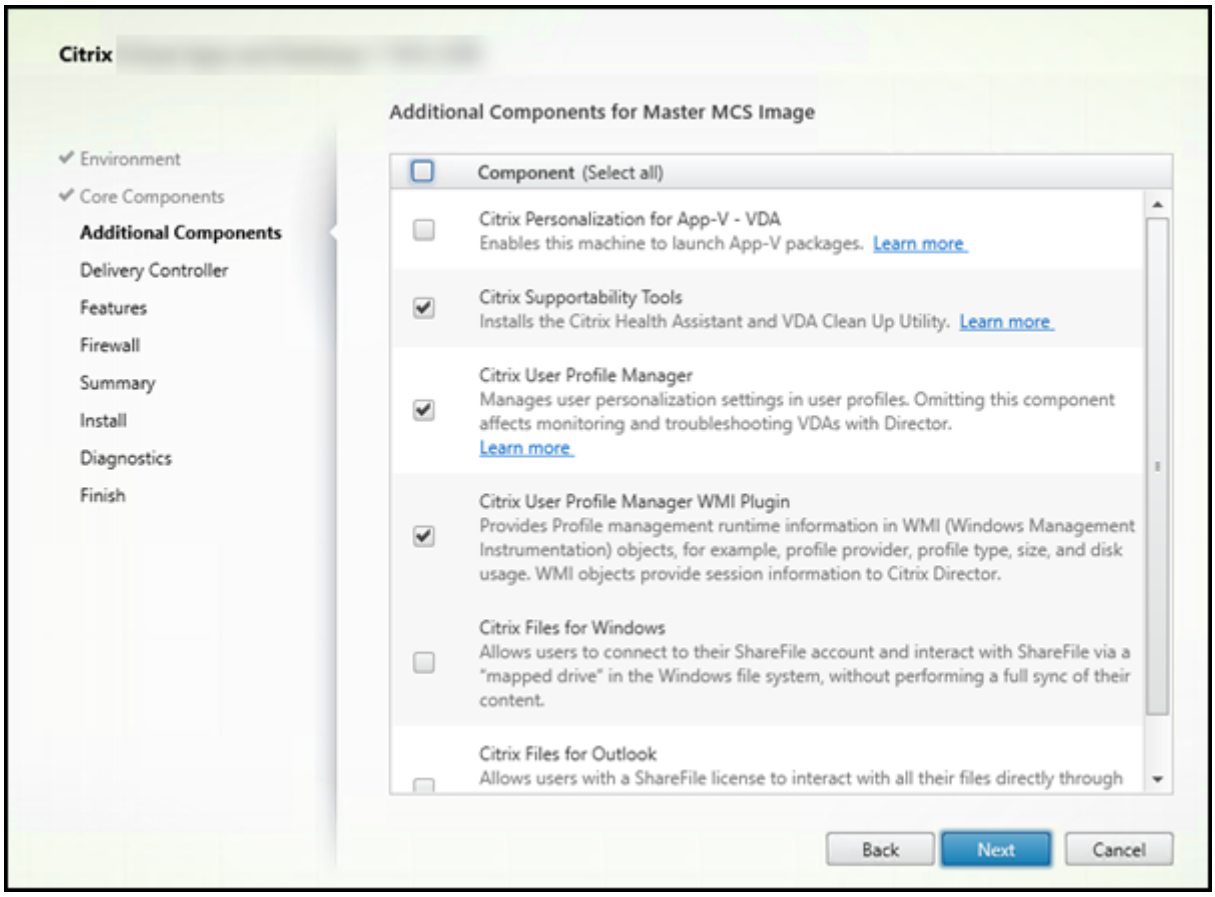
Treffen Sie auf der Seite **Kernkomponenten** folgende Auswahl:

- **Speicherort:** Standardmäßig werden die Komponenten in C:\Programme\Citrix installiert. 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:** Standardmäßig wird die Citrix Workspace-App für Windows nicht mit dem VDA installiert. Wenn Sie das Installationsprogramm VDAWorkstationCoreSetup.exe verwenden, wird die Citrix Workspace-App für Windows nie installiert, daher wird dieses Kontrollkästchen nicht angezeigt.

Klicken Sie auf **Weiter**.

Befehlszeilenoptionen: `/installdir`, `/components vda plugin` zum Installieren des VDAs und der Citrix Workspace-App für Windows

Schritt 6. Installation zusätzlicher Komponenten



Die Seite **Zusätzliche Komponenten** enthält Kontrollkästchen zum Aktivieren oder Deaktivieren der Installation weiterer Features und Technologien mit dem VDA. Bei einer Befehlszeileninstallation können Sie die Option "/exclude"oder "/includeaddition"verwenden, um Komponenten ausdrücklich aus- oder einzuschließen.

In der Tabelle unten werden die Standardeinstellungen der Elemente auf dieser Seite aufgeführt. Die jeweilige Standardeinstellung hängt von der auf der Seite Umgebung ausgewählten Option ab.

Seite "Zusätzliche Komponenten"	Seite "Umgebung": "Masterimage mit MCS"oder "Masterimage mit Citrix Provisioning"ausgewählt	Seite "Umgebung": "Vermittelte Verbindungen zu einem Server aktivieren" (Windows-Multisitzungs-OS) oder "Remote-PC-Zugriff" (Windows-Einzelsitzungs-OS) ausgewählt
Citrix Personalisierung für App-V	Nicht ausgewählt	Nicht ausgewählt
Benutzerpersonalisierungslayer	Nicht ausgewählt	Nicht angezeigt, da für diesen Anwendungsfall nicht gültig
Citrix Supportability Tools	Ausgewählt	Nicht ausgewählt
Citrix User Profile Manager	Ausgewählt	Nicht ausgewählt
Citrix User Profile Manager WMI Plug-In	Ausgewählt	Nicht ausgewählt
Citrix Files für Windows	Nicht ausgewählt	Nicht ausgewählt
Citrix Files für Outlook	Nicht ausgewählt	Nicht ausgewählt

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.)

Aktivieren oder deaktivieren Sie die folgenden Kontrollkästchen:

- **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: `/includeadditional "Citrix Personalization for App-V – VDA"`, um die Komponenteninstallation zu aktivieren, `/exclude "Citrix Personalization for App-V – VDA"`, um die Komponenteninstallation zu verhindern

- **Benutzerpersonalisierungslayer:** Installiert das MSI für den Benutzerpersonalisierungslayer. Weitere Informationen finden Sie unter Benutzerpersonalisierungslayer.

Diese Komponente wird nur angezeigt, wenn ein VDA auf einer Maschine mit Windows 10-Einzelsitzungs-OS installiert wird.

Die Benutzerpersonalisierungslayer-Technologie kann nicht mit PvD und AppDisk koexistieren.

- Für Neuinstallationen sind die Komponenten PvD und AppDisk nicht verfügbar.
- Upgrades:
  - Ist PvD/AppDisk oder ein Benutzerpersonalisierungslayer bereits installiert und das Installationsmedium enthält eine neuere Version der installierten Komponente, wird die installierte Komponente aktualisiert.
  - Ist PvD/AppDisk bereits installiert und das Installationsmedium enthält keine neuere PvD/AppDisk-Version, kann der Benutzerpersonalisierungslayer zur Installation ausgewählt werden.
  - Ist weder PvD/AppDisk noch der Benutzerpersonalisierungslayer installiert, wird der Benutzerpersonalisierungslayer installiert.

Befehlszeilenoption: `/includeadditional "User Personalization Layer"`, um die Komponenteninstallation zu aktivieren, `/exclude "User Personalization Layer"`, um die Komponenteninstallation zu verhindern

- **Citrix Supportability Tools:** installiert die MSI mit Unterstützbarkeitstools wie z. B. Citrix Health Assistant.

  Befehlszeilenoption: `/includeadditional "Citrix Supportability Tools"`, um die Komponenteninstallation zu aktivieren, `/exclude "Citrix Supportability Tools"`, um die Komponenteninstallation zu verhindern

- **Citrix User Profile Manager:** 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 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.

  Befehlszeilenoption: `/includeadditional "Citrix User Profile Manager"`, um die Komponenteninstallation zu aktivieren, `/exclude "Citrix User Profile Manager"`, um die Komponenteninstallation zu verhindern

- **Citrix User Profile Manager 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: `/includeadditional "Citrix User Profile Manager WMI Plugin"`, um die Komponenteninstallation zu aktivieren, `/exclude "Citrix User Profile Manager WMI Plugin"`, um die Komponenteninstallation zu verhindern

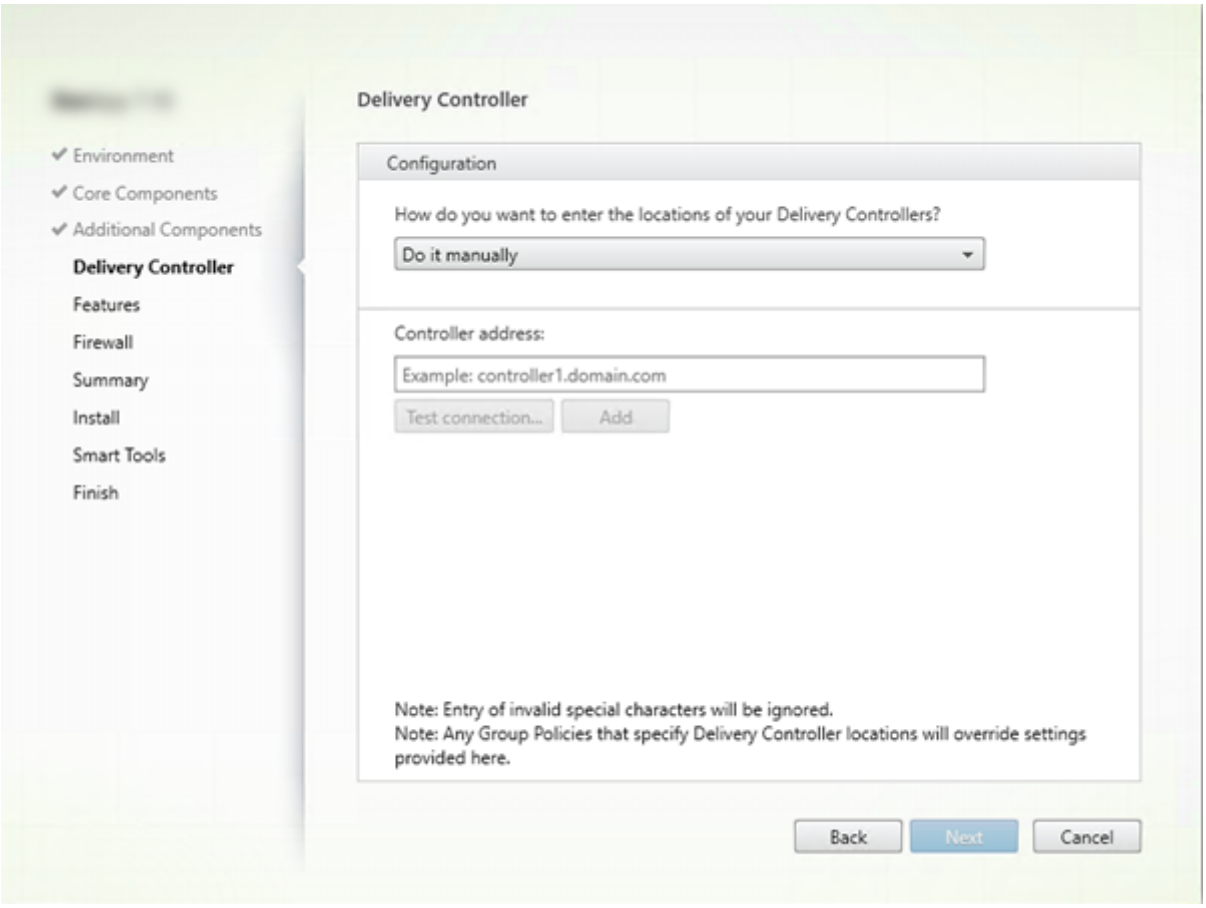
- **Citrix Files für Windows:** Mit dieser Komponente können Benutzer eine Verbindung mit ihrem Citrix Files-Konto herstellen. Sie können dann über ein zugeordnetes Laufwerk im Windows-Dateisystem ohne Erfordernis einer vollständigen Synchronisierung ihrer Inhalte mit Citrix Files interagieren.

  Befehlszeilenoptionen: `/includeadditional "Citrix Files for Windows"` um die Komponenteninstallation zu aktivieren, `/exclude "Citrix Files for Windows"` um die Komponenteninstallation zu verhindern

- **Citrix Files für Outlook:** Mit Citrix Files für Outlook können Sie Dateigrößenbeschränkungen umgehen und Ihre Anlagen oder E-Mails sicherer versenden. Sie können für Mitarbeiter, Kunden und Partner direkt in Ihrer E-Mail eine Anfrage für sicheren Dateiupload bereitstellen. Weitere Informationen finden Sie unter Citrix Files für Outlook.

  Befehlszeilenoptionen: `/includeadditional "Citrix Files for Outlook"` um die Komponenteninstallation zu aktivieren, `/exclude "Citrix Files for Outlook"` um die Komponenteninstallation zu verhindern

Schritt 7. 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:** (Standardeinstellung) 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.

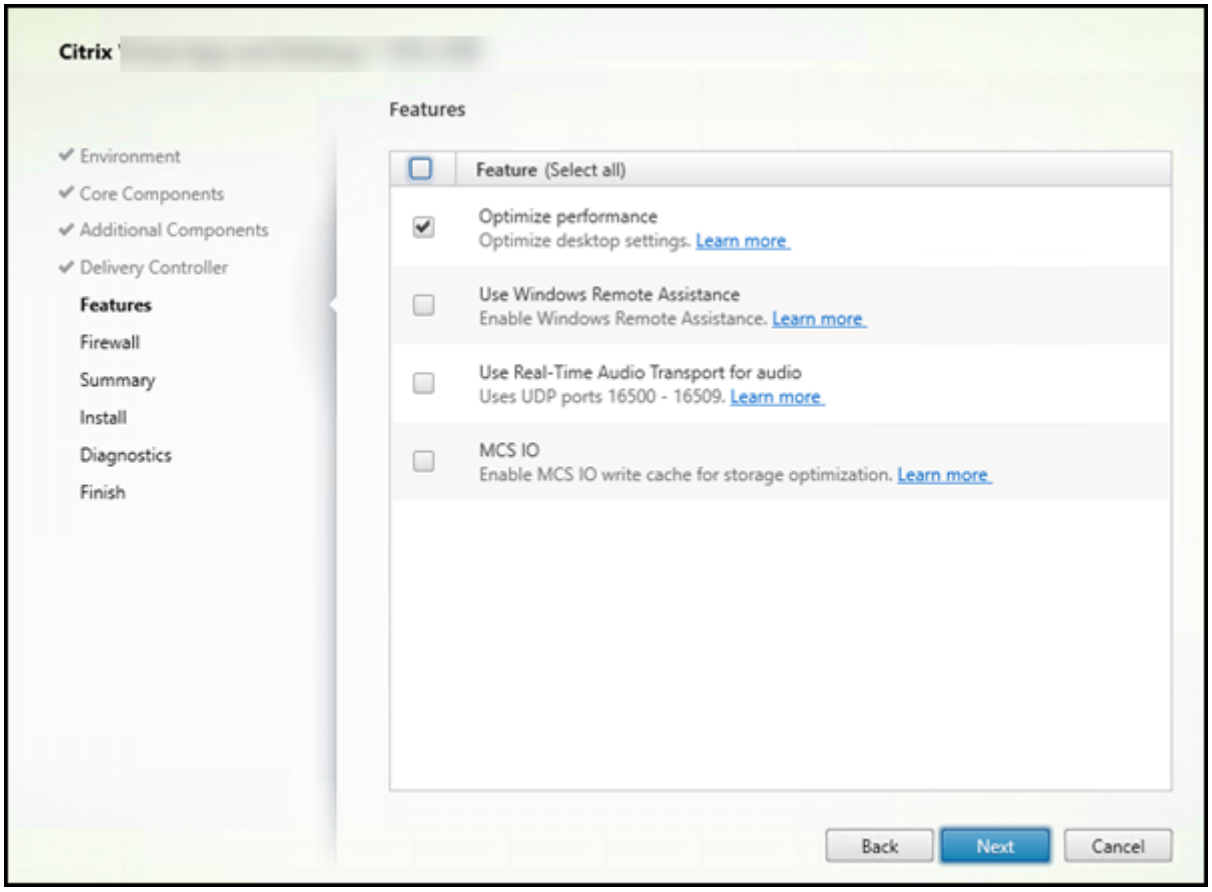
Klicken Sie auf **Weiter**. Wenn Sie "Später (erweitert)"wählen, müssen Sie bestätigen, dass Sie die Controlleradressen später angeben.

Andere Überlegungen

- Die Adresse darf keine nicht alphanumerischen Zeichen 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 VDA-Registrierung.

Befehlszeilenoption: `/controllers`

Schritt 8. 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:** Wenn Sie die Maschinenerstellungsdienste verwenden und dieses Feature aktivieren (Standard), deaktiviert die VM-Optimierung Offlinedateien sowie Hintergrunddefragmentierung und verringert die Größe des Ereignisprotokolls. Einzelheiten finden Sie unter CTX224676.

  Sie müssen die Optimierung aktivieren und zusätzlich den Maschinenidentitätsdienst installieren. Dieser Dienst enthält die Datei `TargetOSOptimizer.exe`. Der Maschinenidentitätsdienst wird automatisch installiert, wenn Sie:

  - Wählen Sie in der grafischen Benutzeroberfläche auf der Seite **Umgebung** die Option **Masterimage erstellen** für MCS.
  - Geben Sie an der Befehlszeilenschnittstelle `/mastermcsimage` oder `/masterimage` an (aber nicht `/exclude "Machine Identity Service"`).

  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)

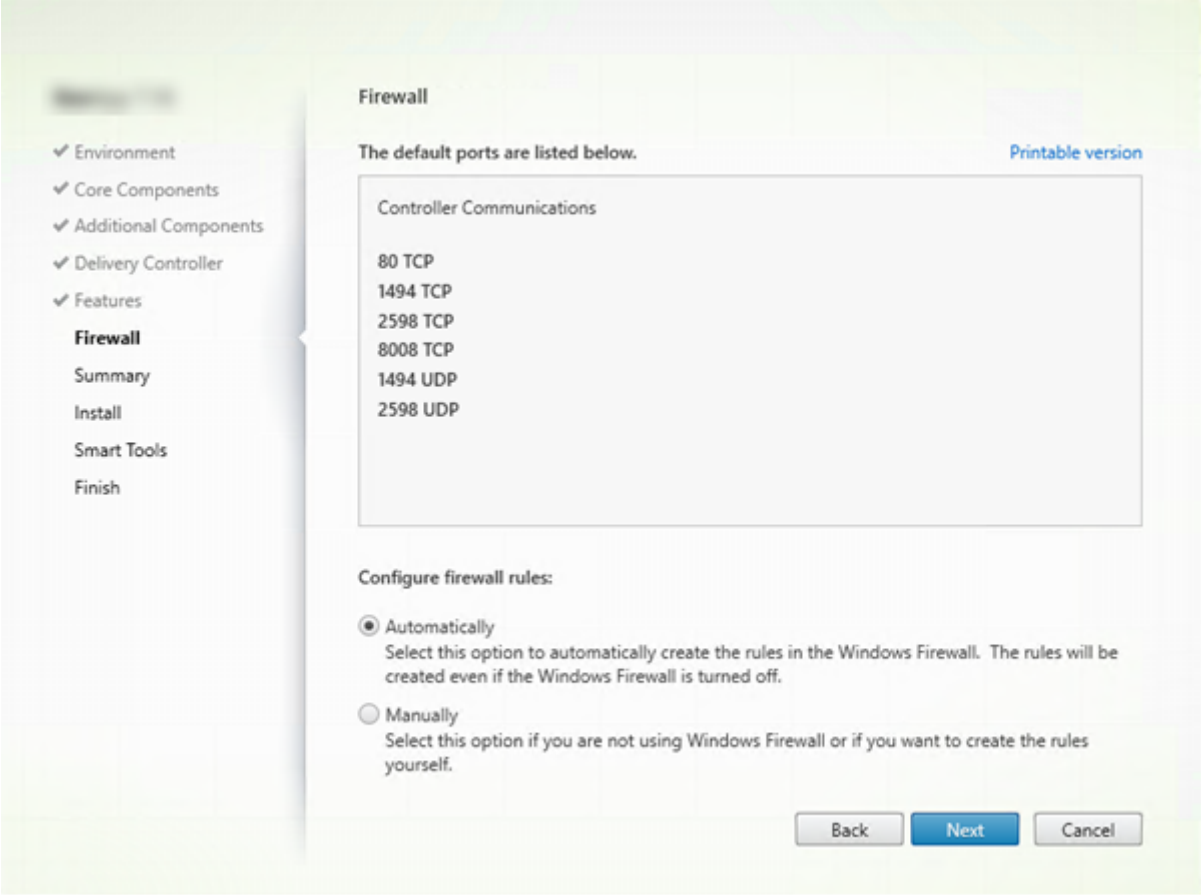
  Befehlszeilenoption: `/enable_real_time_transport`

- **MCS-E/A:** nur gültig, wenn MCS zur Bereitstellung von VMs verwendet wird. Wenn diese Option ausgewählt wird, wird der MCSIO-Schreibcachetreiber installiert. Weitere Informationen finden Sie unter Für Hypervisors freigegebener Speicher und Konfigurieren eines Cache für temporäre Daten.

  Befehlszeilenoption: `/install_mcsio_driver`

Klicken Sie auf **Weiter**.

Schritt 9. Firewallports

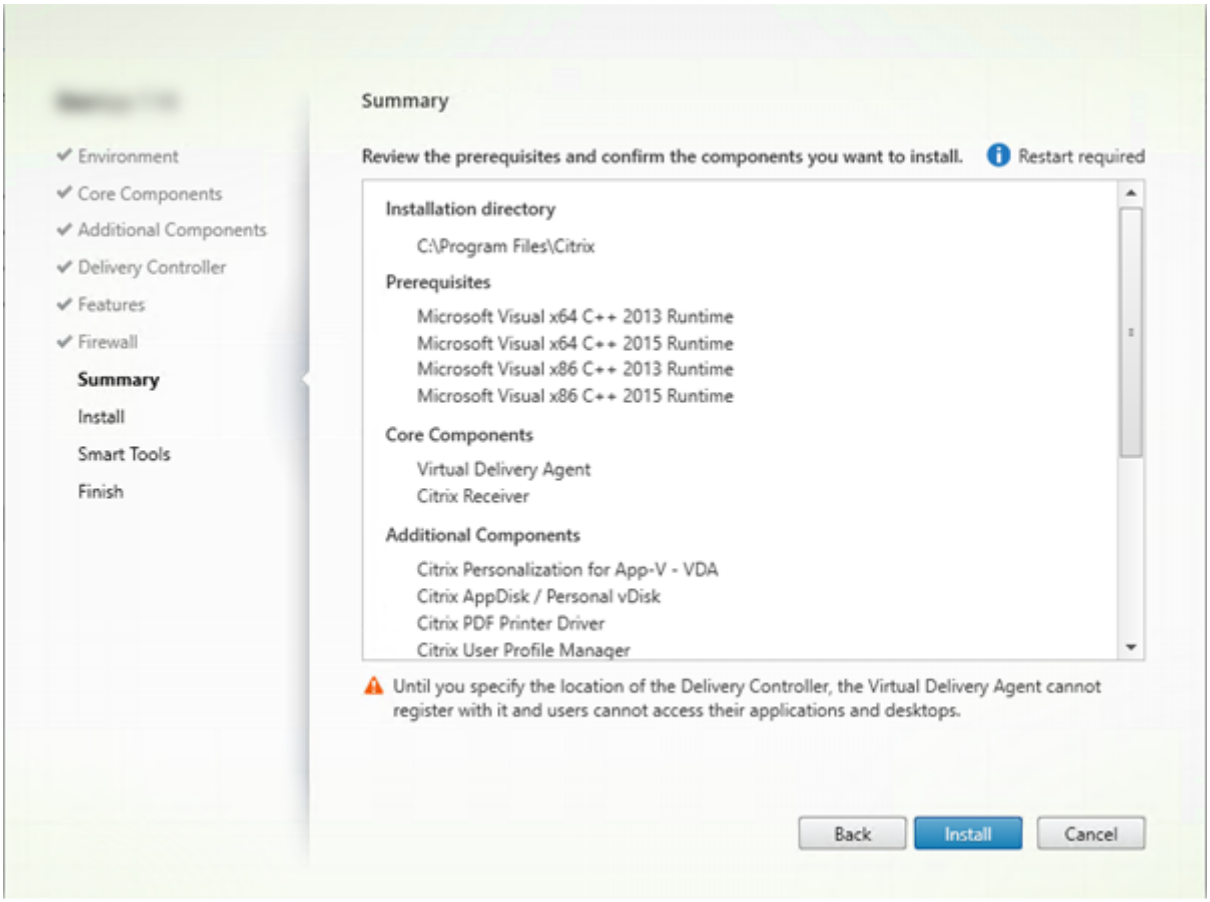


Standardmäßig sind auf der Seite **Firewall** die folgenden Ports geöffnet, wenn der Windows-Firewalldienst ausgeführt wird, selbst wenn die Firewall nicht aktiviert ist. Die Standardeinstellung ist für die meisten Bereitstellungen geeignet. Weitere Informationen zu Ports finden Sie unter Netzwerkports.

Klicken Sie auf **Weiter**.

Befehlszeilenoption: `/enable_hdx_ports`

Schritt 10. Überprüfen der Voraussetzungen und Bestätigen der Installation

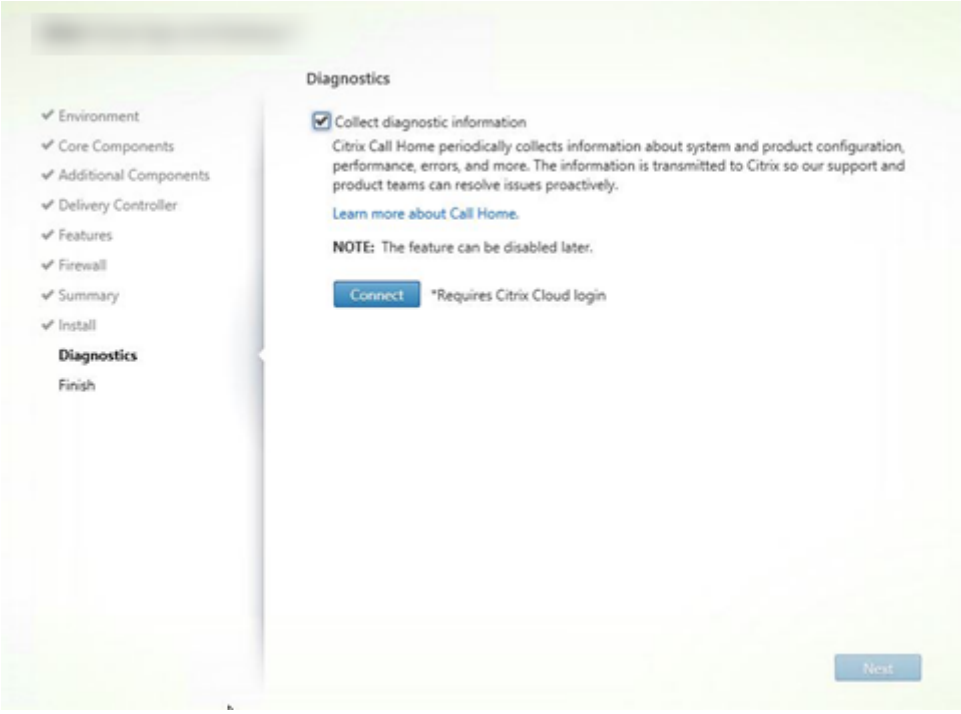


Auf der Seite **Zusammenfassung** wird aufgelistet, was installiert wird. Sie können mit der Schaltfläche Zurück zu vorherigen Seiten zurückkehren und Ihre Auswahl ändern.

Wenn Sie fertig sind, klicken Sie auf **Installieren**.

Wenn erforderliche Software nicht bereits installiert/aktiviert ist wird die Maschine evtl. ein- oder mehrmals neu gestartet. Siehe Vorbereiten der Installation.

Schritt 11. Diagnose

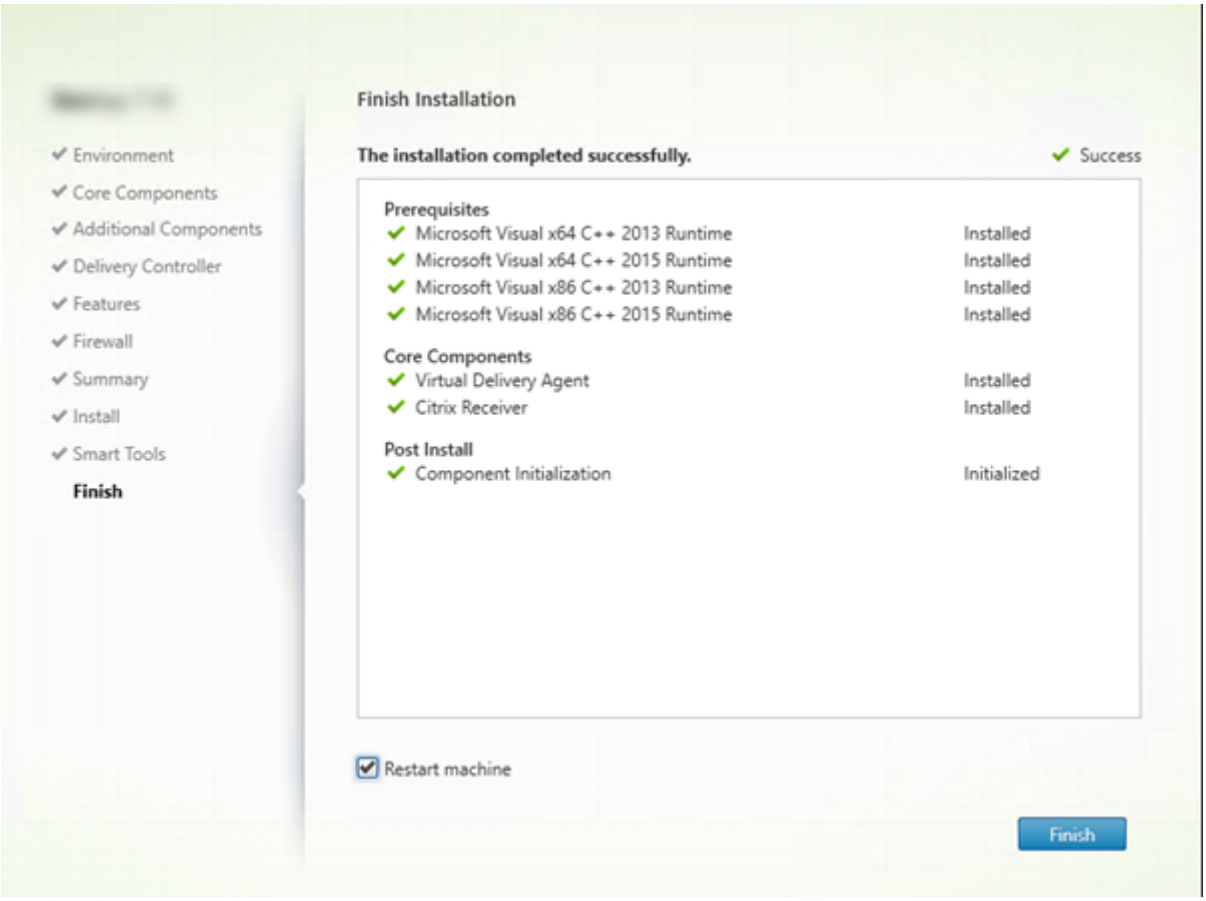


Geben Sie auf der Seite **Diagnose** an, ob Sie bei Citrix Call Home teilnehmen möchten. Wenn Sie teilnehmen möchten (Standardeinstellung), klicken Sie auf **Verbinden**. Geben Sie nach Aufforderung die Anmeldeinformationen Ihres Citrix-Kontos ein.

Wenn Ihre Anmeldeinformationen überprüft sind (bzw. wenn Sie nicht teilnehmen), klicken Sie auf **Weiter**.

Weitere Informationen finden Sie unter Call Home.

Schritt 12. 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.)

Nächste Schritte

Wiederholen Sie das Verfahren oben nach Bedarf zum Installieren weiterer VDAs auf anderen Maschinen oder Images.

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

Anpassen eines VDA

Anpassen eines installierten VDAs:

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

Informationen dazu, wie Citrix das Ergebnis von Komponenteninstallationen meldet, finden Sie unter Citrix Installationsrückgabecodes.

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.

Über die Befehlszeile installieren

January 3, 2023

Dieser Artikel gilt für die Installation von Komponenten auf Maschinen mit Windows-Betriebssystem. Informationen zu VDAs für Linux finden Sie unter Linux Virtual Delivery Agent.

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.

Wenn Sie versuchen, einen Windows-VDA unter einem für diese Produktversion nicht unterstützten Betriebssystem zu installieren (bzw. ein VDA-Upgrade auszuführen) werden Sie durch eine Meldung zu Informationen über Ihre Optionen geleitet. Diese Information ist auch in älteren Betriebssystemen verfügbar.

Informationen dazu, wie Citrix das Ergebnis von Komponenteninstallationen meldet, finden Sie unter Citrix Installationsrückgabecodes.

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 Setupverzeichnis \x64\XenDesktop auf dem Medium den entsprechenden Befehl aus.

Installation von Kernkomponenten: Führen Sie `XenDesktopServerSetup.exe` mit den unter Befehlszeilenoptionen zur Installation der Kernkomponenten beschriebenen Optionen aus.

Zum Installieren von StoreFront: Folgen Sie den Anweisungen unter Installieren von StoreFront über eine Eingabeaufforderung.

VDA-Installation: Führen Sie `XenDesktopVDASetup.exe` mit den unter Befehlszeilenoptionen zur VDA-Installation beschriebenen Optionen aus.

Zum Installieren des universellen Druckservers: Folgen Sie den Anweisungen unter Befehlszeilenoptionen zum Installieren eines universellen Druckservers.

Installation des Verbundauthentifizierungsdiensts: Citrix empfiehlt die Verwendung der grafischen Oberfläche.

Installation der Self-Service-Kennwortrücksetzung: Folgen Sie den Anweisungen unter Self-Service-Kennwortzurücksetzung.

Installation der Sitzungsaufzeichnung: Folgen Sie den Anweisungen unter Sitzungsaufzeichnung.

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 1912 LTSR CU1 war `STOREFRONT` als Wert gültig. Verwenden Sie ab Version 1912 LTSR CU1 die dedizierten, unter Verwenden des Produktinstallationsprogramms aufgeführten StoreFront-Installationsanweisungen.

- **/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** "*feature*"[,"*feature*"]

  Verhindert die Installation der jeweils 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.

- **/help** oder **/h**

  Zeigt die Hilfe für Befehle an.

- **/ignore_hw_check_failure**

  Lässt die Fortsetzung der Installation oder des Upgrades des Delivery Controllers selbst dann zu, wenn die Hardwareprüfung nicht bestanden wird (z. B. wegen unzureichendem Arbeitsspeicher). Weitere Informationen finden Sie unter Hardwareprüfung.

- **/ignore_site_test_failure**

  Gilt nur während des Controllerupgrades. Sitetestfehler werden ignoriert und das Upgrade wird fortgesetzt. Wenn dieser Wert ausgelassen oder auf "falsch"festgelegt wird, führt jeglicher Sitetestfehler dazu, dass das Installationsprogramm fehlschlägt und kein Upgrade durchgeführt wird. Standard = false

- **/installdir *directory***

  Vorhandenes leeres Verzeichnis, in dem die Komponenten installiert werden. Standard: C:\Programme\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_pending_reboot_check**

  Verhindert beim Installieren oder Update von Kernkomponenten die Überprüfung auf einen ausstehenden Neustart aus einer vorherigen Windows-Installation auf der Maschine.

- **/ 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 Citrix Virtual Apps. Wenn diese Option ausgelassen wird, wird Citrix Virtual Apps and Desktops installiert.

Beispiele zur Installation der Kernkomponenten

Mit dem folgenden Befehl werden ein Citrix Virtual Apps and Desktops-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 Citrix Virtual Apps-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
```

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**.

1. Laden Sie das benötigte Paket von Citrix herunter.

- Virtual Delivery Agent für Multisitzungs-OS: `VDAServerSetup.exe`
- Virtual Delivery Agent für Einzelsitzungs-OS: `VDAWorkstationSetup.exe`
- Core Services Virtual Delivery Agent für Einzelsitzungs-OS: `VDAWorkstationCoreSetup.exe`

2. 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 Extrahierung fehl.) Führen Sie dann separat den entsprechenden Befehl unten mit den gültigen Optionen aus, die in diesem Artikel aufgeführt sind.

   - Für `VDAServerSetup_XXXX.exe` führen Sie `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe` aus.
   - Für `VDAWorkstationCoreSetup_XXXX.exe` führen Sie `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopRemotePCSetup.exe` aus.
   - Für `VDAWorkstationSetup_XXXX.exe` führen Sie `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe` aus.

   Um das heruntergeladene Paket auszuführen, führen Sie den Namen aus: `VDAServerSetup.exe`, `VDAWorkstationSetup.exe` oder `VDAWorkstationCoreSetup.exe`. Verwenden Sie die im vorliegenden Artikel beschriebenen, gültigen 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 VDA-Installation

Die folgenden Optionen gelten für einen oder mehrere der folgenden Befehle (Installer): `XenDesktopVDASetup.exe`, `VDAServerSetup.exe`, `VDAWorkstationSetup.exe` oder `VDAWorkstationCoreSetup.exe`.

Weitere Informationen zu den Optionen finden Sie unter Installieren von VDAs.

- **/baseimage**

Nur bei Installation von VDAs für Einzelsitzungs-OS auf einer VM zulässig. Ermöglicht die Verwendung von persönlichen vDisks mit einem Masterimage. Persönliche vDisk ist veraltet.

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 Workspace-App für Windows

  Zum Installieren des VDAs und der Citrix Workspace-App für Windows geben Sie `/components vda plugins` an.

  Ohne Angabe dieser Option wird nur der VDA installiert (nicht die Citrix Workspace-App).

  Diese Option ist ungültig, wenn Sie das Installationsprogramms `VDAWorkstationCoreSetup.exe` verwenden. Mit dem Installationsprogramm kann die Citrix Workspace-App 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_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.

  Zum Öffnen der UDP-Ports, die der adaptive HDX-Transport verwendet, geben Sie zusätzlich zu `/enable_hdx_ports` die Option `/enable_hdx_udp_ports` an.

- **/enable_hdx_udp_ports**

  Öffnet die vom adaptiven HDX-Transport verwendeten 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.

Zum Öffnen weiterer Ports für den VDA geben Sie zusätzlich zu `/enable_hdx_udp_ports` die Option `/enable_hdx_ports` an.

- **/enable_real_time_transport**

  Aktiviert oder deaktiviert die Verwendung von UDP für Audiopakete (RealTime 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 jeweils 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 Maschinenidentitätsdienstkomponente. Gültige Werte:

  - `AppDisks VDA Plug-in`
  - `Personal vDisk`
  - `Machine Identity Service` (enthält TargetOSOptimizer.exe)
  - `Citrix User Profile Manager`
  - `Citrix User Profile Manager WMI Plug-in`
  - `Citrix Universal Print Client`
  - `Citrix Telemetry Service`
  - `Citrix Personalization for App-V - VDA`
  - `Citrix Supportability Tools`
  - `Citrix Files for Windows`
  - `Citrix Files for Outlook`
  - `User Personalization Layer`

  Ausschließen der Citrix User Profilverwaltung aus der Installation (`/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.

Wenn Sie MCS zum Bereitstellen von VMs verwenden möchten, schließen Sie den Maschinenidentitätsdienst nicht aus. Durch Ausschließen dieses Diensts wird auch die Installation von `TargetOSOptimizer.exe` ausgeschlossen.

Wenn Sie sowohl `/exclude` als auch `/includeadditional` mit demselben zusätzlichen Komponentennamen angeben, wird diese Komponente nicht installiert.

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.

- **/includeadditional** "*component*"[,"*component*"]

  Bewirkt die Installation der jeweils in geraden Anführungszeichen angegebenen (durch Kommas getrennten) optionalen Komponenten. Bei Komponentennamen muss die Groß- und Kleinschreibung beachtet werden. Die Option kann hilfreich sein, wenn Sie eine Remote-PC-Zugriff-Bereitstellung erstellen und zusätzliche Komponenten installieren möchten, die standardmäßig nicht enthalten sind. Gültige Werte:

  ```
  - Personal vDisk
  - Citrix User Profile Manager
  - Citrix User Profile Manager WMI Plug-in
  - Citrix Universal Print Client
  - Citrix Telemetry Service
  - Citrix Personalization for App-V - VDA
  - Citrix Supportability Tools
  - Citrix Files for Windows
  - Citrix Files for Outlook
  - User Personalization Layer
  ```

  Wenn Sie sowohl `/exclude` als auch `/includeadditional` mit demselben zusätzlichen Komponentennamen angeben, wird diese Komponente nicht installiert.

  Wenn Sie `Personal vDisk` und `user personalization layer` im selben Befehl verwenden, wird nur `user personalization layer` installiert.

- **/installdir** *directory*

  Vorhandenes leeres Verzeichnis, in dem die Komponenten installiert werden. Standard: C:\Programme\Citrix

- **/install_mcsio_driver**

  Aktiviert MCS-E/A-Schreibcache für Speicheroptimierung.

- **/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 entspricht `/mastermcsimage`.

  Diese Option ist ungültig, wenn Sie das Installationsprogramms `VDAWorkstationCoreSetup.exe` verwenden.

- **/mastermcsimage**

  Gibt an, dass die Maschine als Masterimage für die Maschinenerstellungsdienste verwendet wird. Diese Option installiert auch TargetOSOptimizer.exe (es sei denn, Sie geben auch `/exclude "Machine Identity Service"` an, dies enthält den Optimierungsinstaller). Diese Option entspricht `/masterimage`.

- **/masterpvsimage**

  Gibt an, dass die Maschine als Masterimage und Citrix Provisioning oder das Tool eines Fremdherstellers (z. B. Microsoft System Center Configuration Manager) zur Bereitstellung von VMs werden soll.

- **/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.

- **/nodesktopexperience**

  Gilt nur für die Installation von VDAs für Multisitzungs-OS. 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**

  Wenn Sie die Maschinenerstellungsdienste (MCS) verwenden und dieses Feature aktivieren (Standard), deaktiviert die VM-Optimierung Offlinedateien sowie die Hintergrunddefragmentierung und verringert die Größe des Ereignisprotokolls. Einzelheiten finden Sie unter CTX224676.

  Sie müssen die Optimierung aktivieren und zusätzlich den Maschinenidentitätsdienst installieren. Dieser Dienst enthält TargetOSOptimizer.exe. Der Maschinenidentitätsdienst wird automatisch installiert, wenn Sie /`mastermcsimage` oder /`masterimage` angeben (und nicht /`exclude "Machine Identity Service"` angeben).

  Geben Sie diese Option nicht für Remote-PC-Bereitstellungen an.

- **/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 (Einzelsitzungs-OS) oder vermittelte Verbindungen (Multisitzungs-OS). Verhindert die Installation der folgenden Komponenten unter einem Einzelsitzungs-OS:

  – Citrix Personalisierung für App-V

  - Citrix User Profile Manager
  - Citrix User Profile Manager WMI Plug-In
  - Maschinenidentitätsdienst (enthält TargetOSOptimizer.exe).
  - Personal vDisk
  - Citrix Supportability Tools
  - Citrix Files für Windows
  - Citrix Files für Outlook
  - Benutzerpersonalisierungslayer

  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 Einzelsitzungs-OS auf einer Maschine mit einem unterstützten Windows-Multisitzungs-OS. Wenn Sie einen VDA für Multisitzungs-OS auf einer Maschine für Multisitzungs-OS installieren, lassen Sie diese Option aus. Lesen Sie vor dem Verwenden dieser Option Server-VDI.

  Diese Option sollte nur mit dem VDA-Installationsprogramm für das vollständige Produkt verwendet werden. 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. Standard = 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 für die Installation eines VDAs

Installieren eines VDAs mit dem Komplettinstallationsprogramm:

Mit dem folgenden Befehl werden ein VDA für Einzelsitzungs-OS und die Citrix Workspace-App am Standardspeicherort auf einer VM installiert. Der VDA wird als Masterimage verwendet und MCS zur Bereitstellung von VMs. Zunächst wird der VDA bei dem Controller auf dem Server `Contr-Main` in der Domäne `mydomain` registriert. Der VDA verwendet den Benutzerpersonalisierungslayer, das Optimierungsfeature und die Windows-Remoteunterstützung.

```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /components vda,
plugins /controllers "Contr-Main.mydomain.local"/enable_hdx_ports /
includeadditional "User Personalization Layer"/optimize /mastermcsimage
 /enable_remote_assistance
```

Installation eines VDAs mit Einzelsitzungs-OS mit dem eigenständigen Installationsprogramm VDAWorkstationCoreSetup:

Mit dem folgenden Befehl wird ein Kernkomponenten-VDA unter einem Einzelsitzungs-OS zur Verwendung in einer Remote-PC-Zugriff- oder VDI-Bereitstellung installiert. Die Citrix Workspace-App 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 VDA

Nachdem VDA installiert wurde, können Sie einige Einstellungen anpassen. Führen Sie auf dem Produktmedium im `\x64\XenDesktop Setup`-Verzeichnis `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

Befehlszeilenoptionen zum Installieren eines universellen Druckservers

Die folgende Option ist bei Befehl XenDesktopPrintServerSetup.exe gültig.

- **/enable_upsserver_port**

Software	Ordner	Dateiname
Microsoft Visual C++ 2017 Runtime (32-Bit und 64-Bit)	Support > VcRedist_2017	vcredist_x64.exe und vcredist_x86.exe
Citrix Diagnostic Facility	x64 > Virtual Desktop Components	cdf_x64.msi
Universeller Druckserver	x64 > Universal Print Server	UpsServer_x64.msi

Wenn diese Option nicht angegeben wird, wird im Installationsprogramm die Seite **Firewall** angezeigt. Wählen Sie **Automatisch**, um die Windows-Firewallregeln automatisch vom Installationsprogramm hinzufügen zu lassen, oder **Manuell**, damit der Administrator die Firewall manuell konfigurieren kann.

Nach der Installation der Software auf den Druckservern konfigurieren Sie den universellen Druckserver anhand der Anweisungen unter Bereitstellen von Druckern.

VDAs mit Skripts installieren

May 10, 2023

> **Hinweis:**
>
> Citrix übernimmt keine Verantwortung für Probleme, die durch Skripts entstehen, die an die Produktionsumgebung des Kunden angepasst wurden. Bei Citrix-bezogenen Installationsproblemen können Sie im Citrix Support-Portal einen technischen Supportfall erstellen, unter Angabe der entsprechenden Installationsprotokolle.

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 Citrix Provisioning (zuvor "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 beim vollständigen Produkt-ISO ist `XenDesktopVdaSetup.exe`, im eigenständigen Installationsprogramm `VDAWorkstationSetup.exe` oder `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.

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 VDAs 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. 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 VDAs 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.

VDAs mit SCCM installieren

May 10, 2023

> **Hinweis:**
>
> Citrix übernimmt keine Verantwortung für Probleme nach Bereitstellung eines Virtual Delivery Agent (VDA) mit Softwareverteilungstools wie Microsoft System Center Configuration Manager (SCCM), die an die Produktionsumgebung des Kunden angepasst wurden. Bei Citrix-bezogenen Installationsproblemen können Sie im Citrix Support-Portal einen technischen Supportfall erstellen, unter Angabe der entsprechenden Installationsprotokolle.

Übersicht

Zum erfolgreichen Bereitstellen eines Virtual Delivery Agent (VDA) mit Microsoft SCCM (System Center Configuration Manager) oder einem ähnlichen Softwareverteilungstool empfiehlt Citrix, die Reihenfolge der Schritte des VDA-Installationsprogramms einzuhalten.

Citrix empfiehlt nicht, das Programm VDA Cleanup Utility als Teil einer VDA-Installation oder eines VDA-Upgrades zu verwenden. Verwenden Sie VDA Cleanup Utility nur dann, wenn das VDA-Installationsprogramm zuvor fehlgeschlagen ist.

Neustarts

Wie viele Neustarts während der Installation des VDA erforderlich sind, hängt von der Umgebung ab. Beispiel:

- Ein Neustart kann für ausstehende Updates oder es können Neustarts von früheren Softwareinstallationen erforderlich sein.

- Dateien, die zuvor von anderen Prozessen gesperrt wurden, müssen möglicherweise aktualisiert werden, was einen zusätzlichen Neustart erzwingt.
- Optionale Komponenten im VDA-Installationsprogramm (z. B. Citrix Profilverwaltung und Citrix Files) können einen Neustart erfordern.

Der SCCM Task Sequencer verwaltet alle erforderlichen Neustarts.

Definieren der Tasksequenz

Nachdem Sie alle Voraussetzungen und Neustarts erfasst haben, führen Sie folgende Schritte mit dem SCCM Task Sequencer aus:

- Der VDA kann von einer zugänglichen Kopie des Installationsmediums oder von einem der eigenständigen VDA-Installationsprogramme installiert werden:

  - `VDAWorkstationSetup_XXXX.exe`
  - `VDAServerSetup_XXXX.exe`
  - `VDAWorkstationCoreSetup_XXXX.exe`

  Weitere Informationen zu VDA-Installationsprogrammen finden Sie unter Installationsprogramme.

- Beim Upgrade eines VDA muss sich die Maschine, auf dem er installiert ist, im Wartungsmodus ohne Sitzungen befinden.
- Wenn eine VDA-Installation zum ersten Mal auf einer Maschine ausgeführt wird, wird das verwendete VDA-Installationsprogramm auf diese Maschine kopiert.

  - Bei Verwendung eines anderen VDA-Installationsprogramms als `VDAWorkstationCoreSetup_XX` `.exe` wird das VDA-Installationsprogramm nach `%ProgramData%\Citrix\XenDesktopSetup\XenDesktopVdaSetup.exe` kopiert.
  - Bei Verwendung von `VDAWorkstationCoreSetup_XXXX.exe` wird das VDA-Installationsprogramm nach `%ProgramData%\Citrix\XenDesktopSetup\XenDesktopRemotePCSetup.exe` kopiert.

    ‘

- Der Verzeichnisspeicherort des VDA-Installationsprogramms wird ebenfalls in der Registrierung gespeichert: “`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaInstall`” “`MetaInstallerInstallLocation`”.
- Fügen Sie Ihren Befehlszeilenoptionen die Optionen `/NOREBOOT`, `/NORESUME` und `/QUIET` hinzu.

  - `/QUIET`: Die Benutzeroberfläche wird während der Installation nicht angezeigt, sodass SCCM die Kontrolle über den Installationsvorgang hat.

- /NOREBOOT: Unterdrückt den automatischen Neustart des VDA-Installationsprogramms. SCCM löst bei Bedarf Neustarts aus.
- /NORESUME: Normalerweise legt das VDA-Installationsprogramm, wenn während der Installation ein Neustart erforderlich ist, einen runonce-Registrierungsschlüssel fest (\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce). Beim Neustart der Maschine verwendet Windows den Schlüssel, um das VDA-Installationsprogramm zu starten. Das ist ein Problem für SCCM, da SCCM die Installation nicht überwachen und den Exitcode nicht erfassen kann.

Beispiel einer Installationssequenz mit SCCM

Das folgende Beispiel zeigt die Installationssequenz.

1. **SCCM TASK1:** Bereiten Sie die Maschine vor, indem Sie sie neu starten.
2. **SCCM TASK2:** Starten Sie die VDA-Installation.

   a) Fügen Sie Ihren Befehlszeilenoptionen die Optionen /quiet, /noreboot und /noresume hinzu.
   b) Führen Sie das VDA-Installationsprogramm Ihrer Wahl aus (lokales Image oder eines der Minimalinstallationsprogramme).
   c) SCCM muss den Rückgabecode erfassen.
      - Wenn der Rückgabecode 0 oder 8 lautet, ist die Installation abgeschlossen und ein Neustart ist erforderlich.
      - Wenn der Rückgabecode 3 ist, starten Sie die Maschine neu und übergeben Sie dann die Steuerung an SCCM TASK3.

3. **SCCM TASK3:** Setzen Sie die VDA-Installation fort.

   a) Wenn SCCM TASK2 keine 0 oder 8 zurückgibt, muss die Installation nach Abschluss des Neustarts fortgesetzt werden.
   b) SCCM TASK3 wiederholt dann den Vorgang, bis das VDA-Installationsprogramm eine 0 oder 8 (was eine erfolgreiche Installation anzeigt) oder 3 (was anzeigt, dass SCCM TASK3 wiederholt werden muss) zurückgibt. Betrachten Sie jeden anderen Rückgabecode als Fehler. SCCM TASK3 sollte einen Fehler melden und anhalten.
   c) Setzen Sie die VDA-Installation fort, indem Sie das entsprechende VDA-Installationsprogramm (in den meisten Fällen XenDesktopVdaSetup.exe, bzw. XenDesktopRemotePCSetup.exe, falls VDAWorkstationCoreSetup_XXXX.exe verwendet wurde) von dem Speicherort ausführen, an den es kopiert wurde (wie unter Definieren der Tasksequenz beschrieben), ohne Befehlszeilenparameter. (Das VDA-Installationsprogramm verwendet die Parameter, die bei der ersten Ausführung des Programms gespeichert wurden.)
   d) Achten Sie auf den Rückgabecode des VDA-Installationsprogramms.

- 0 oder 8: Erfolg, Installation abgeschlossen, Neustart erforderlich.
- 3: Installation nicht abgeschlossen. Starten Sie die Maschine neu und wiederholen Sie SCCM TASK3, bis eine 0 oder 8 zurückgegeben wird. Betrachten Sie jeden anderen Rückgabecode als Fehler. SCCM TASK3 sollte einen Fehler melden und den Vorgang beenden.

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.

- VDAs installieren
- Über die Befehlszeile installieren

Installationsbefehle für Remote-PC-Zugriff

- Der folgende Befehl verwendet das Basis-VDA-Installationsprogramm für Einzelsitzungs-OS (`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 (`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 (`VDAWorkstationSetup.exe`):

  ```
  VDAWorkstationSetup.exe /quiet /components vda /controllers “control.domain.com” /enable_hdx_ports /enable_remote_assistance /noresume /noreboot
  ```


Erstellen einer Site

March 15, 2022

Eine *Site* ist der Name, den Sie einer Citrix Virtual Apps and Desktops-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.

Wenn der Controller unter Server Core installiert ist, verwenden Sie PowerShell-Cmdlets des Citrix Virtual Apps and Desktops-SDKs, um eine Site zu 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 http://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 vorliegenden Artikel bevor Sie die Site erstellen.

Schritt 1. Studio öffnen und Assistenten für die Siteerstellung starten

Öffnen Sie Studio, falls es nicht geöffnet ist. Sie werden automatisch zu der Aktion zum Starten des Assistenten für die Siteerstellung geführt. Wählen Sie diese Aktion.

Schritt 2. Name und Typ der Site

Wählen Sie auf der Seite **Einführung** einen Sitetyp aus:

- **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*).

Schritt 3. 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 Delivery Controller-Software auf anderen Servern installiert haben und der Site weitere Delivery Controller hinzufügen möchten, können Sie dies über diese Seite tun. Wenn Sie außerdem Skripts für die Einrichtung der Datenbanken generieren möchten, fügen Sie die Controller vor dem Generieren der Skripts hinzu.

Schritt 4. Lizenzierung

Geben Sie auf der Seite **Lizenzierung** die Adresse des Lizenzservers an und legen Sie fest, welche Lizenz verwendet (installiert) werden soll.

- Geben Sie die Lizenzserveradresse im folgenden Format `name:[port]` an. 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 fortfahren, wenn eine Verbindung zum Lizenzserver hergestellt wurde.
- Wenn eine Verbindung hergestellt wird, wird die Option **Vorhandene Lizenz verwenden** standardmäßig ausgewählt. Es werden basierend auf den installierten Lizenzen die kompatiblen Konfigurationsoptionen für die Produkte angezeigt.
  - Wenn Sie das Produkt unter Verwendung einer dieser Lizenzen als eines der aufgeführten Produkte konfigurieren möchten (z. B. Citrix Virtual Apps Premium oder Citrix Virtual Desktops Premium), wählen Sie den entsprechenden Eintrag aus.

- Wenn Sie mit dem Citrix Manage Licenses-Tool bereits eine Lizenz für das Produkt zugeteilt und heruntergeladen, jedoch noch nicht installiert haben, gehen Sie folgendermaßen vor:
  - Klicken Sie auf **Nach Lizenzdatei suchen**.
  - Suchen Sie im Datei-Explorer die heruntergeladene Lizenz und wählen Sie sie aus. Die zugeordneten Produkte werden nun auf der Seite **Lizenzierung** des Assistenten für die Siteerstellung angezeigt. Wählen Sie den gewünschten Eintrag aus.
- Wenn das gewünschte Produkt nicht angezeigt wird oder Sie keine zugeteilten und heruntergeladenen Lizenzen haben, können Sie eine Lizenz zuweisen, herunterladen und installieren. Dazu muss der Lizenzserver über Internetzugriff verfügen. Sie benötigen einen Lizenzzugangscode für das gewünschte Produkt. Citrix sendet Ihnen diesen Code per E-Mail zu.
  - Klicken Sie auf **Zuteilen und herunterladen**.
  - Geben Sie im Dialogfeld **Lizenzen zuteilen** den von Citrix erhaltenen Lizenzzugangscode ein. Klicken Sie auf **Lizenzen zuteilen**.
  - Die der neuen Lizenz zugeordneten Produkte werden nun auf der Seite **Lizenzierung** des Assistenten für die Siteerstellung angezeigt. Wählen Sie den gewünschten Eintrag aus.

  Alternativ wählen Sie **Kostenloses 30-Tage-Probeabo verwenden** und installieren Sie die Lizenzen später. Weitere Informationen finden Sie in der Dokumentation für die Lizenzierung.

Schritt 5. Energieverwaltung (nur Remote-PC-Zugriff)

Siehe Schritt 8. Remote-PC-Zugriff.

Schritt 6. 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.

- Informationen zu den Angaben auf der Seite **Verbindung** finden Sie unter Verbindungen und Ressourcen.
  - 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.

- Informationen zu den Angaben auf den Seiten **Speicher** und **Netzwerk** unter Hostspeicher, Speicherverwaltung und Speicherauswahl.

Schritt 7. Weitere Features

Auf der Seite **Zusätzliche Features** können Sie weitere Features zum Anpassen der Site auswählen. Wenn Sie das Kontrollkästchen eines Elements aktivieren, wird ein Dialogfeld zur Konfiguration angezeigt.

- **AppDNA-Integration:** (Dieses Feature ist veraltet.) 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.
- **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.

Schritt 8. 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 Configuration Manager und Remote-PC-Zugriff-Wake-On-LAN.

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**.

Es wird automatisch der Maschinenkatalog "Remote PC User Machine Accounts"erstellt. Der Maschinenkatalog enthält alle Maschinenkonten, die Sie im Assistenten für die Siteerstellung hinzugefügt haben. Es wird automatisch die Bereitstellungsgruppe "Remote PC User Desktops"is erstellt. Sie enthält alle Benutzer und Gruppen, die Sie hinzugefügt haben.

Schritt 9. Zusammenfassung

Auf der Seite **Zusammenfassung** werden die 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 (Site*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.

Sitetests werden automatisch ausgeführt, wenn Sie eine ältere Bereitstellung aktualisieren. Weitere Informationen finden Sie unter Sitetests zur Vorbereitung.

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.

Maschinenkataloge erstellen

June 27, 2024

Sammlungen von physischen oder virtuellen Maschinen werden als Einheit in einem sogenannten Maschinenkatalog verwaltet. Maschinen in einem Katalog haben den gleichen Betriebssystemtyp: Multisitzungs-OS oder Einzelsitzungs-OS. Ein Katalog mit Maschinen mit Multisitzungs-OS 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.

> **Tipp:**
>
> Wenn Sie ein Upgrade für eine vorhandene Bereitstellung durchführen, das die MCS-Speicheroptimierung (MCS E/A) aktiviert, ist keine zusätzliche Konfiguration erforderlich. Der VDA und das Delivery Controller-Upgrade behandeln das MCS-E/A-Upgrade.

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 Citrix Provisioning (zuvor "Provisioning Services") verwenden. Alternativ können Sie eigene Tools verwenden.

Berücksichtigen Sie dabei:

- MCS unterstützt einen einzelnen Systemdatenträger vom VM-Image. Die übrigen mit dem Image verbundenen Datenträger werden ignoriert.
- Wenn Sie Maschinen mit Citrix Provisioning erstellen, lesen Sie die zugehörige Dokumentation.
- Bei Verwendung von Maschinenerstellungsdiensten (MCS) stellen Sie ein Masterimage (bzw. einen Image-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. den Snapshot) und geben die Anzahl der in dem Katalog zu erstellenden VMs und weitere Informationen an.

- Selbst wenn Sie die Maschinen bereits haben, erstellen Sie mindestens einen Maschinenkatalog für diese Maschinen.
- Wenn Sie einen Katalog direkt mit dem PowerShell-SDK erstellen, können Sie alternativ zu einem Image bzw. einem Snapshot eine Hypervisorvorlage (VMTemplates) angeben.

Beim Erstellen des ersten Maschinenkatalogs mit MCS oder Citrix Provisioning 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. Führen Sie die Tests jederzeit über Studio aus.

> **Hinweis:**
>
> MCS unterstützt Windows 10 IoT Core und Windows 10 IoT Enterprise nicht. Weitere Informationen finden Sie auf der Website von Microsoft.

Technische Details zu den Citrix Provisioning-Tools finden Sie unter Citrix Virtual Apps and Desktops Image Management.

Prüfung auf RDS-Lizenz

In Citrix Studio wird derzeit nicht auf gültige Microsoft RDS-Lizenzen geprüft, wenn ein Maschinenkatalog mit Multisitzungs-Windows-Maschinen erstellt wird. Zum Anzeigen des Status der Microsoft RDS-Lizenz einer **Multisitzungs-Windows-Maschine** verwenden Sie Citrix Director. Zeigen Sie den Status der Lizenz für Microsoft RDS (Remotedesktopdienste) im Fenster **Maschinendetails** auf den Seiten **Maschinendetails** und "Benutzerdetails"an. Weitere Informationen finden Sie unter Microsoft RDS-Lizenzstatus.

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), fügen Sie die Maschine dennoch hinzu.

Weitere Informationen:

- CTX136668 zur Problembehandlung bei der VDA-Registrierung
- VDA-Versionen und Funktionsebenen
- VDA-Registrierung

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; 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 über den Delivery Controller 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.

Überlegungen zum MCS-Speicher

Es gibt viele Faktoren bei der Entscheidung über Speicherlösungen, Konfigurationen und Kapazitäten für MCS. Die folgenden Informationen enthalten Überlegungen zur Speicherkapazität:

Kapazitätsüberlegungen:

- Datenträger

  Die Delta- oder Differenzdatenträger (Diff) benötigen den meisten Speicherplatz in den meisten MCS-Bereitstellungen für jede VM. Jede VM, die von MCS erstellt wurde, erhält beim Erstellen mindestens 2 Datenträger.

  - Disk0 = Diff Disk: Enthält das Betriebssystem, wenn von dem Masterbasisimage kopiert.
  - Disk1 = Identitätsdatenträger: 16 MB, enthält Active Directory-Daten für jede VM.

  Im Laufe der Weiterentwicklung des Produkts, müssen Sie möglicherweise zusätzliche Datenträger hinzufügen, um den Verbrauch bestimmter Anwendungsfälle und Features abzudecken. Beispiel:

  - Personal vDisk bietet Endbenutzern die Möglichkeit, Anwendungen ohne Administratoreingriff auf einem separaten Datenträger zu installieren, der mit der VM verbunden ist.
  - AppDisk bietet Endbenutzern die Möglichkeit, Nur-Anwendungsdatenträger an VMs anzuhängen, primär für Multisitzungs-OS-Kataloge.
  - Die MCS-Speicheroptimierung erstellt einen Schreibcachedatenträger für jede VM.
  - MCS hat die Möglichkeit hinzugefügt, vollständige Klons zu verwenden, im Gegensatz zu dem oben beschriebenen Szenario mit Deltadatenträgern.

  Hypervisorfeatures spielen auch eine Rolle. Beispiel:

  - Citrix Hypervisor IntelliCache erstellt einen Lesedatenträger im lokalem Speicher für jeden Citrix Hypervisor, um IOPS gegen das Masterimage zu sparen, das möglicherweise an einem freigegebenen Speicherort ist.

- Mehraufwand für den Hypervisor

Unterschiedliche Hypervisors verwenden bestimmte Dateien, die einen Mehraufwand für VMs verursachen. Hypervisors verwenden auch Speicher für Verwaltungs- und allgemeine Protokollierungsvorgänge. Berücksichtigen Sie beim Speicherplatz den Mehraufwand für:

  - Protokolldateien
  - Hypervisorspezifische Dateien. Beispiel:
    * VMware fügt dem **VM-Speicherordner** zusätzliche Dateien hinzu. Siehe VMware Best Practices.
    * Berechnen Sie erforderliche Gesamtgröße für virtuelle Maschinen. Vorschlag für die virtuelle Maschine: 20 GB für den virtueller Datenträger, 16 GB für die Auslagerungsdatei der virtuellen Maschine (die Größe des zugewiesenen Arbeitsspeichers) und 100 MB für Protokolldateien also 36,1 GB insgesamt.
  - Snapshots for XenServer; Snapshots for VMware.

- Mehraufwand für die Verarbeitung

  Das Erstellen eines Katalogs, Hinzufügen einer Maschine und Aktualisieren eines Katalogs haben spezielle Auswirkungen auf den Speicher. Beispiel:

  - Für die anfängliche Katalogerstellung muss eine Kopie des Basisdatenträgers an jeden Speicherort kopiert werden.
    * Außerdem müssen Sie vorübergehend eine Vorbereitungs-VM erstellen.
  - Das Hinzufügen einer Maschine zu einem Katalog erfordert nicht das Kopieren der Basisdatenträger an jeden Speicherort. Die Katalogerstellung variiert je nach ausgewählten Features. Daher benötigt ein Katalog, der PvD oder AppDisks verwendet, mehr Speicherplatz als ein einfacher zufällig gepoolter Katalog.
  - Beim Aktualisieren des Katalogs kann für jeden Speicherort ein zusätzlicher Basisdatenträger erstellt werden. Für Katalogupdates kommt es zu einer vorübergehenden Speicherverbrauchspitze, bei der jede VM im Katalog für eine bestimmte Zeit 2 Diff-Datenträger hat.

Weitere Überlegungen:

- **RAM-Dimensionierung:** Beeinflusst die Größe bestimmter Hypervisordateien und -datenträger, einschließlich E/A-Optimierungsdatenträger, Schreibcache und Snapshotdateien.
- **Thin / Thick Provisioning:** NFS-Speicher wird wegen der schlanke Speicherzuweisungsfunktionen bevorzugt.

MCS-Speicheroptimierung

Mit der MCS-Speicheroptimierung (Maschinenerstellungsdienste), die als MCS E/A bezeichnet wird:

- Der Schreibcachecontainer ist jetzt wie bei Citrix Provisioning *dateibasiert*. Beispielsweise lautet der Name des Citrix Provisioning-Schreibcache `D:\vdiskdif.vhdx` und der des MCS-E/A-Schreibcache `D:\mcsdif.vhdx`.
- Verbesserungen bei der Diagnose werden durch die Unterstützung für eine im Schreibcachedatenträger gespeicherte Windows-Absturzabbilddatei erzielt.
- MCS E/A behält die Technologie *Cache im RAM mit Überlauf auf Festplatte* bei, um die optimale Schreibcachelösung auf mehreren Ebenen bereitzustellen. Mit dieser Funktion können Administratoren die Kosten in den Bereichen RAM, Datenträger und Leistung ausgleichen, um die Workload-Erwartungen zu erfüllen.

Die Aktualisierung der Schreibcachemethode von *datenträgerbasiert* auf *dateibasiert* erfordert die folgenden Änderungen:

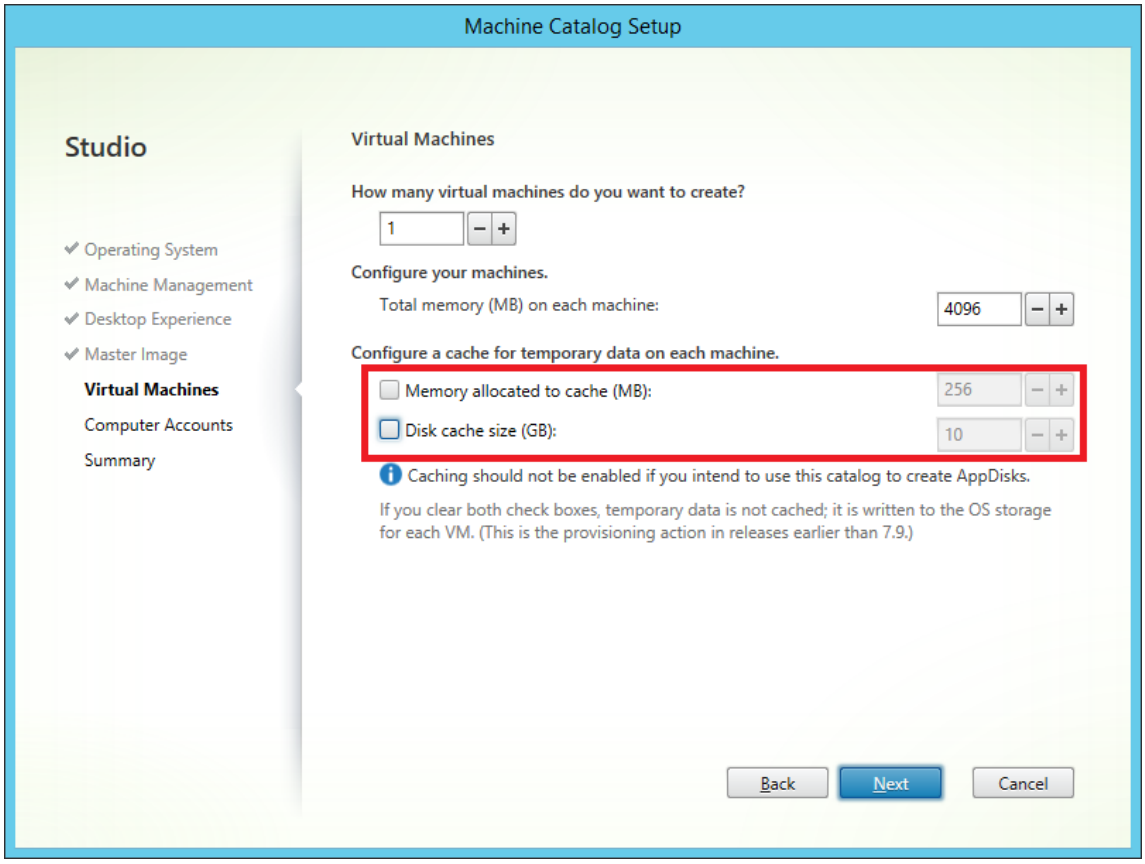
1. MCS-E/A unterstützt einen ausschließlich RAM-basierten Cache nicht mehr. Geben Sie beim der Erstellen des Maschinenkatalogs eine Datenträgergröße in Citrix Studio an.
2. Der VM-Schreibcachedatenträger wird beim ersten Starten einer VM automatisch erstellt und formatiert. Sobald die VM läuft, wird die Schreibcachedatei `mcsdif.vhdx` in das formatierte Volume `MCSWCDisk` geschrieben.
3. Mit Ausnahme von Microsoft Azure-Umgebungen wird die Auslagerungsdatei an das formatierte Volume `MCSWCDisk` umgeleitet. Daher wird bei der Festplattengröße die Gesamtmenge des Festplattenspeichers berücksichtigt, einschließlich des Deltas zwischen der Festplattengröße und der generierten Workload plus Auslagerungsdateigröße (die normalerweise mit der VM-RAM-Größe zusammenhängt). Die Microsoft Azure Auslagerungsdatei ist zur Verwendung eines lokalen temporären Datenträgers vorkonfiguriert und wird von der MCS-E/A-Speicheroptimierung nicht an `MCSWCDisk` umgeleitet.

Aktivieren der neuen MCS-Speicheroptimierung Zum Aktivieren der MCS E/A-Speicheroptimierung aktualisieren Sie den Delivery Controller und den VDA auf die neueste Version von Citrix Virtual Apps and Desktops.

> **Hinweis:**
>
> Wenn Sie eine vorhandene Bereitstellung aktualisieren, in der MCS E/A aktiviert ist, ist keine zusätzliche Konfiguration erforderlich. Der VDA und das Delivery Controller-Upgrade behandeln das MCS-E/A-Upgrade.

Berücksichtigen Sie bei der Aktivierung der neuen MCS-Speicheroptimierung Folgendes:

- Beim Erstellen eines Maschinenkatalogs können RAM- und Datenträgergröße konfiguriert werden.



- Beim Aktualisieren eines Maschinenkatalogs auf einen neuen VM-Snapshot, der einen VDA mit Citrix Virtual Apps and Desktops Version 1903 enthält, wird die MCS-E/A-Einstellung des Katalogs für RAM und Datenträgergröße weiterverwendet. Der bestehende Rohdatenträger wird formatiert.

> **Wichtig:**
>
> Die MCS-Speicheroptimierung wurde in Citrix Virtual Apps and Desktops 1912 LTSR geändert. Dieses Release unterstützt einen dateibasierten Schreibcache und bietet damit mehr Leistung und Stabilität. Die neue Funktion, die von MCS-E/A bereitgestellt wird, erfordert möglicherweise mehr Schreibcachespeicher als frühere Versionen von Citrix Virtual Apps and Desktops. Citrix empfiehlt, gegebenenfalls die Datenträgergröße anzupassen, damit genügend Speicherplatz für den zugewiesenen Workflow und die größere Auslagerungsdatei vorhanden ist. Die Größe von Auslagerungsdatei und System-RAM sind in der Regel miteinander verbunden. Reicht die Datenträgergröße des Katalogs nicht aus, erstellen Sie einen neuen Maschinenkatalog und weisen einen größeren Schreibcachedatenträger zu.

Microsoft Azure-Umgebungen Standardmäßig wird der MCS-E/A-Schreibcachedatenträger beim ersten VM-Start bereitgestellt und nach dem Herunterfahren der VM gelöscht. Dies ist die kostengünstigste Einstellung. Allerdings dauert der VM-Start länger, da der Schreibcachedatenträger formatiert

werden muss und ein zusätzlicher Neustart erforderlich ist. Für Umgebungen mit Workloads, bei denen ein schneller Start wichtig ist, empfiehlt Citrix die Erstellung einer VM mit permanentem MCS-E/A-Cachedatenträger mithilfe von PowerShell. Ein permanenter Cachedatenträger wird beim Ausschalten nicht gelöscht, doch sollten die Azure-Speicherkosten berücksichtigt werden.

Verwenden von PowerShell zum Erstellen eines Azure-Katalogs mit permanentem Zurückschreibcachedatenträger Zum Konfigurieren eines Azure-Katalogs mit permanentem Zurückschreibcachedatenträger verwenden Sie den PowerShell-Parameter `New-ProvScheme CustomProperties`. Dieser Parameter unterstützt die zusätzliche Eigenschaft `PersistWBC`, welche bestimmt, ob der Zurückschreibcachedatenträger bei von Azure Resource Manager gehosteten und von MCS-bereitgestellten Maschinen permanent oder flüchtig ist. Die Eigenschaft `PersistWBC` wird nur verwendet, wenn der Parameter `UseWriteBackCache` angegeben wird und Parameter `WriteBackCacheDiskSize` so konfiguriert ist, dass ein Datenträger erstellt wird.

> **Tipp:**
>
> Da es in Azure viele bereitstellungsspezifische Eigenschaften gibt, wird das Feld `CustomProperties` für viele Einstellungen verwendet.

Beispiele für Eigenschaften im Parameter `CustomProperties` vor Unterstützung von `PersistWBC`:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
     />
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
    Premium_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="
    benvaldev5RG3" />
</CustomProperties>
<!--NeedCopy-->
```

Berücksichtigen bei Verwendung dieser Eigenschaften deren Standardwerte, wenn die Eigenschaften im Parameter `CustomProperties` ausgelassen werden. Die Eigenschaft `PersistWBC` hat zwei mögliche Werte: **true** oder **false**.

Wenn `PersistWBC` auf **true** festgelegt wird, wird der Zurückschreibcachedatenträger nicht gelöscht, wenn der Citrix Virtual Apps and Desktops-Administrator die Maschine mit Citrix Studio herunterfährt.

Wird `PersistWBC` auf **false** festgelegt, wird der Zurückschreibcachedatenträger gelöscht, wenn der Citrix Virtual Apps and Desktops-Administrator die Maschine mit Citrix Studio herunterfährt.

> **Hinweis:**
>
> Wird die Eigenschaft `PersistWBC` nicht angegeben, so gilt der Standardwert **false** und der Zurückschreibcachedatenträger wird bei Herunterfahren der VM mit Citrix Studio gelöscht.

Beispiel der Verwendung des Parameters `CustomProperties` zur Einstellung von `PersistWBC` auf "true":

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
    />
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
   Premium_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="
   benvaldev5RG3" />
<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />
</CustomProperties>
<!--NeedCopy-->
```

> **Wichtig:**
>
> Die Eigenschaft `PersistWBC` kann nur mit dem PowerShell-Cmdlet `New-ProvScheme` festgelegt werden. Eine Änderung der `CustomProperties` eines Provisioningschemas nach der Erstellung hat keine Auswirkungen auf den Maschinenkatalog und die Permanenz des Zurückschreibcachedatenträger beim Herunterfahren von Maschinen. Der Wert von `PersistWBC` wird nur für Kataloge verwendet, die in Azure Resource Manager bereitgestellt werden.

Beispiel der Einstellung von `New-ProvScheme` zur Verwendung des Zurückschreibcache und Einstellung von `PersistWBC` auf "true":

```
New-ProvScheme
-CleanOnBoot
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com
   /2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
   XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"
   UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"
   StringProperty`" Name=`"StorageAccountType`" Value=`"Premium_LRS`"
   /><Property xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
   Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`" Name
   =`"PersistWBC`" Value=`"true`" /></CustomProperties>"
-HostingUnitName "adSubnetScale1"
-IdentityPoolName "BV-WBC1-CAT1"
-MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
   GoldImages.resourcegroup\W10MCSIO-01
   _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
-NetworkMapping @{
```



```
 "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.folder\
    CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
    adSubnetScale1.network" }

-ProvisioningSchemeName "BV-WBC1-CAT1"
-ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
   folder\Standard_D2s_v3.serviceoffering"
-UseWriteBackCache
-WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256
<!--NeedCopy-->
```

Unterstützung der AWS-Host-Tenancy

Sie können mit MCS dedizierte AWS-Hosts bereitstellen. Ein Administrator kann einen Katalog mit Maschinen erstellen, deren Host-Tenancy über PowerShell definiert wird.

Ein dedizierter Amazon [EC2]-Host ist ein physischer Server mit [EC2]-Instanzkapazität, der vollständig dediziert ist und die Verwendung vorhandener Socket- oder VM-Softwarelizenzen gestattet.

Für dedizierte Hosts gilt eine voreingestellte Nutzung basierend auf dem Instanztyp. Ein einzelner dedizierter Host des Instanztyps C4 Large ist beispielsweise auf die Ausführung von 16 Instanzen beschränkt. Weitere Informationen finden Sie auf der AWS-Website.

Voraussetzungen für die Bereitstellung auf AWS-Hosts:

- Ein importiertes Bring Your Own License-Image (AMI). Mit dedizierten Hosts können Sie Ihre vorhandenen Lizenzen verwenden und verwalten.
- Eine Zuordnung dedizierter Hosts mit ausreichender Nutzungskapazität.
- Aktiviertes **Auto-Placement**.

Verwenden Sie zur Bereitstellung auf einem dedizierten Host in AWS mit PowerShell das Cmdlet **New-ProvScheme** mit dem auf *Host* festgelegten Parameter "TenancyType".

Weitere Informationen finden Sie in der Citrix Dokumentation für Entwickler.

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 Citrix Provisioning verwenden, können Sie entweder ein Masterimage oder einen physischen Computer als Masterzielgerät verwenden. Die Terminologie in Bezug auf Images ist bei Citrix Provisioning anders als bei MCS. Informationen hierzu finden Sie in der Dokumentation von Citrix Provisioning.
- 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 Microsoft Key Management Server-Aktivierung 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.

Installieren und konfigurieren Sie die folgende Software auf dem Masterimage:

- Integrationstools für den Hypervisor (z. B. Citrix VM 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 Citrix Provisioning 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 Citrix Provisioning erstellen Sie eine VHD-Datei für den virtuellen Datenträger von Ihrem Masterzielgerät, bevor Sie das Masterzielgerät in eine Domäne einbinden. Informationen hierzu finden Sie in der Dokumentation von Citrix Provisioning.
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.

Erstellen eines Maschinenkatalogs mit Studio

Lesen Sie diesen Abschnitt, bevor Sie den Assistenten zum Erstellen von Katalogen starten.

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 folgenden Elemente. Die angezeigten Assistentenseiten unterscheiden sich je nach der von Ihnen vorgenommenen Auswahl.

Betriebssystem

Jeder Katalog enthält nur Maschinen eines Typs. Wählen Sie eine Option aus.

- **Multisitzungs-OS:** Ein Katalog für Multisitzungs-OS bietet gehostete freigegebene Desktops. 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.
- **Einzelsitzungs-OS:** Ein Einzelsitzungs-OS-Katalog stellt VDI-Desktops bereit, die Sie verschiedenen Benutzern zuweisen 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 wird.

- 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:** (zuvor "Provisioning Services") verwaltet Zielgeräte als Gerätesammlung. Ein als Image eines Masterzielgeräts erstellter virtueller Datenträger in Citrix Provisioning liefert Desktops und Anwendungen.

  > **Hinweis:**
  >
  > Diese Option wird nicht mehr unterstützt. Verwenden Sie den **Exportassistenten für Citrix Provisioning-Geräte**, um ein Citrix Provisioning-Zielgerät in einen Citrix Virtual Apps and Desktops-Katalog zu importieren.

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

- Benutzeränderungen am Desktop auf separater persönlicher vDisk speichern (Persönliche vDisk ist veraltet.)
- Benutzeränderungen am Desktop auf dem lokalen Datenträger speichern
- Änderungen verwerfen und virtuelle Desktops bei Abmeldung entfernen Wählen Sie diese Option, wenn Sie den Benutzerpersonalisierungslayer verwenden.

Masterimage

Diese Seite wird nur angezeigt, wenn Sie VMs mit MCS erstellen.

Wählen Sie auf der Seite **Masterimage** 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 Citrix Provisioning 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), enthält der Assistent zum Erstellen von Maschinenkatalogen zusätzliche Seiten für den spezifischen Host.

Einzelheiten finden Sie unter Informationen zu Verbindungstypen.

Gerätesammlung

Diese Seite wird nur angezeigt, wenn Sie VMs mit Citrix Provisioning erstellen.

Die Seite **Gerätesammlung** enthält die Gerätesammlungen und Geräte, die noch keinem Katalog hinzugefügt wurden.

Wählen Sie die gewünschten Gerätesammlungen.

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:

- Legen Sie fest, wie viele virtuelle Maschinen erstellt werden sollen.
- Wählen Sie die Menge Arbeitsspeicher in MB für jede VM.
- 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 die Größe des virtuellen Datenträgers in GB 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.

Wenn Sie Citrix Provisioning verwenden:

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:

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 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 Seite sind.

Bei der Verwendung von Citrix Provisioning oder anderer Tools (nicht MCS) führen Sie folgende Schritte aus:

Ein Symbol und eine QuickInfo für jede hinzugefügte (bzw. importierte oder aus einer Citrix Provisioning-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. Um Features zu verwenden, die in neueren Produktversionen eingeführt wurden ist 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 nicht registriert werden.

In einem Menü am unteren Rand der Seite **Maschinen** (bzw. **Geräte**) kann die VDA-Mindestebene festgelegt werden. Damit wird die Mindestfunktionsstufe des Katalogs festgelegt. 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 Citrix Virtual Apps and Desktops-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: Version 7.17 enthält zwar einen VDA der Version 7.17, die Standardfunktionsebene ("7.9 oder später") ist jedoch weiterhin die aktuelle. Nach der Installation bzw. einem Upgrade der Komponenten von Version 7.9-7.16 auf 7.17 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 mit dem Assistenten fortfahren. Betroffene Maschinen können in der Regel später keine Registrierung bei einem Controller durchführen. 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 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 Multisitzungs-OS-Katalog oder das Hinzufügen einer für die zufällige Zuteilung erstellten Einzelsitzungs-OS-Maschine zu einem Katalog mit statischen Maschinen.

> **Wichtig:**
>
> Für Release 1811 wurde eine zusätzliche Funktionsebene hinzugefügt: **1811 (oder neuer)**. Die Ebene ist für die Verwendung mit künftigen Citrix Virtual Apps and Desktops-Features vorgesehen. Die Standardebene ist weiterhin **7.9 (oder neuer)**. Die Standardebene gilt derzeit für alle Bereitstellungen.
>
> Wenn Sie **1811 (oder neuer)** auswählen können sich VDAs älterer Versionen in dem Katalog nicht mehr bei einem Controller oder Cloud Connector registrieren. Wenn der Katalog jedoch nur VDAs der Version 1811 oder neuer enthält, können sich alle registrieren.

Konfigurieren eines Cache für temporäre Daten

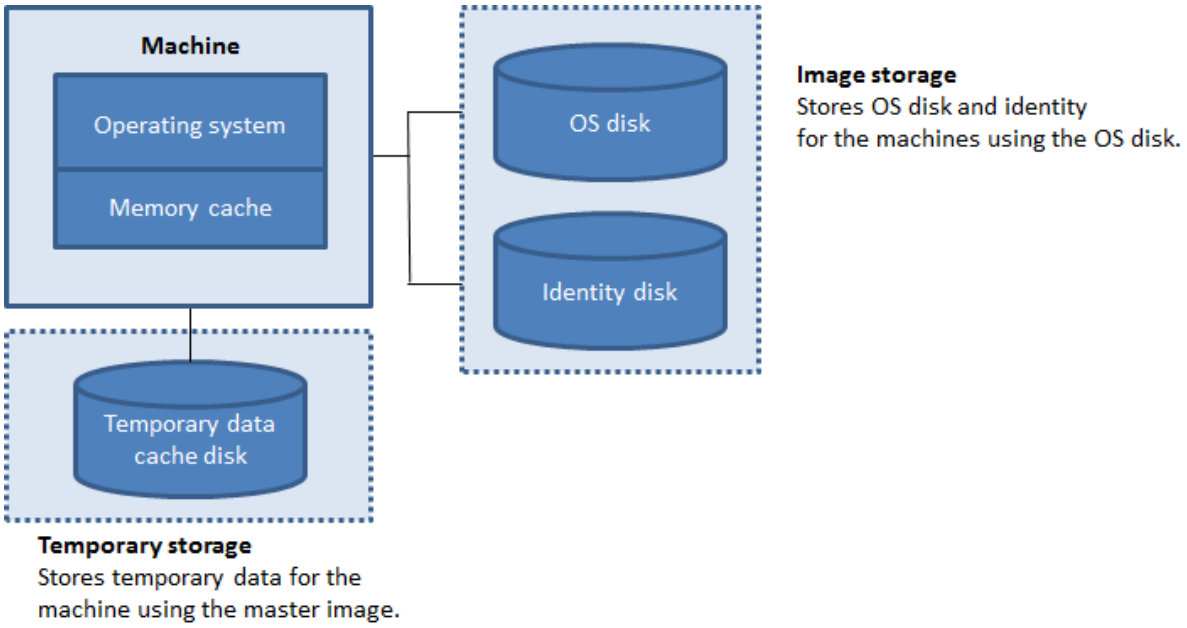
Das lokale Zwischenspeichern temporärer Daten auf VMs ist optional. Sie können den temporären Datencache auf Maschinen aktivieren, wenn Sie MCS zum Verwalten gepoolter (nicht dedizierter) Maschinen in einem Katalog verwenden. Wenn für einen Katalog eine Verbindung verwendet wird, durch die die Speicherung temporärer Daten festgelegt ist, können Sie bei der Katalogerstellung den temporäre Datencache aktivieren und konfigurieren.

> **Wichtig:**
>
> Das Feature erfordert einen aktuellen MCS-E/A-Treiber. Die Installation dieses Treibers ist eine Option, wenn Sie einen VDA installieren oder aktualisieren. Standardmäßig wird der Treiber nicht installiert.

Beim Erstellen einer Verbindung für den Katalog legen Sie fest, ob die temporären Daten in einem freigegebenen oder im lokalen Speicher abgelegt werden. Weitere Informationen finden Sie unter Verbindungen und Ressourcen. Zum Konfigurieren eines Cache für temporäre Daten auf jeder Maschine stehen zwei Optionen zur Auswahl: **Dem Cache zugewiesener Speicher (MB)** und **Größe des Datenträgercache (GB)**. Standardmäßig sind beide Optionen deaktiviert. Zum Aktivieren der Option "Dem Cache zugewiesener Speicher (MB)"aktivieren Sie das Kontrollkästchen "Größe des Datenträgercache (GB)". Wenn das Kontrollkästchen **Größe des Datenträgercache** nicht aktiviert ist, ist die Option "Dem Cache zugewiesener Speicher"ausgegraut. Die Standardwerte der Optionen können je nach Verbindungstyp variieren. Im Allgemeinen sind die Standardwerte für die meisten Fälle ausreichend. Berücksichtigen Sie jedoch den benötigten Platz für:

- 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 Daten von Anwendungen, die Benutzer möglicherweise sitzungsintern installieren

Windows gestattet nicht, dass für eine Sitzung 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.



Beachten Sie beim Konfigurieren eines Cache für temporäre Daten auf den Maschinen die folgenden drei Szenarien:

- Wenn Sie die Optionen "Größe des Datenträgercache"und "Dem Cache zugewiesener Speicher" nicht aktivieren, werden temporäre Daten nicht zwischengespeichert. Sie werden für jede VM direkt auf den differenzierenden Datenträger (im Betriebssystemspeicher) geschrieben. (Dies ist die Provisioningaktion in Version 7.8 und davor.)
- Wenn Sie das Kontrollkästchen "Größe des Datenträgercache"aktivieren und das Kontrollkästchen "Dem Cache zugewiesener Speicher"deaktiviert lassen, werden temporäre Daten direkt auf den Cachedatenträger geschrieben, wobei ein minimale Menge an Speichercache verwendet wird.
- Wenn Sie "Größe des Datenträgercache "und "Dem Cache zugewiesener Speicher"aktivieren, werden temporäre Daten zuerst 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.

> **Wichtig:**
>
> - Wenn auf dem Datenträgercache nicht mehr genügend Speicherplatz vorhanden ist, wird die Sitzung des Benutzers unbrauchbar.
> - 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 Erstellung der VM nicht geändert werden.

Hinweis:

- Der Speichercache ist Teil der Gesamtspeichermenge auf jeder Maschine. Wenn Sie das Kontrollkästchen "Dem Cache zugewiesener Speicher"aktivieren, sollten Sie daher ggf. die Gesamtspeichergröße auf jeder Maschine erhöhen.
- 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.

Netzwerkkarten

Diese Seite wird nicht angezeigt, wenn Sie einen Katalog für Remote-PC-Zugriff-Maschinen erstellen.

Wenn Sie mehrere Netzwerkkarten (NICs) verwenden möchten, weisen Sie auf der Seite **Netzwerkkarten** jeder Karte 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 auf der Seite **Maschinenkonten** 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 auf der Seite **Computerkonten** an, ob Konten erstellt oder vorhandene Konten verwendet werden sollen, und geben Sie den Speicherort für diese Konten an.

- Beim Erstellen von Konten müssen Sie berechtigt sein, Computerkonten in der Organisationseinheit zu erstellen, in der sich die Maschinen befinden.

  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 Aktivieren 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 Citrix Provisioning erstellt wurden, werden Computerkonten für Zielgeräte anders verwaltet. Weitere Informationen hierzu finden Sie in der Dokumentation zu Citrix Provisioning.

Zusammenfassung, Name und Beschreibung

Überprüfen Sie auf der Seite **Zusammenfassung** die von Ihnen angegebenen Informationen. Geben Sie einen Namen und eine Beschreibung für den Katalog ein. Diese Informationen werden in Studio angezeigt.

Wenn Sie fertig sind, klicken Sie auf **Fertig stellen**, um das Erstellen des Katalogs zu starten.

Problembehandlung

> **Wichtig:**
>
> Wenn Sie den Maschinenkatalog mit Citrix Studio erstellt haben, können Sie den PowerShell-Befehl `Get-ProvTask` nicht mehr zum Abrufen der Aufgaben für die Erstellung des Maschinenkatalogs verwenden. Diese Einschränkung ist die Folge der Tatsache, dass Studio diese Aufgaben nach der Erstellung des Maschinenkatalogs löscht, unabhängig davon, ob die Erstellung erfolgreich verlief.

Citrix empfiehlt, Protokolle zu erstellen, um die Arbeit des Supportteams zu unterstützen. Führen Sie bei Verwendung von Citrix Provisioning folgende Schritte zum Generieren von Protokolldateien aus:

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 Snapshot.
3. Führen Sie den folgenden PowerShell-Befehl auf dem Delivery Controller aus: `Set-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown -Value $True`.
4. Erstellen Sie einen Katalog basierend auf diesem Snapshot.
5. Wenn die Vorbereitungs-VM auf dem Hypervisor erstellt wurde, melden Sie sich an und extrahieren Sie folgende Dateien aus dem Stammverzeichnis von C:\: Image-prep.log und 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_NoAutoShutdown`.

So geht es weiter

Wenn Sie den ersten Katalog erstellen, werden Sie von Studio zum Erstellen einer Bereitstellungsgruppe geleitet.

Maschinenkataloge verwalten

May 10, 2023

Einführung

Sie können Maschinen in Maschinenkatalogen hinzufügen, entfernen und umbenennen, Maschinenbeschreibungen ändern und die Active Directory-Computerkonten des Katalogs verwalten.

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 Maschinenerstellungsdienste (MCS) erstellt wurden, können Sie pflegen, indem Sie das Masterimage des Katalogs und dann die Maschinen aktualisieren. So können Sie eine große Anzahl Maschinen effizient aktualisieren.
- Bei mit Citrix Provisioning erstellten Maschinen werden Updates über den virtuellen Datenträger verteilt. Informationen hierzu finden Sie in der Dokumentation von Citrix Provisioning.
- Bei Katalogen mit statischen (permanent zugewiesenen) oder Remote-PC-Zugriff-Maschinen verwalten Sie Updates an den Benutzermaschinen Studio-extern. Tun Sie dies entweder für einzelne Maschinen oder alle Maschinen mit Bereitstellungssoftware von Drittanbietern.

Weitere Informationen zum Erstellen und Verwalten von Verbindungen mit Hosthypervisors und Clouddiensten finden Sie unter Verbindungen und Ressourcen.

> **Hinweis:**
>
> MCS unterstützt Windows 10 IoT Core und Windows 10 IoT Enterprise nicht. Weitere Informationen finden Sie auf der Website von Microsoft.

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 Image. Bereits vorhandene Instanzen verwenden weiterhin die ursprüngliche Instanz. 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 zum 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.

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.

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 eines Katalogs

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 Katalogen mit Maschinen für Einzelsitzungs- und Multisitzungs-OS. 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. Rollback oder Wiederherstellen von Maschinen in einem Katalog, um die vorherige Masterimageversion zu verwenden. Führen Sie diese Aufgabe aus, wenn Benutzer Probleme durch Updates haben, die Sie auf den Desktops bereitgestellt haben, um Ausfallzeiten zu minimieren. Masterimages dürfen nicht gelöscht, verschoben oder umbenannt werden, da ansonsten Kataloge nicht auf ihre Verwendung zurückgesetzt werden können.

Bei Maschinenkatalogen, die Citrix Provisioning (zuvor "Provisioning Services") verwenden, müssen Sie einen neuen virtuellen Datenträger veröffentlichen, um Änderungen auf den Katalog anzuwenden. Informationen hierzu finden Sie in der Dokumentation zu Citrix Provisioning.

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 Citrix Hypervisor-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.
5. Überprüfen Sie die Informationen auf der Seite **Zusammenfassung** und klicken Sie auf **Fertig stellen**. Jede Maschine wird nach erfolgter Aktualisierung automatisch neu gestartet.

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 Citrix Provisioning verwenden, aktualisieren Sie die VDA-Version. Die Provisioning Konsole behält die VDA-Version nicht bei. Citrix Provisioning kommuniziert direkt mit dem Citrix Virtual Apps and Desktops-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.
- Informationen zum Beheben von Problemen bei VMs, für die ständig ein unbekannter Energiezustand angezeigt wird, finden Sie unter How to fix VMs that continuously show an unknown power state.

Erstellen von Bereitstellungsgruppen

September 21, 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 auf der Seite **Maschinen** 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.
- Die folgenden Kompatibilitätsprüfungen werden durchgeführt:
  - MinimumFunctionalLevel muss kompatibel sein
  - SessionSupport muss kompatibel sein
  - AllocationType muss für SingleSession kompatibel sein
  - ProvisioningType muss kompatibel sein
  - PersistChanges muss für MCS und Citrix Provisioning kompatibel sein
  - Der RemotePC-Katalog ist nur mit dem RemotePC-Katalog kompatibel
  - AppDisk-bezogene Überprüfung

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 aktivieren.

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

AppDisks sind veraltet.

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.

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. In der Standardeinstellung gilt die Anwendungsanspruch-Richtlinienregel für alle Benutzer. Weitere Informationen finden Sie in den `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 der Citrix Workspace-App 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 der Citrix Workspace-App 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 "Anon*XYZ*"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

Schritt 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 der Citrix Workspace-App doppelt angezeigt.

Klicken Sie auf **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 unter 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

Der Titel dieser Seite hängt davon ab, welchen Maschinenkatalog Sie auf der Seite **Maschinen** ausgewählt haben:

- Wenn Sie einen Maschinenkatalog mit gepoolten Maschinen gewählt haben, lautet der Titel **Desktops**.
- Wenn Sie einen Katalog mit zugewiesenen Maschinen gewählt und auf der Seite **Bereitstellungstyp** "Desktops"gewählt haben, ist der Titel **Desktopbenutzerzuweisungen**.
- Wenn Sie einen Katalog mit zugewiesenen Maschinen gewählt und auf der Seite **Bereitstellungstyp** "Anwendungen"gewählt haben, ist 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 der Citrix Workspace-App 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 unter 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**.

Maximale Desktopinstanzen in einer Site (nur PowerShell)

Konfigurieren der maximalen Desktopinstanzen in einer Site (nur PowerShell):

- Verwenden Sie in PowerShell das geeignete BrokerEntitlementPolicyRule-Cmdlet mit dem Parameter "MaxPerEntitlementInstances". Mit dem folgenden Cmdlet wird beispielsweise die Regel "tsvda-desktop"so geändert, dass die in der Site maximal zulässige Zahl der Instanzen eines Desktops auf zwei festgelegt wird. Werden zwei Desktopinstanzen ausgeführt und ein dritter Abonnent versucht, einen Desktop zu starten, tritt ein Fehler auf.

  ```
  Set-BrokerEntitlementPolicyRule -Name tsvda-desktop -MaxPerEntitlementInst
    2
  ```

- Hilfe können Sie mit dem Cmdlet "Get-Help"aufrufen. Beispiel: `Get-Help Set-BrokerEntitlementPolicyRule-Parameter MaxPerEntitlementInstances`.

Schritt 7. Zusammenfassung

Geben Sie einen Namen für die Bereitstellungsgruppe ein. Sie können optional eine Beschreibung eingeben, die in der Citrix Workspace-App 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

November 14, 2022

Einführung

In diesem Artikel werden Verfahren zum Verwalten von Bereitstellungsgruppen über die Verwaltungskonsole 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.

Die Verfahren sind nach Kategorien geordnet: Allgemeines, Benutzer, Maschinen und Sitzungen. Einige Aufgaben fallen in mehrere Kategorien. Das Thema "Unterbinden der Benutzerverbindung mit Maschinen"wird beispielsweise in der Kategorie "Maschinen"beschrieben, es betrifft aber auch Benutzer. Wenn Sie eine Aufgabe unter einer Kategorie nicht finden, schauen Sie unter einer verwandten Kategorie nach.

Auch andere Artikel enthalten verwandte Informationen:

- Unter Anwendungen finden Sie Informationen zur Verwaltung von Anwendungen in Bereitstellungsgruppen.
- Das Verwalten von Bereitstellungsgruppen erfordert die Berechtigungen des Bereitstellungsgruppen-Administrators. Weitere Informationen finden Sie unter Delegierte Administration.

Allgemein

- Ändern der Bereitstellungsmethode
- Ändern der StoreFront-Adressen
- Aktualisieren einer Bereitstellungsgruppe
- Verwalten von Remote-PC-Zugriff-Bereitstellungsgruppen

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 Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Bereitstellungsgruppe und klicken Sie im Aktionsbereich auf **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. Alternativ klicken Sie auf **OK** um die Konfigurationsänderungen anzuwenden und das Fenster zu schließen.

Ändern der StoreFront-Adressen

1. Wählen Sie im Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Bereitstellungsgruppe und klicken Sie im Aktionsbereich auf **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 Workspace-App-Instanz verwendet werden sollen.

4. Klicken Sie auf **Anwenden**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt. Alternativ klicken Sie auf **OK** um die Konfigurationsänderungen anzuwenden und das Fenster zu schließen.

Sie können die StoreFront-Serveradresse auch festlegen, indem Sie im Navigationsbereich **Konfiguration > StoreFront** auswählen.

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 Citrix Provisioning (zuvor "Provisioning Services") verwenden, aktualisieren Sie die VDA-Version in der Citrix Provisioning Console.
- Starten Sie die Maschinen mit dem aktualisierten VDA, damit sie sich bei dem Delivery Controller registrieren können. Dadurch wird in der Konsole 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 der Upgrade-Dokumentation.

Bereitstellungsgruppen aktualisieren:

1. Wählen Sie im Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Bereitstellungsgruppe und klicken Sie im Aktionsbereich auf **Upgrade von Bereitstellungsgruppe durchführen**. Die Aktion **Upgrade von Bereitstellungsgruppe durchführen** wird nur angezeigt, wenn aktualisierte VDAs erkannt werden.

Es wird angezeigt, welche Maschinen ggf. nicht aktualisiert werden können 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 auswählen und dann im Aktionsbereich auf **Rückgängig machen** klicken.

Verwalten von Remote-PC-Zugriff-Bereitstellungsgruppen

Wenn eine Maschine eines Remote-PC-Zugriff-Maschinenkatalogs keinem Benutzer zugewiesen wurde, wird sie vorübergehend einer Bereitstellungsgruppe zugewiesen, 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. Die Priorität legen Sie mit dem PowerShell-SDK fest.

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 Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Remote-PC-Zugriff-Gruppe aus.
3. Klicken Sie im Abschnitt **Details** auf die Registerkarte **Maschinenkataloge** und wählen Sie einen Remote-PC-Zugriff-Maschinenkatalog.
4. Um eine Zuordnung hinzuzufügen oder wiederherzustellen, klicken Sie auf **Desktops hinzufügen**. Zum Entfernen einer Zuordnung klicken Sie auf **Zuordnung entfernen**.

Benutzer

- Ändern der Benutzereinstellungen
- Hinzufügen oder Entfernen von Benutzern

Ändern der Benutzereinstellungen für eine Bereitstellungsgruppe

Der Name dieser Seite lautet **Benutzereinstellungen** oder **Grundeinstellungen**.

1. Wählen Sie im Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Bereitstellungsgruppe und klicken Sie im Aktionsbereich auf **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. Alternativ klicken Sie auf **OK** um die Konfigurationsänderungen anzuwenden und das Fenster zu schließen.

Einstellung	Beschreibung
Beschreibung	Text, der in Citrix Workspace (oder StoreFront) angezeigt wird
Bereitstellungsgruppe aktivieren	Zeigt an, ob die Bereitstellungsgruppe aktiviert ist.
Zeitzone	Die Zeitzone, die für die Maschinen dieser Bereitstellungsgruppe gelten muss. Die Option listet die von der Site unterstützten Zeitzonen auf.
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 unter Benutzer.

1. Wählen Sie im Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Bereitstellungsgruppe und klicken Sie im Aktionsbereich auf **Bereitstellungsgruppe bearbeiten**.
3. Gehen Sie auf der Seite **Benutzer** folgendermaßen vor:
   - 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**.
   - Aktivieren oder deaktivieren Sie das Kontrollkästchen zur Steuerung des Zugriffs durch nicht authentifizierte Benutzer.
4. Klicken Sie auf **Anwenden**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt. Alternativ klicken Sie auf **OK** um die Konfigurationsänderungen anzuwenden

und das Fenster zu schließen.

Importieren und Exportieren von Benutzerlisten Bei Bereitstellungsgruppen mit physischen Maschinen mit Windows-Einzelsitzungs-OS 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 Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Bereitstellungsgruppe und klicken Sie im Aktionsbereich auf **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. Alternativ klicken Sie auf **OK** um die Konfigurationsänderungen anzuwenden und das Fenster zu schließen.

Maschinen

- Ändern der Maschinen-Benutzer-Zuweisung
- Ändern der maximalen Anzahl Maschinen pro Benutzer
- Aktualisieren einer Maschine
- Hinzufügen, Ändern oder Entfernen von Tagbeschränkungen für einen Desktop
- Entfernen einer Maschine
- Einschränken des Zugriffs auf Maschinen
- Unterbinden der Benutzerverbindung mit Maschinen (Wartungsmodus)
- Herunterfahren und Neustart von Maschinen
- Erstellen und Verwalten von Neustartzeitplänen für Maschinen
- Lastverwaltung bei Maschinen
- Energieverwaltung für Maschinen

Ändern der Maschinen-Benutzer-Zuweisung in einer Bereitstellungsgruppe

Sie können die Zuweisungen von Maschinen mit Windows-Einzelsitzungs-OS ändern, die mit MCS bereitgestellt wurden. Die Zuweisungen für Maschinen mit Windows-Multisitzungs-OS und mit Citrix Provisioning bereitgestellte Maschinen können Sie nicht ändern.

1. Wählen Sie im Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Bereitstellungsgruppe und klicken Sie im Aktionsbereich auf **Bereitstellungsgruppe bearbeiten**.
3. Geben Sie die neuen Benutzer auf der Seite **Desktops** bzw. **Desktopzuweisungsregeln** (Seitentitel abhängig vom Typ des Maschinenkatalogs) an.
4. Klicken Sie auf **Anwenden**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt. Alternativ klicken Sie auf **OK** um die Konfigurationsänderungen anzuwenden und das Fenster zu schließen.

Ändern der maximalen Anzahl Maschinen pro Benutzer in einer Bereitstellungsgruppe

1. Wählen Sie im Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Bereitstellungsgruppe und klicken Sie im Aktionsbereich auf **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. Alternativ klicken Sie auf **OK** um die Konfigurationsänderungen anzuwenden und das Fenster zu schließen.

Aktualisieren einer Maschine in einer Bereitstellungsgruppe

1. Wählen Sie im Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Gruppe und klicken Sie im Aktionsbereich auf **Maschinen anzeigen**.
3. Wählen Sie eine Maschine und klicken Sie im Aktionsbereich auf **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**. Geben Sie anschließend Folgendes an:

- Zeitpunkt der Aktualisierung des Masterimages: jetzt oder beim nächsten Neustart
- Neustart-Verteilungszeit (Zeit insgesamt, während derer das Update aller Maschinen beginnen soll)
- Ob Benutzer über den Neustart benachrichtigt werden
- Meldung, die die Benutzer erhalten sollen

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 Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Bereitstellungsgruppe und klicken Sie im Aktionsbereich auf **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. Ändern oder Entfernen einer Tagbeschränkung:
   - Wählen Sie ein anderes Tag.
   - Entfernen Sie die Tagbeschränkung durch Deaktivieren von **Starts auf Maschinen mit Tag beschränken**.
6. Klicken Sie auf **Anwenden**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt. Alternativ klicken Sie auf **OK** um die Konfigurationsänderungen anzuwenden und das Fenster zu schließen.

Entfernen von Maschinen aus Bereitstellungsgruppen

Durch Entfernen von Maschinen werden diese aus Bereitstellungsgruppen gelöscht. Sie werden jedoch nicht aus dem Maschinenkatalog der Bereitstellungsgruppe gelöscht. 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. Ziehen Sie ggf. ein Reimaging solcher Maschinen in Betracht.

1. Wählen Sie im Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Gruppe und klicken Sie im Aktionsbereich auf **Maschinen anzeigen**.
3. Stellen Sie sicher, dass die Maschine heruntergefahren ist.
4. Wählen Sie die Maschine aus und klicken Sie auf im Aktionsbereich auf **Aus Bereitstellungsgruppe entfernen**.

Sie können eine Maschine auch über die von der Maschine verwendete Verbindung aus einer Bereitstellungsgruppe entfernen.

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 unter Delegierte Administration.
- **Einschränken des Zugriffs für Benutzer über SmartAccess-Richtlinienausdrücke:** Verwenden Sie Richtlinienausdrücke, mit denen über Citrix Gateway hergestellte Benutzerverbindungen gefiltert werden.

  1. Wählen Sie im Navigationsbereich **Bereitstellungsgruppen** aus.
  2. Wählen Sie eine Bereitstellungsgruppe und klicken Sie im Aktionsbereich auf **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 Citrix 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 Citrix Gateway.
  5. Klicken Sie auf **Anwenden**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt. Alternativ klicken Sie auf **OK** um die Konfigurationsänderungen anzuwenden und das Fenster zu schließen.

- **Einschränken des Zugriffs für Benutzer über Ausschlussfilter:** Verwenden Sie 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 im Skript `Set-BrokerAccessPolicy` auf `VPDesktops_*` auf beide Maschinen angewendet.

Wenn Sie über einen Webbrowser verbunden sind oder die Citrix Workspace-App-Benutzeroberfläche im Store aktiviert ist, können Sie keinen Ausschlussfilter auf Basis des Clientnamens verwenden.

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 eine Maschine mit Windows-Multisitzungs-OS im Wartungsmodus ist, können Benutzer eine Verbindung mit vorhandenen Sitzungen herstellen, aber keine neuen Sitzungen starten.
- Bei einer Maschine mit Windows-Einzelsitzungs-OS (oder 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 Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Gruppe aus.
3. Zum Aktivieren des Wartungsmodus für alle Maschinen in der Bereitstellungsgruppe klicken Sie im Aktionsbereich auf **Wartungsmodus einschalten**.

   Zum Aktivieren des Wartungsmodus für einzelne Maschinen klicken Sie im Aktionsbereich auf **Maschinen anzeigen**. Wählen Sie eine Maschine aus und klicken Sie im Aktionsbereich auf **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 Multisitzungs-OS-Maschine 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 den Wartungsmodus auch für Folgendes ein- oder ausschalten:

- Verbindungen, dies wirkt sich auf die Maschinen aus, die die Verbindung verwenden.
- Maschinenkataloge, dies wirkt sich auf die Maschinen in dem betreffenden Katalog aus.

Herunterfahren und Neustarten von Maschinen in einer Bereitstellungsgruppe

Dieser Vorgang wird für Remote-PC-Zugriff-Maschinen nicht unterstützt.

1. Wählen Sie im Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Gruppe und klicken Sie im Aktionsbereich auf **Maschinen anzeigen**.
3. Wählen Sie die Maschine und klicken Sie im Aktionsbereich auf einen der folgenden Einträge (einige Optionen sind je nach Maschinenzustand ggf. nicht verfügbar):

    - **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 die Maschine im aktuellen Zustand.
    - **Neustart erzwingen:** Das Betriebssystem wird zwangsweise heruntergefahren und die Maschine dann neu gestartet.
    - **Anhalten:** Die Maschine wird ohne Herunterfahren angehalten die Liste der Maschinen wird aktualisiert.
    - **Herunterfahren:** Das Betriebssystem wird aufgefordert, herunterzufahren.

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 Maschinen mit Windows-Einzelsitzungs-OS während einer Sitzung nicht zulassen. Einzelheiten finden Sie in der Microsoft-Dokumentation zu Richtlinien.

Sie können auch Maschinen mit Verbindung herunterfahren und neu starten.

Erstellen und Verwalten von Neustartzeitplänen für Maschinen in einer Bereitstellungsgruppe

Über einen Neustartzeitplan wird der regelmäßige Neustart aller Maschinen in einer Bereitstellungsgruppe festgelegt. Sie können einen oder mehrere Zeitpläne für eine Bereitstellungsgruppe erstellen. Ein Zeitplan kann sich auf Folgendes auswirken:

- Alle Maschinen in der Gruppe
- Eine oder mehrere (aber nicht alle) Maschinen Die Maschinen werden durch ein Tag identifiziert. Es handelt sich hierbei um eine "Tagbeschränkung", da die Aktion auf Elemente (in diesem Fall Maschinen) beschränkt wird, die über das Tag verfügen.

Angenommen, alle Maschinen befinden sich in einer Bereitstellungsgruppe. Sie möchten alle Maschinen mindestens einmal wöchentlich neu starten. Die Maschinen der Buchhaltung sollen täglich neu gestartet werden. Sie richten hierzu einen Zeitplan für alle Maschinen und einen weiteren für die Maschinen der Buchhaltung ein.

Ein Zeitplan enthält Datum und Uhrzeit des Beginns sowie die Dauer des Neustarts. Die Dauer repräsentiert entweder das Neustarten aller betroffenen Maschinen gleichzeitig oder ein Intervall, das für die Neustarts benötigt wird.

Sie können Zeitpläne aktivieren und deaktivieren. Das Deaktivieren kann beim Testen, während bestimmter Zeiten oder beim Vorbereiten von Zeitplänen hilfreich sein.

Sie können Zeitpläne nicht für das automatisierte Einschalten oder Herunterfahren über die Verwaltungskonsole verwenden, sondern nur für Neustarts.

Zeitplanüberlagerungen Mehrere Zeitpläne können einander überschneiden. Im obigen Beispiel wirken sich beide Pläne auf die Maschinen der Buchhaltung aus. Die Maschinen können am Sonntag zweimal neu gestartet werden. Der Zeitplancode ist darauf ausgelegt, unerwünschte 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 für die Buchhaltung (je nach der jeweils konfigurierten Dauer).

Weitere Informationen zu Neustartplänen finden Sie unter Reboot schedule internals.

Anzeigen von Neustartzeitplänen

1. Wählen Sie im Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Bereitstellungsgruppe und klicken Sie im Aktionsbereich auf **Bereitstellungsgruppe bearbeiten**.
3. Wählen Sie die Seite **Neustartzeitplan**.

Die Seite **Neustartzeitplan** enthält die folgenden Informationen für jeden konfigurierten Zeitplan:

- Zeitplanname
- Gegebenenfalls verwendete Tagbeschränkung
- Anzahl der Maschinenneustarts
- Ob Maschinenbenutzer eine Benachrichtigung erhalten
- Ob der Zeitplan aktiviert ist. Das Deaktivieren kann beim Testen, während bestimmter Zeiten oder beim Vorbereiten von Zeitplänen hilfreich sein.

Hinzufügen (Anwenden) von Tags Wenn Sie einen Neustartzeitplan mit einer Tagbeschränkung konfigurieren, stellen Sie sicher, dass das Tag den Maschinen hinzugefügt wird (bzw. auf sie angewendet wird), auf die der Zeitplan angewendet werden soll. Im obigen Beispiel wird ein Tag auf jede Maschine der Buchhaltung angewendet. Einzelheiten finden Sie unter Tags.

Sie können zwar mehrere Tags auf eine Maschine anwenden, ein Neustartzeitplan kann jedoch nur ein Tag enthalten.

1. Wählen Sie im 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. Klicken Sie im Aktionsbereich auf **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**.

Erstellen eines Neustartzeitplans

1. Wählen Sie im Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Bereitstellungsgruppe und klicken Sie im Aktionsbereich auf **Bereitstellungsgruppe bearbeiten**.
3. Klicken Sie auf der Seite **Neustartzeitplan** auf **Hinzufügen**.
4. Führen Sie auf der Seite **Neustartzeitplan** folgende Schritte aus:

    - Geben Sie einen Namen und eine Beschreibung für den Zeitplan ein.
    - Wenn Sie eine Tagbeschränkung verwenden möchten, wählen Sie das Tag aus.
    - Legen Sie unter **Neustartintervall** fest, wie oft der Neustart durchgeführt werden soll: täglich, an Werktagen, am Wochenende oder an einem bestimmten Wochentag.
    - Geben Sie die Tageszeit an, zu der der Neustart beginnen soll.
    - 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.
    - Wählen Sie unter **Benachrichtigung an Benutzer senden** 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 unter Benachrichtigungsintervall vorgeben, dass die Meldung alle fünf Minuten nach Erstanzeige wiederholt werden soll. Standardmäßig wird die Meldung nicht wiederholt angezeigt.
    - Geben Sie den Titel und den Text der Benachrichtigung 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. Der Wert verringert sich in jeder wiederholten Nachricht um fünf Minuten. Sofern Sie keinen gleichzeitigen Neustart aller Maschinen festgelegt haben, wird die Meldung auf jeder Maschine zu der von dem internen Algorithmus berechneten Zeit angezeigt.
    - Aktivieren Sie das Kontrollkästchen, um den Zeitplan zu aktivieren. Deaktivieren Sie das Kontrollkästchen, um den Zeitplan zu deaktivieren.

5. Klicken Sie auf **Anwenden**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt. Alternativ klicken Sie auf **OK** um die Konfigurationsänderungen anzuwenden und das Fenster zu schließen.

Bearbeiten, Entfernen, Aktivieren und Deaktivieren von Neustartzeitplänen

1. Wählen Sie im Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Bereitstellungsgruppe und klicken Sie im Aktionsbereich auf **Bereitstellungsgruppe bearbeiten**.
3. Wählen Sie auf der Seite **Neustartzeitplan** das Kontrollkästchen eines Zeitplans.

    - Um den Zeitplan zu bearbeiten, klicken Sie auf **Bearbeiten**. Aktualisieren Sie die Zeitplankonfiguration gemäß den Anweisungen unter Erstellen eines Neustartzeitplans.
    - Klicken Sie auf **Bearbeiten**, um den Zeitplan zu aktivieren oder zu deaktivieren. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Neustartzeitplan aktivieren**.
    - Klicken Sie zum Entfernen des Zeitplans auf **Löschen**. Bestätigen Sie das Entfernen. Das Entfernen eines Zeitplans hat keine Auswirkungen auf die auf die betroffenen Maschinen angewendeten Tags.

Verzögerung geplanter Neustarts aufgrund eines Datenbankausfalls

> **Hinweis:**
>
> Dieses Feature ist nur über PowerShell verfügbar.

Fällt vor einem geplanten Neustart von Maschinen (VDAs) in einer Bereitstellungsgruppe die Standortdatenbank aus, beginnt der Neustart erst nach Ende des Ausfalls. Dies kann zu unbeabsichtigten Ergebnissen führen.

Angenommen, Sie haben die Neustarts einer Bereitstellungsgruppe für außerhalb der Produktion (ab 3:00 Uhr nachts) geplant. Ein Ausfall der Standortdatenbank tritt eine Stunde vor Beginn des geplanten Neustarts (um 2:00 Uhr) auf. Der Ausfall dauert sechs Stunden (bis 8:00 Uhr). Der Neustartzeitplan beginnt, wenn die Verbindung zwischen dem Delivery Controller und der Standortdatenbank wiederhergestellt ist. Die VDA-Neustarts beginnen jetzt fünf Stunden nach dem ursprünglich geplanten Zeitpunkt. Das kann dazu führen, dass VDAs während der Produktionszeit neu gestartet werden.

Um dies zu vermeiden, können Sie den Parameter `MaxOvertimeStartMins` für die Cmdlets `New-BrokerRebootScheduleV2` und `Set-BrokerRebootScheduleV2` verwenden. Der Wert gibt den maximalen Zeitraum außerhalb der geplanten Startzeit in Minuten an, nach dem ein Neustart-Zeitplan beginnen darf.

Wenn die Datenbankverbindung innerhalb dieser Zeit wiederhergestellt wird (geplante Zeit + `MaxOvertimeStartMins`), beginnt der VDA-Neustart.

Wenn die Datenbankverbindung innerhalb dieser Zeit nicht wiederhergestellt wird, beginnt der VDA-Neustart nicht.

Wird dieser Parameter weggelassen, beginnt der geplante Neustart unabhängig von der Ausfalldauer, sobald die Verbindung zur Datenbank wiederhergestellt wird.

Weitere Informationen finden Sie in der Hilfe zum Cmdlet. Dieses Feature ist nur über PowerShell verfügbar. Sie können diesen Wert nicht festlegen, wenn Sie einen Neustartzeitplan in Studio konfigurieren.

Lastverwaltung von Maschinen in Bereitstellungsgruppen

Die Lastverwaltung ist nur bei Maschinen mit Windows-Multisitzungs-OS 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 Maschine mit Windows-Multisitzungs-OS wird nur für den Lastausgleich berücksichtigt, wenn der Wartungsmodus für sie deaktiviert ist.
- **Serverlastindex:** bestimmt, mit welcher Wahrscheinlichkeit ein Server, der Maschinen mit Windows-Multisitzungs-OS 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 Lastauswertungskriterien werden in den Richtlinieneinstellungen für die Lastverwaltung festgelegt.

  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.

  Sie können den Lastindex in Director (Überwachung), über die Suche in Studio (Verwalten) und im SDK überwachen.

  Wählen Sie in Konsolenanzeigen zum Einblenden der Spalte **Lastindex** (die standardmäßig ausgeblendet ist) eine Maschine, klicken Sie mit der rechten Maustaste auf eine Spaltenüberschrift und wählen Sie **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.

- **Richtlinieneinstellung "Toleranzwert für gleichzeitige Anmeldungen":** maximale Anzahl gleichzeitiger Serveranmeldeanforderungen. (Diese Einstellung entspricht der Lastdrosselung in XenApp-Versionen 6.x.)

  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.

Energieverwaltung für Maschinen in einer Bereitstellungsgruppe

Die Energieverwaltung ist nur bei virtuellen Maschinen mit Windows-Einzelsitzungs-OS, nicht aber bei physischen Maschinen (einschließlich Remote-PC-Zugriff-Maschinen) möglich. Maschinen mit Windows-Einzelsitzungs-OS und GPU-Funktionen können nicht angehalten werden, sodass Energieverwaltungsvorgänge fehlschlagen. Für Maschinen mit Windows-Multisitzungs-OS können Sie einen Neustartzeitplan erstellen.

In Bereitstellungsgruppen mit gepoolten Maschinen können virtuelle Maschinen mit Windows-Einzelsitzungs-OS einen der folgenden Zustände annehmen:

- Zufällig zugewiesen und in Verwendung
- Nicht zugewiesen und nicht verbunden

In Bereitstellungsgruppen mit statischen Maschinen können virtuelle Maschinen mit Windows-Einzelsitzungs-OS 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 des Benutzers 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 zugeordneter Maschinen, die aktiviert werden, wenn die Anzahl der Maschinen im Pool unter einen Schwellenwert fällt. Der Schwellenwert ist ein Prozentsatz der Bereitstellungsgruppengröße. Bei großen Bereitstellungsgruppen wird bei Erreichen des Schwellenwerts evtl. eine große Zahl Maschinen aktiviert. Dies ist beim Planen der Bereitstellungsgruppengröße zu berücksichtigen, alternativ verwenden Sie das SDK, um die Standardpuffergröße anzupassen.

- **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).

Energieverwaltung bei virtuellen Maschinen mit Windows-Einzelsitzungs-OS

1. Wählen Sie im Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Bereitstellungsgruppe und klicken Sie im Aktionsbereich auf **Bereitstellungsgruppe bearbeiten**.
3. Wählen Sie auf der Seite **Energieverwaltung** unter **Energieverwaltung für Maschinen** die Option **Wochentage**. Wochentage umfassen standardmäßig die Tage von Montag bis Freitag.
4. Klicken Sie bei zufälligen Bereitstellungsgruppen unter **Maschinen einschalten** auf **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 unter **Energieverwaltung für Maschinen** die Option **Wochenende** und konfigurieren Sie die Spitzenzeiten und Energiestatustimer für Wochenenden.
8. Klicken Sie auf **Anwenden**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt. Alternativ klicken Sie auf **OK** um die Konfigurationsänderungen anzuwenden und das Fenster zu schließen.

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
- Deaktivieren der Energieverwaltung Siehe CTX217289.

Energieverwaltung von VDI-Maschinen beim Übergang in einen anderen Zeitraum mit getrennten Sitzungen

> **Wichtig:**
>
> Diese Erweiterung gilt nur für VDI-Maschinen mit getrennten Sitzungen. Sie gilt nicht für VDI-Maschinen mit abgemeldeten Sitzungen.

In früheren Versionen blieben VDI-Maschinen beim Übergang in einen Zeitraum, in dem eine Aktion (Trennaktion = **Anhalten** oder **Herunterfahren**) erforderlich war, eingeschaltet. Das Szenario trat auf, wenn eine Maschine während eines Zeitraums (Spitzen- oder Nebenzeit) getrennt wurde, in der keine Aktion (Trennaktion = **Nothing**) erforderlich war.

Ab Citrix Virtual Apps and Desktops 7 1909 werden Maschinen angehalten oder ausgeschaltet, wenn die angegebene Trennzeit abläuft, abhängig von der für den Zielzeitraum konfigurierten Trennaktion.

Beispielsweise konfigurieren Sie die folgenden Energierichtlinien für eine VDI-Bereitstellungsgruppe:

- `PeakDisconnectAction` = Nothing
- `OffPeakDisconnectAction` = Shutdown
- `OffPeakDisconnectTimeout` = 10

> **Hinweis:**
>
> Weitere Informationen zur Energierichtlinie mit Trennaktionen finden Sie unter https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/about_Broker_PowerManagement/#power-policy und https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/.

In früheren Versionen blieben VDI-Maschinen, bei denen während der Spitzenzeit eine Sitzung getrennt wurde, beim Übergang von der Spitzen- in die Nebenzeit eingeschaltet. Ab Citrix Virtual Apps and Desktops 7 1909 werden die Richtlinienaktionen `OffPeakDisconnectAction` und `OffPeakDisconnectTimeout` beim Übergang zu einem neuen Zeitraum auf VDI-Maschinen angewendet. Infolgedessen werden solche Maschine 10 Minuten nach dem Übergang in die Nebenzeit ausgeschaltet.

Wenn Sie zum vorherigen Verhalten zurückkehren möchten (d. h. keine Aktion auf Maschinen mit getrennten Sitzungen beim Übergang von der Spitzen- zur Nebenzeit oder umgekehrt auszuführen), führen Sie einen der folgenden Schritte aus:

- Legen Sie den Registrierungswert "LegacyPeakTransitionDisconnectedBehaviour"auf 1 (wahr, d. h. aktiviert das vorherige Verhalten) fest. Standardmäßig ist der Wert 0 (falsch, d. h. löst beim Übergang die Trennaktion der Energierichtlinie aus).
  - Pfad: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer
  - Name: LegacyPeakTransitionDisconnectedBehaviour
  - Typ: REG_DWORD
  - Wert: 0x00000001 (1)
- Konfigurieren Sie die Einstellung mit dem PowerShell-Befehl `Set-BrokerServiceConfigurationDa` . Beispiel:
  - `PS C:\> Set-BrokerServiceConfigurationData HostingManagement.LegacyPeakTransitionDisconnectedBehaviour -SettingValue $true`

Eine Maschine muss die folgenden Kriterien erfüllen, damit Energierichtlinienaktionen beim Zeitraumwechsel auf sie angewendet werden können:

- Es liegt eine getrennte Sitzung vor.
- Es stehen keine Energieaktionen aus.
- Sie gehört zu einer VDI-Bereitstellungsgruppe (für Einzelsitzungen), die in einen anderen Zeitraum übergeht.
- Es liegt eine Sitzung vor, die während eines bestimmten Zeitraums (Spitzen- oder Nebenzeit) getrennt wurde und die Maschine wechselt zu einem Zeitraum, für den eine Energieaktion zugewiesen ist.

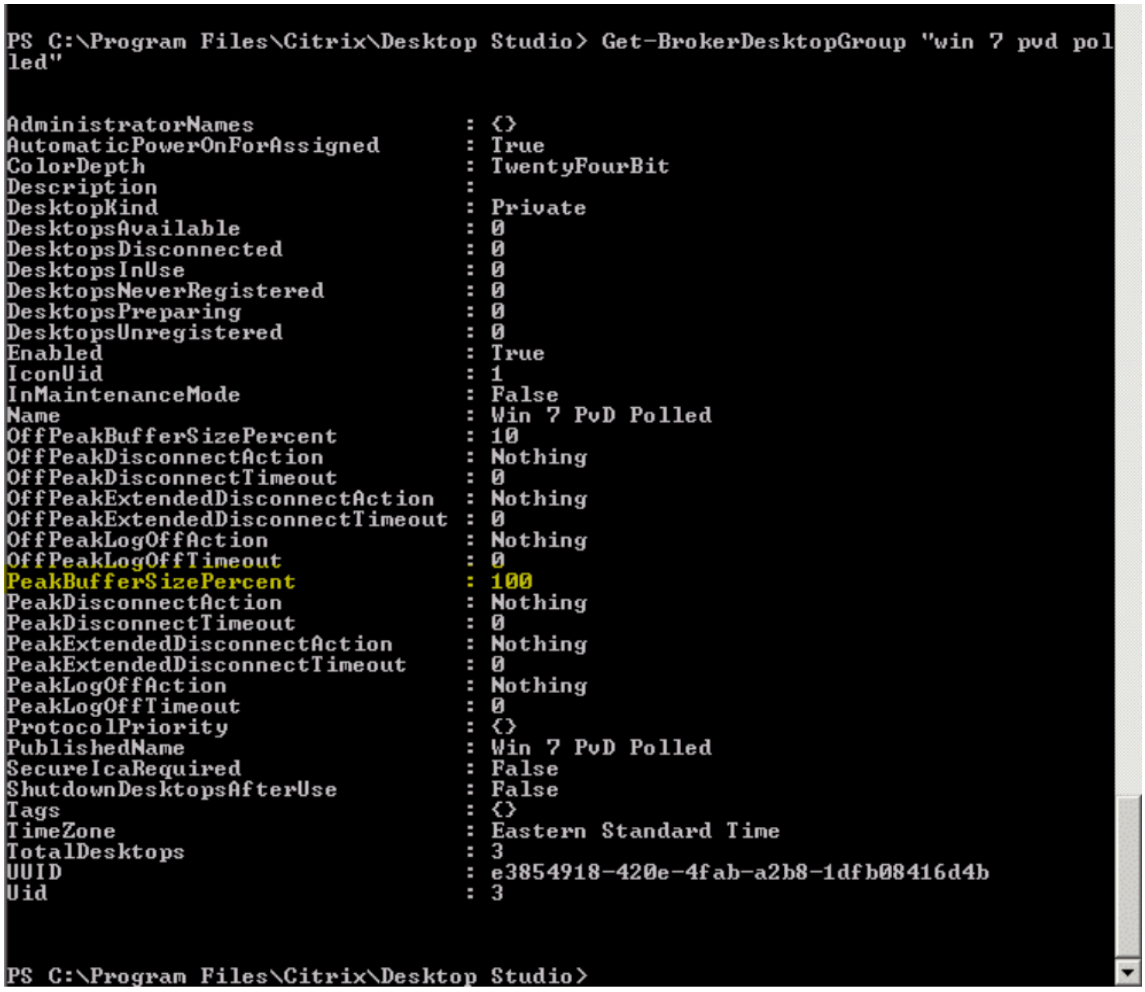
Ändern des Prozentsatzes der VDAs im aktivierten Zustand für Kataloge

1. Passen Sie die Spitzenzeiten für die Bereitstellungsgruppe über den Bereich **Energieverwaltung** für die **Bereitstellungsgruppe** an.
2. Notieren Sie sich den Namen der Desktopgruppe.
3. Starten Sie PowerShell mit Administratorrechten und führen Sie die folgenden Befehle aus. Ersetzen Sie "Desktop Group Name"durch den Namen der Desktopgruppe mit dem geänderten Prozentsatz ausgeführter VDAs.

   ```
   asnp Citrix*

   # Set-BrokerDesktopGroup "Desktop Group Name"-PeakBufferSizePercent
    100
   ```

   Der Wert 100 bedeutet, dass 100 Prozent der VDAs betriebsbereit sind.
4. Überprüfen Sie die Lösung mit folgendem Befehl:

   ```
   #Get-BrokerDesktopGroup "Desktop Group Name"
   ```

Es kann bis zu einer Stunde dauern, bis Änderungen wirksam werden.

Zum Herunterfahren der VDAs nach dem Abmelden der Benutzer geben Sie Folgendes ein:

```
# Set-BrokerDesktopGroup "Desktop Group Name"-ShutDownDesktopsAfterUse
 $True
```

Um VDAs zu Spitzenzeiten neu zu starten, damit sie für die Benutzer nach deren Abmeldung bereit sind, geben Sie Folgendes ein:

```
# Set-BrokerDesktopGroup "Desktop Group Name"-AutomaticPowerOnForAssignedDurin
 $True
```

Sitzungen

- Abmelden oder Trennen einer Sitzung oder Senden einer Nachricht an Benutzer
- Konfigurieren des Vorabstarts und des Fortbestehens von Sitzungen

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 Maschinen mit Einzelsitzungs-OS 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 Maschinen mit Multisitzungs-OS 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.

Standardmäßig werden Sitzungsvorabstart und Sitzungsfortbestehen nicht verwendet. Eine Sitzung wird gestartet, wenn ein Benutzer eine Anwendung startet und sie bleibt aktiv, bis die letzte geöffnete Anwendung in der Sitzung geschlossen wird.

Überlegungen:

- Die Bereitstellungsgruppe muss Anwendungen unterstützen und auf den Maschinen muss ein VDA für Multisitzungs-OS in mindestens Version 7.6 ausgeführt werden.
- Diese Features werden nur bei Verwendung der Citrix Workspace-App für Windows unterstützt, sie erfordern außerdem zusätzliche Citrix Workspace-App-Konfigurationsschritte. Anweisungen hierzu finden Sie in der Produktdokumentation zu Ihrer Citrix Workspace-App für Windows-Version. Suchen Sie dort nach "Sitzungsvorabstart".
- Die Citrix Workspace-App für HTML5 wird nicht unterstützt.
- Wird eine Maschine in den Modus "Anhalten"oder in den Ruhezustand versetzt, funktioniert der Sitzungsvorabstart unabhängig von den Vorabstarteinstellungen nicht. Die Benutzer können ihre Maschinen/Sitzungen sperren. Wenn sie sich jedoch von der Citrix Workspace-App 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. Bei Verwendung einer Benutzer-/Gerätelizenz gilt die Lizenz 90 Tage. 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 der Citrix Workspace-App 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. 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 nur über das SDK (`New`/`Set-BrokerSessionPreLaunch` Cmdlet) und nicht über die Verwaltungskonsole aktivieren. Wenn Sie das Timeout deaktivieren, wird es für die betreffende Bereitstellungsgruppe in der Konsole 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.

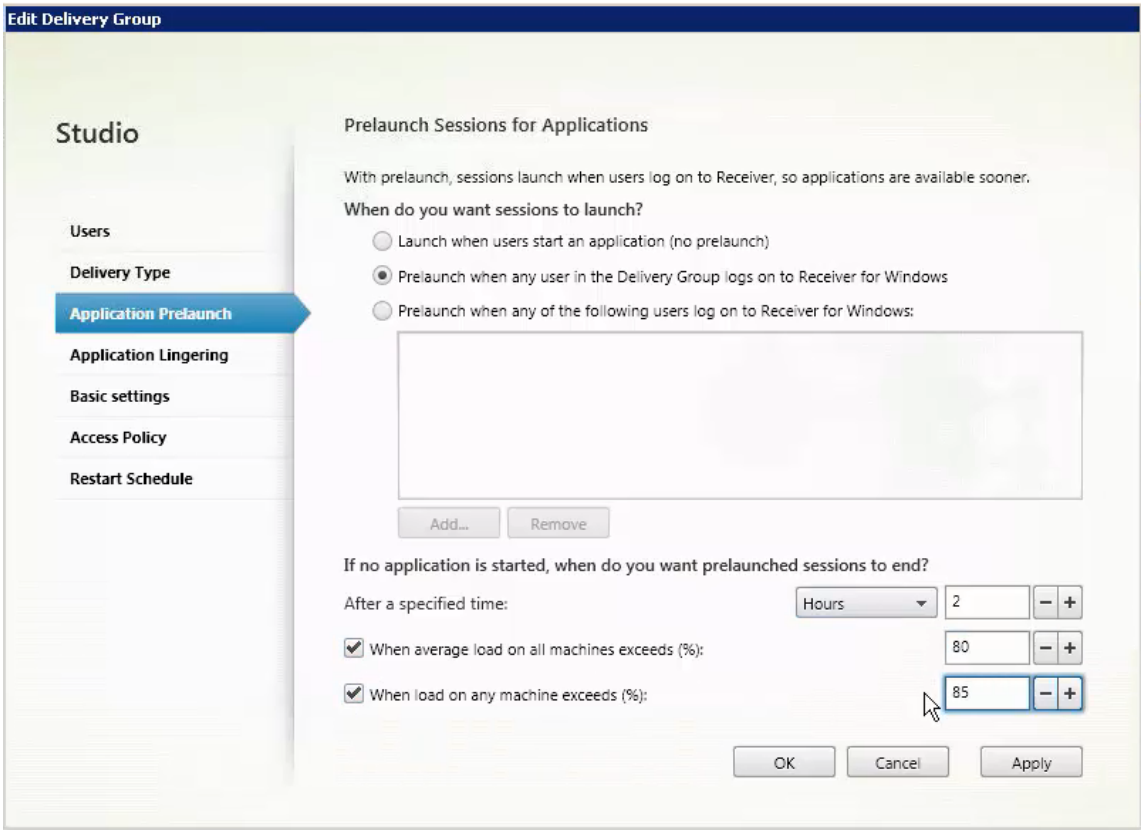
Server mit VDAs, die nicht bei einem Controller registriert sind, und Server im Wartungsmodus gelten als voll ausgelastet. Bei einem ungeplanten Ausfall werden vorab gestartete und fortbestehende Sitzungen automatisch beendet, um Kapazität freizugeben.

Aktivieren des Vorabstarts von Sitzungen

1. Wählen Sie im Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Bereitstellungsgruppe und klicken Sie im Aktionsbereich auf **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. Vorabstartsitzungen sind deaktiviert.
   - Wenn ein Benutzer der Bereitstellungsgruppe sich bei der Citrix Workspace-App für Windows anmeldet.

- Wenn ein beliebiger Benutzer einer Liste mit Benutzern und Bereitstellungsgruppen sich bei der Citrix Workspace-App für Windows anmeldet. Bei Auswahl dieser Option müssen Sie auch die Benutzer oder Benutzergruppen festlegen.



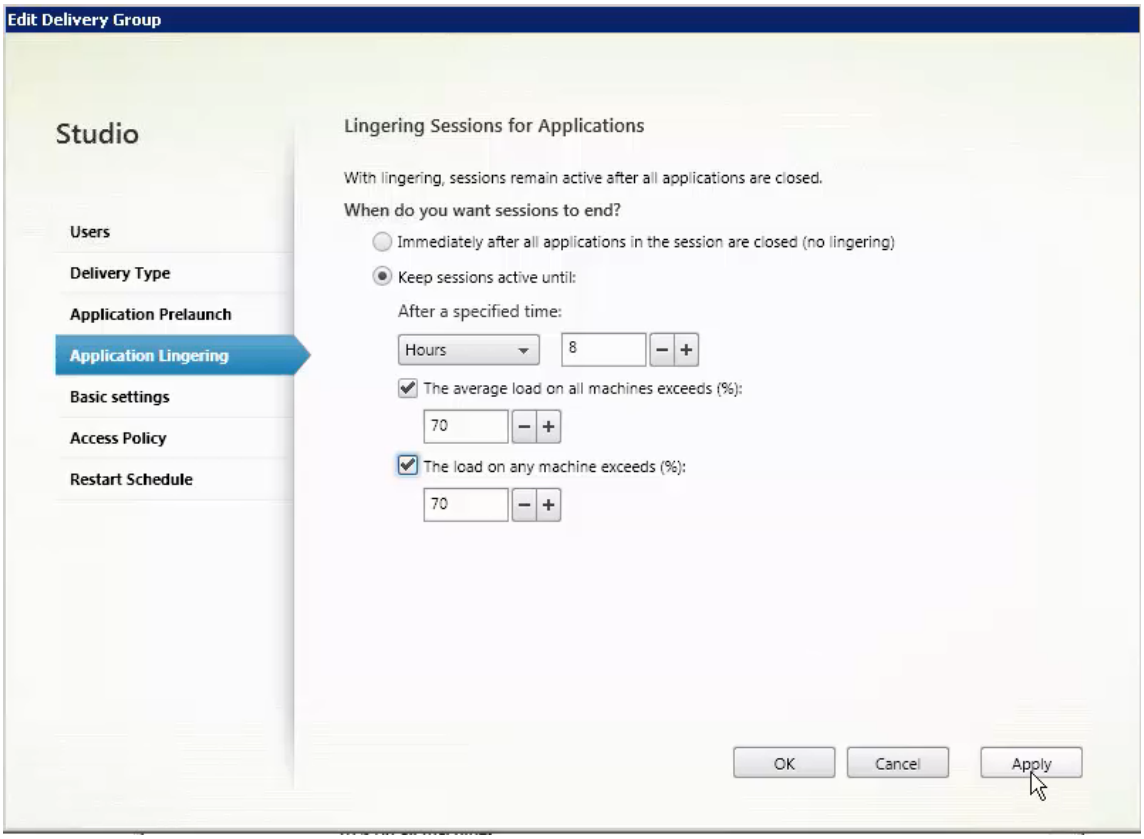
4. Eine vorab gestartete Sitzung wird durch eine normale Sitzung ersetzt, wenn der Benutzer eine Anwendung startet. Wenn der Benutzer keine Anwendung startet (d. h. die vorab gestartete Sitzung wird nicht verwendet), wird durch die folgenden Einstellungen bestimmt, wie lange die Sitzung aktiv bleibt.

   - 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 Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Bereitstellungsgruppe und klicken Sie im Aktionsbereich auf **Bereitstellungsgruppe bearbeiten**.
3. Aktivieren Sie auf der Seite **Anwendungsfortbestehen** das Sitzungsfortbestehen durch Aktivieren von **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 kommen beim Start gebrokerter Sitzungen nicht in die Auswahl. Dies hat eine mangelnde Auslastung verfügbarer Ressourcen zur Folge. Es gibt eine Reihe von Gründen, warum ein VDA nicht registriert sein könnte. Viele können vom Administrator behandelt werden. Die Detailanzeige bietet Informationen zur Problembehandlung im Assistenten zum Erstellen von Maschinenkatalogen und nach dem Hinzufügen eines Katalogs zu einer Bereitstellungsgruppe.

  Nach Erstellung einer Bereitstellungsgruppe wird im zugehörigen Detailbereich die Anzahl der Maschinen angezeigt, die registriert sein müssten, es jedoch nicht sind. Es kann beispielsweise 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.

  Informationen zur Fehlerbehebung bei der VDA-Registrierung finden Sie unter CTX136668.

- 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

September 21, 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.

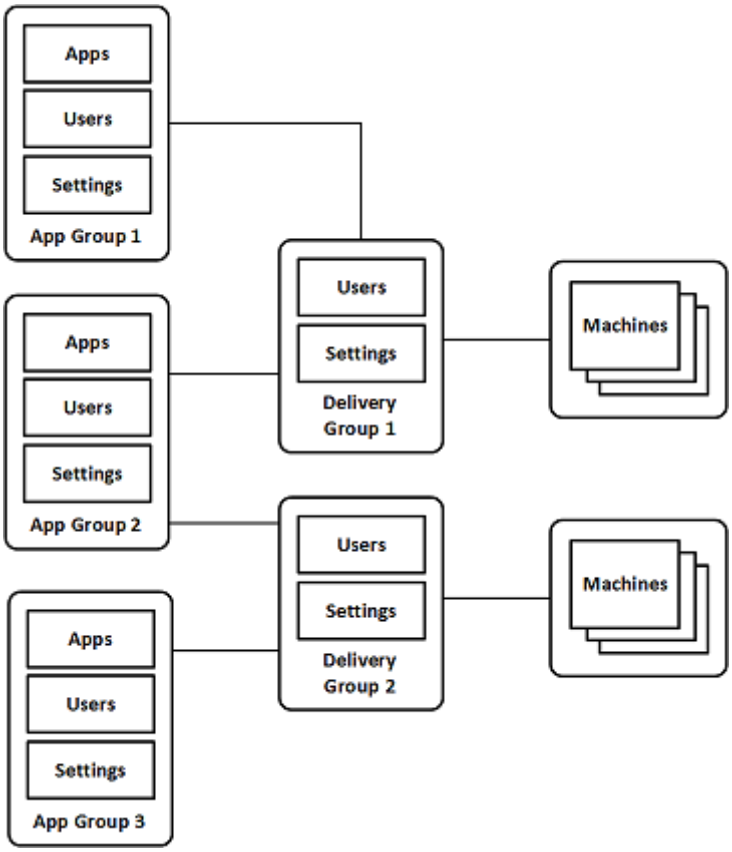
Die Verwendung von Anwendungsgruppen kann für die Anwendungsverwaltung und Ressourcensteuerung gegenüber der Verwendung weiterer Bereitstellungsgruppen folgende Vorteile bieten:

- 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 Citrix Virtual Apps and Desktops-Bereitstellung mit Anwendungsgruppen:



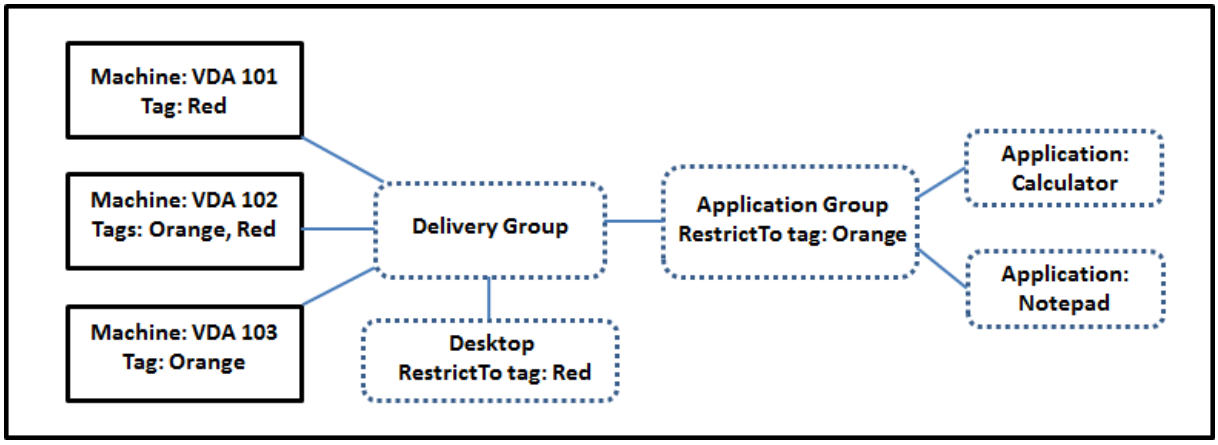
In dieser Konfiguration werden Anwendungen Anwendungsgruppen und nicht Bereitstellungsgruppen hinzugefügt. Über die Bereitstellungsgruppen wird festgelegt, welche Maschinen verwendet werden. (Obwohl dies nicht ausgezeichnet ist, sind die Maschinen in Maschinenkatalogen.)

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 Folgendes:

1. Upgrade von VDAs auf den Maschinen in der Bereitstellungsgruppe
2. Upgrade der Maschinenkataloge, die die Maschinen enthalten

3. 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. Weitere Informationen finden Sie unter 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 der Gruppe 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 der Gruppe 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.

Schritt 1. Bereitstellungsgruppen

Auf der Seite **Bereitstellungsgruppen** werden alle Bereitstellungsgruppen 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) Maschinen mit Windows-Einzelsitzungs-OS und Windows-Multisitzungs-OS.
- 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 folgende Bedingungen erfüllt sind:

- Die Bereitstellungsgruppe enthält freigegebene Maschinen und wurde mit einer XenDesktop-Version vor 7.9 erstellt.
- Sie haben die Berechtigung zum Bearbeiten der Bereitstellungsgruppe.

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.

Schritt 2. 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.

Informationen darüber, wo Benutzerlisten festgelegt werden, finden Sie unter Festlegung von Benutzerlisten.

Schritt 3. 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. Andernfalls 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)**. Andernfalls wird den Benutzern der Name in der Citrix Workspace-App 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 steht nicht zur Verfügung, wenn Sie eines der folgenden Elemente ausgewählt haben:

  - Anwendungsgruppen, denen keine Bereitstellungsgruppen zugeordnet sind.
  - Anwendungsgruppen mit zugeordneten Bereitstellungsgruppen, die keine Maschinen enthalten.
  - Eine Bereitstellungsgruppe, 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).

Schritt 4. Geltungsbereiche

Diese Seite wird nur angezeigt, wenn Sie zuvor einen benutzerdefinierten Geltungsbereich erstellt haben. Standardmäßig ist der Bereich **Alles** ausgewählt. Weitere Informationen finden Sie unter Delegierte Administration.

Schritt 5. 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

September 21, 2021

> Hinweis:
> Bei Verwendung von Anwendungsgruppen mit dem Citrix Virtual Apps and Desktops-Dienst ist das Feature zur Tagbeschränkung derzeit nicht verfügbar.

Einführung

Nachfolgend 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 bei der Erstellung automatisch aktiviert. Dies können Sie bei der Erstellung der Gruppe 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 der Gruppe nicht ändern. Weitere Informationen 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 PowerShell-SDK können Sie Anwendungsgruppen konfigurieren, bei denen die Sitzungsfreigabe zwischen den enthaltenen Anwendungen deaktiviert ist. In manchen Situationen kann dies vorteilhaft sein. Ein Beispiel wäre, wenn Benutzer Nicht-Seamless-Anwendungen in voller Fenstergröße auf separaten Monitoren öffnen sollen.

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. Wenn die Situation unter den gleichen Bedingungen erneut auftritt, wird die gleiche Sitzung gewählt. Ansonsten ist die Wahl nicht vorhersagbar.

Mit dem 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
```

Überlegungen

- 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. Ist die Option beispielsweise für eine Gruppe auf "True"und für eine andere auf "False"festgelegt, führt dies zu unvorhersehbarem Verhalten.

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 folgende Bedingungen erfüllt sind:

- Die Bereitstellungsgruppe enthält freigegebene Maschinen und wurde mit einer Version vor 7.9 erstellt.
- Sie haben die Berechtigung zum Bearbeiten der Bereitstellungsgruppe.

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

Das Hinzufügen, Bearbeiten und Entfernen von Tagbeschränkungen kann unerwartete Auswirkungen darauf haben, welche Maschinen für den Anwendungsstart in Betracht gezogen werden. Lesen Sie die Informationen und Hinweise unter 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.

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 unter 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 sie nicht aus ihrer ursprünglichen Quelle gelöscht. Wenn Sie sie jedoch 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

June 27, 2024

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:**
>
> Weitere Informationen zu den unterstützten Betriebssystemversionen finden Sie unter Systemanforderungen für den Einzelsitzungs-OS-VDA und 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.

> **Wichtig:**
>
> Physische Windows 11-Systeme (und einige, auf denen Windows 10 ausgeführt wird) verfügen über virtualisierungsbasierte Sicherheitsfeatures, die dazu führen, dass die VDA-Software sie fälschlicherweise als virtuelle Maschinen erkennt. Um dieses Problem zu beheben, haben Sie die folgenden Optionen:
>
> - Verwenden Sie die Option "/physicalmachine"zusammen mit der Option "/remotepc"in der VDA-Befehlszeileninstallation.
> - Fügen Sie nach der Installation des VDA den folgenden Registrierungswert hinzu, falls die oben genannte Option nicht verwendet wurde.
>   `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`
>
>   - Name: ForceEnableRemotePC
>   - Typ: DWORD
>   - Daten: 1

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 die Sitzung eines Remotebenutzers 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
- Daten:
  - 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

Abblenden des Monitors funktioniert nicht

Wenn der lokale Monitor des Windows-PCs während einer aktiven HDX-Sitzung nicht leer ist (der lokale Monitor zeigt an, was in der Sitzung passiert), ist dies wahrscheinlich auf Probleme mit dem Treiber des GPU-Herstellers zurückzuführen. Um das Problem zu beheben, geben Sie dem Citrix Indirect Display-Treiber (IDD) höhere Priorität als der Grafikkartentreiber des Herstellers, indem Sie den folgenden Registrierungswert festlegen:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\AdapterMerits`

- Name: CitrixIDD
- Typ: DWORD
- Wert: 3

Weitere Informationen zu Anzeigeadapterprioritäten und Monitorerstellung finden Sie im Knowledge Center-Artikel CTX237608.

Die Sitzung wird getrennt, wenn Sie Strg+Alt+Entf auf der Maschine drücken, auf der die Sitzungsverwaltungsbenachrichtigung aktiviert ist

Die vom Registrierungswert **SasNotification** gesteuerte Sitzungsverwaltungsbenachrichtigung funktioniert nur, wenn der Remote-PC-Zugriffsmodus auf dem VDA aktiviert ist. Wenn auf dem physischen PC die Hyper-V-Rolle oder virtualisierungsbasierte Sicherheitsfeatures aktiviert sind, wird der PC als virtuelle Maschine gemeldet. Wenn der VDA erkennt, dass er auf einer virtuellen Maschine ausgeführt wird, deaktiviert er automatisch den Remote-PC-Zugriff-Modus. Um den Remote-PC-Zugriff-Modus zu aktivieren, fügen Sie folgenden Registrierungswert hinzu:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Name: ForceEnableRemotePC
- Typ: DWORD
- Wert: 1

Starten Sie den PC neu, damit die Einstellung wirksam wird.

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.

Aktive Remotesitzung zeichnet lokale Touchscreeneingabe auf

Wenn der VDA den Remote-PC-Zugriff-Modus aktiviert, ignoriert die Maschine die lokale Touchscreeneingabe während einer aktiven Sitzung. Wenn auf dem physischen PC die Hyper-V-Rolle

oder virtualisierungsbasierte Sicherheitsfeatures aktiviert sind, wird der PC als virtuelle Maschine gemeldet. Wenn der VDA erkennt, dass er auf einer virtuellen Maschine ausgeführt wird, deaktiviert er automatisch den Remote-PC-Zugriff-Modus. Um den Remote-PC-Zugriff-Modus zu aktivieren, fügen Sie die folgende Registrierungseinstellung hinzu:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Name: ForceEnableRemotePC
- Typ: DWORD
- Wert: 1

Starten Sie den PC neu, damit die Einstellung wirksam wird.

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

September 21, 2021

Verwenden von App-V in Citrix Virtual Apps and Desktops

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	Citrix Virtual Apps and Desktops-Delivery Controller	Citrix Virtual Apps and Desktops-VDA
5.0 und 5.0 SP1	XenDesktop 7 bis aktuelle Version, XenApp 7.5 bis aktuelle Version	7.0 bis aktuelle Version

App-V	Citrix Virtual Apps and Desktops-Delivery Controller	Citrix Virtual Apps and Desktops-VDA
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 die Citrix Workspace-App
- Über den App-V-Client und die Citrix Workspace-App
- 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. In dynamischen Konfigurationsdateien gespeicherte Anwendungsanpassungen werden ebenfalls beim Start der Anwendung angewendet.

Verwaltungsmethoden

Sie können mit dem App-V Sequencer erstellte und auf einem App-V-Server oder einer Netzwerkfreigabe gehostete App-V-Pakete und dynamische Konfigurationsdateien 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. Bei dieser Methode verarbeitet der Verwaltungsserver die dynamischen Konfigurationsdateien. Bei Verwendung der dualen Verwaltung wird die Registrierung des zum Anwendungsstart erforderlichen Veröffentlichungsservers über die Citrix App-V-Komponenten verwaltet. Dadurch wird sichergestellt, dass der Veröffentlichungsserver zum entsprechenden Zeitpunkt für den Benutzer synchronisiert ist. Der Veröffentlichungsserver verwaltet andere Aspekte des Paketlebenszyklus (z. B. Aktualisieren bei Anmeldung und Verbindungsgruppen) mithilfe der konfigurierten Einstellungen.

- **Netzwerkfreigabe:** Werden Pakete und XML-Bereitstellungskonfigurationsdateien 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 für die Verwendung von App-V-Paketen und -Anwendungen nur die Studiokonsole erforderlich ist. Sie navigieren zu der Netzwerkfreigabe und fügen von dort die App-V-Pakete der Anwendungsbibliothek [1] auf Siteebene hinzu. Bei dieser Methode verarbeiten die Citrix App-V-Komponenten die Bereitstellungskonfigurationsdateien beim Start der Anwendung. (Benutzerkonfigurationsdateien werden nicht unterstützt.) Bei Verwenden der Einzelverwaltung werden alle Aspekte des Paketlebenszyklus auf der Hostmaschine durch die Citrix App-V-Komponenten verwaltet. Pakete werden der

Maschine beim Start des Brokers hinzugefügt oder wenn eine Konfigurationsänderung erkannt wird (dies kann auch beim Sitzungsstart erfolgen). Pakete werden für einzelne Benutzer bei Bedarf veröffentlicht, sobald eine Startanforderung von der Citrix Workspace-App empfangen wurde.

Die Einzelverwaltung verwaltet auch den Lebenszyklus von Verbindungsgruppen, die zum Einhalten der in Studio definierten Isolationsgruppenkonfiguration erforderlich sind.

[1] *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.

Wenn in beiden Verwaltungsmethoden der VDA so konfiguriert ist, dass Benutzerdaten verworfen werden, muss die Veröffentlichung (oder Synchronisierung) beim nächsten Sitzungsstart erneut durchgeführt werden.

Sie können eine Verwaltungsmethode verwenden oder beide parallel. Das heißt, die einer Bereitstellungsgruppe hinzugefügten Anwendungen dürfen aus App-V-Paketen stammen, die auf App-V-Servern oder in einer Netzwerkfreigabe gespeichert sind.

> **Hinweis:**
>
> Wenn Sie beide Verwaltungsmethoden gleichzeitig verwenden und das App-V-Paket an beiden Speicherorten eine dynamische Konfigurationsdatei hat, wird die Datei auf dem App-V-Server (duale Verwaltung) verwendet.

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 und Verknüpfungen im Paket angezeigt.

Dynamische Konfigurationsdateien

Übersicht App-V-Pakete können mithilfe dynamischer Konfigurationsdateien angepasst werden, durch die bei Anwendung auf ein Paket dessen Eigenschaften geändert werden. Sie können damit beispielsweise zusätzliche Anwendungsverknüpfungen und -verhalten definieren. Citrix App-V unterstützt beide Arten dynamischer Konfigurationsdateien. Dateieinstellungen werden beim Start der Anwendung angewendet:

- Bereitstellungskonfigurationsdateien bieten eine maschinenweite Konfiguration für alle Benutzer. Der Name dieser Dateien muss <*Name der Paketdatei*>_DeploymentConfig.xml lauten und sich im selben Ordner wie das zugehörige App-V-Paket befinden. Sie werden von der Einzel- und der dualen Verwaltung unterstützt.

- Benutzerkonfigurationsdateien bieten eine benutzerspezifische Konfiguration, die benutzerspezifische Anpassungen für ein Paket ermöglicht. Die Einzelverwaltung unterstützt Benutzerkonfigurationsdateien mit dem Benennungsformat *packageFileName*>_[UserSID | Username | GroupSID |GroupName_]UserConfig.xml, die im selben Ordner sind, wie das zugehörige App-V-Paket.

Gibt es mehrere Benutzerkonfigurationsdateien für ein Paket, werden sie mit der folgenden Priorität angewendet:

1. Benutzer-SID
2. Benutzername
3. AD-Gruppen-SID (zuerst gefundene erhält Vorrang)
4. AD-Gruppenname (zuerst gefundene erhält Vorrang)
5. Standard

Zum Beispiel

```
MyAppVPackage_S-1-5-21-000000001-0000000001-000000001-001_UserConfig.
    xml
MyAppVPackage_joeblogs_UserConfig.xml
MyAppVPackage_S-1-5-32-547_UserConfig.xml
MyAppVPackage_Power Users_UserConfig.xml
MyAppVPackage_UserConfig.xml
```

> **Hinweis:**
>
> Der benutzerspezifische Teil des Dateinamens darf optional auch am Ende stehen (z. B. MyAppV-Package_UserConfig_**joeblogs**.xml).

Speicherort dynamischer Konfigurationsdateien Bei der Einzelverwaltung verarbeiten die Citrix App-V-Komponenten nur dynamische Konfigurationsdateien, die sich im selben Ordner wie das App-V-Paket befinden. Wenn Anwendungen im Paket gestartet werden, werden alle Änderungen an den zugehörigen dynamischen Konfigurationsdateien erneut angewendet. Befinden sich dynamische Konfigurationsdateien an einem anderen Speicherort als die Pakete, verwenden Sie eine Zuordnungsdatei zur Zuordnung von Paketen und Bereitstellungskonfigurationsdateien.

Erstellen einer Zuordnungsdatei

1. Öffnen Sie eine neue Textdatei.
2. Fügen Sie für jede dynamische Konfigurationsdatei eine Zeile hinzu, die den Pfad zum Paket angibt. Format: <PaketGUID> : Pfad.

   Beispiel:

   F1f4fd78ef044176aad9082073a0c780 : c:\widows\file\packagedeploy.xml

3. Speichern Sie die Datei unter dem Namen "ctxAppVDynamicConfigurations.cfg"im selben Ordner wie das Paket. Bei jedem Start einer Anwendung in dem App-V-Paket wird die gesamte Verzeichnishierarchie der UNC-Freigabe des Pakets rekursiv nach oben nach dieser Datei durchsucht.

> **Hinweis**
>
> Sie können keine Änderungen an der dynamischen Bereitstellungskonfiguration anwenden, wenn eine Anwendung im Paket in einer Benutzersitzung geöffnet ist. Sie können Änderungen an Dateien zur dynamischen Benutzerkonfiguration anwenden, wenn *andere als der aktuelle Benutzer* eine Anwendung aus dem Paket geöffnet haben.

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.

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.

Einrichtung

Die folgende Tabelle enthält die Reihenfolge der Setupaufgaben zur Verwendung von App-V in Citrix Virtual Apps and Desktops in der Einzel- und der dualen Verwaltung.

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/.

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 und die zugehörigen dynamischen Konfigurationsdateien 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 bei der Installation eines VDAs standardmäßig ausgeschlossen.

Sie können dieses Standardverhalten während der Installation steuern. Aktivieren 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 **/includeadditional "Citrix Personalisierung für App-V - VDA"**.

Wenn Sie die Citrix App-V-Komponenten bei der VDA-Installation nicht einschließen und später App-V-Anwendungen verwenden möchten, klicken Sie in der Liste "Programme und Features"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 Anwendungen bzw. Anwendungsverknüpfungen, 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 die Eigenschaften einer App-V-Anwendung mithilfe dynamischer Konfigurationsdateien anpassen, setzen die Eigenschaften alle Änderungen außer Kraft, die Sie beim Hinzufügen zu einer Bereitstellungsgruppe vorgenommen haben.
- 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 mehr als 100 App-V-Anwendungen in einer einzelnen Bereitstellungsgruppe veröffentlichen, werden Anwendungen möglicherweise nicht gestartet. Erhöhen Sie in diesem Fall in der Konfiguration des Delivery Controllers und/oder Broker-Agent auf dem VDA die maximal zu empfangene Nachrichtengröße über die MaxReceivedMessageSize-Eigenschaft für das entsprechende Bindungselement.

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).
- Ist der Studio-Administrator gleichzeitig App-V-Serveradministrator? Der Studio-Administrator muss auf dem App-V-Verwaltungsserver zu der *Administratorengruppe* gehören, um mit dem Server 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 Benutzer-

namen und Kennwörter"einen Eintrag mit den Anmeldeinformationen des Benutzers ein, der Administratorberechtigungen auf dem App-V-Server hat. Erläuterungen finden Sie unter http://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 folgende Fehlermeldung angezeigt: *"The config setting TrustedHosts cannot be changed because use is controlled by policies. 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 dem Server 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).
- Haben die Pakete die richtigen Sicherheitsberechtigungen, sodass der Studio-Administrator Zugriff hat?

App-V-Anwendungen werden nur in einer Browserversion gestartet.

- Wenn Sie mehrere sequenzierte Versionen derselben Browser-App veröffentlichen, kann nur jeweils eine Version der App pro Benutzer auf dem VDA gestartet werden. Dies ist auch der Fall, wenn keine Citrix Komponenten beteiligt sind und der Benutzer die sequenzierten Apps über Desktop-Verknüpfungen startet, die auf unterschiedliche Pfade verweisen.

  Die von einem Benutzer zuerst gestartete Browserversion bestimmt, welche Browserversion später ausgeführt wird. Wenn Firefox einen zweiten Firefox-Start erkennt, erstellt es keinen neuen Prozess, sondern eine Instanz des bereits laufenden Prozesses. Bei anderen Browsern kann dies auch so sein.

Sie können die Anwendung in der gewünschten Firefox-Version starten, indem Sie dem Startbefehl der Verknüpfung den Befehlszeilenparameter **-no-remote** hinzufügen. Bei anderen Browsern gibt es die gleiche oder ähnliche Möglichkeiten.

> **Hinweis:**
>
> Diese Verknüpfungsenumeration ist nur unter XenApp 7.17 oder höher verfügbar. Außerdem müssen Sie das Paket in beiden App-Versionen ändern, um die Bidirektionalität zu erzielen.

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**.
- Bei Anzeige des Fehlers "RegistrationManager.AttemptRegistrationWithSingleDdc: Registrierung fehlgeschlagen": Erhöhen Sie in diesem Fall in der Konfiguration des Delivery Controllers und/oder Broker-Agent auf dem VDA die maximal zu empfangene Nachrichtengröße

über die MaxReceivedMessageSize-Eigenschaft für das entsprechende Bindungselement.

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

December 12, 2022

> **Hinweis:**
>
> AppDisks sind veraltet.

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 Citrix Virtual Apps and Desktops 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 betriebssystemübergreifend 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 aus-

führbare 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 kann Citrix Virtual Apps and Desktops 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 Citrix Virtual Apps and Desktops und der AppLibrary. Citrix Virtual Apps and Desktops interagiert dann mit Maschinenerstellungsdienste (MCS) oder Citrix Provisioning (zuvor "Provisioning Services") 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, die Delivery Controller und Studio der XenApp und XenDesktop-Version ab 7.8 enthalten, einschließlich der automatisch installierten Voraussetzungen (.NET 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* der Gruppe bezeichnet. Weitere Informationen zur Funktionsebene finden Sie unter Erstellen von Bereitstellungsgruppen.

Zum Bereitstellen von VMs, die zum Erstellen von AppDisks verwendet werden sollen, können Sie Folgendes verwenden:

- MCS wird mit dem Delivery Controller bereitgestellt.
- Auf der Downloadseite zusammen mit der verwendeten Citrix Virtual Apps and Desktops-Version verfügbare Citrix Provisioning-Version
- Unterstützte Hypervisors:
  - XenServer
  - VMware (mindestens Version 5.1)
  - Microsoft System Center Virtual Machine Manager

AppDisks können nicht mit anderen, für Citrix Virtual Apps and Desktops 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:

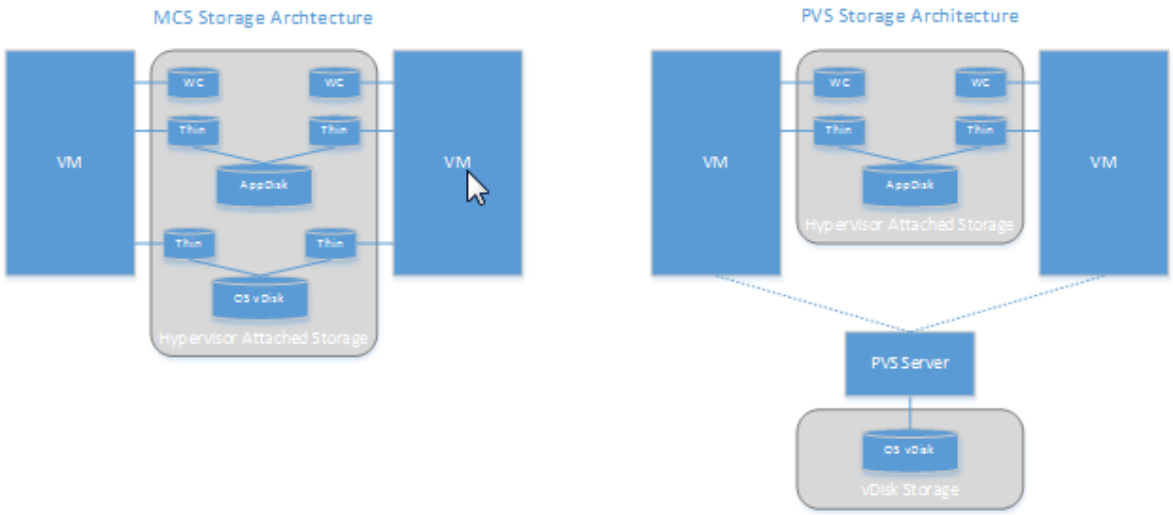
- Lesen Sie die AppDNA-Dokumentation und die FAQ zu AppDisk.
- Die AppDNA-Software muss auf einem anderen Server als solchen mit Controller installiert werden. Verwenden Sie die mit diesem Release von Citrix Virtual Apps and Desktops gelieferte AppDNA-Version. Weitere Anforderungen für AppDNA sind in 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 Citrix Virtual Apps and Desktops-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 (PDF-Download, Englisch)	-	-	-	-	-	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 Citrix Provisioning. “WC”steht für den Schreibcache 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.

In Citrix Provisioning-Umgebungen:

- Sie müssen eine Steigerung von Kapazität und IOPS berücksichtigen, da Anwendungen vom AppDisk-Speicher in den an den Hypervisor angeschlossenen Speicher umsiedeln.
- In Citrix Provisioning-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 Citrix Provisioning-Umgebung entsprechend wählen.
- AppDisks im am Hypervisor angeschlossenen Speicher erzeugen mehr IOPS, die Betriebssystem-vDisks hingegeben weniger.
- Schreibcache: Citrix Provisioning 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 Citrix Provisioning-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 Citrix Provisioning-Umgebungen sind die Anwendungen nicht auf der Betriebssystem-vDisk, sodass weniger Anforderungen beim Citrix Provisioning-Server eingehen. Aufgrund der geringeren Last auf den einzelnen Zielgeräten kann der Citrix Provisioning-Server an mehr Ziele streamen. Eine höhere Ziel-Server-Dichte kann allerdings die Leistung bei einem Boot Storm beeinträchtigen.

Überlegungen zur AppDisk-Erstellung

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.
- 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 Citrix Provisioning

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 einer AppDisk:

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**.

Wenn Sie Citrix Provisioning verwenden, folgen Sie den Anweisungen unter Überlegungen zu Citrix Provisioning.

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”
.

Anwendungen auf AppDisk installieren:

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 müssen Sie die Hypervisor-Verwaltungskonsole verwenden. Verwenden Sie nicht die Aufgabe **Anwendungen installieren** im Aktionsbereich von Studio.)

Versiegeln der AppDisk:

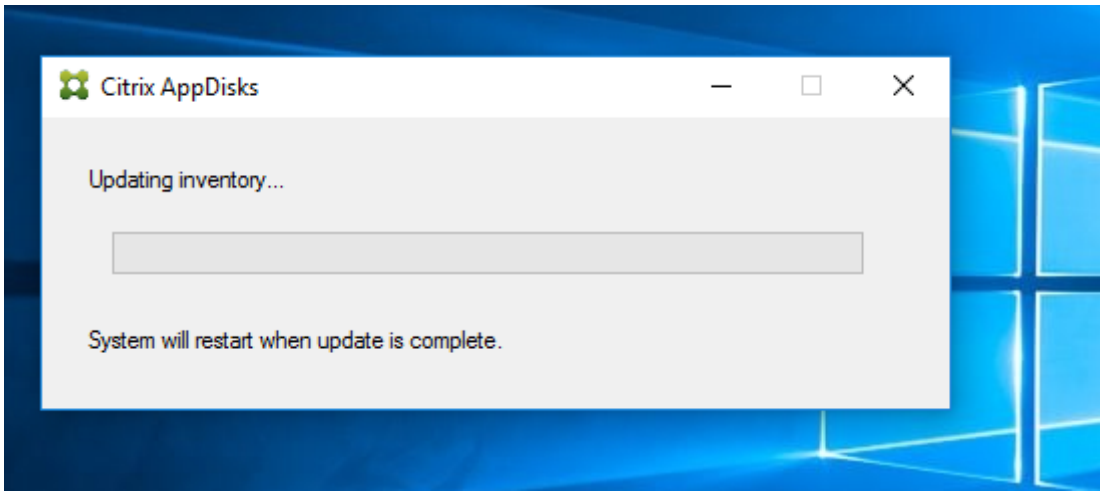
1. Wählen Sie im Studio-Navigationsbereich **AppDisks**.
2. Wählen Sie die zuvor erstellte AppDisk und dann im Studio-Aktionsbereich **AppDisk versiegeln**.

Nachdem Sie eine AppDisk erstellt, Anwendungen darauf installiert und die AppDisk versiegelt haben, weisen Sie sie einer Bereitstellungsgruppe zu.

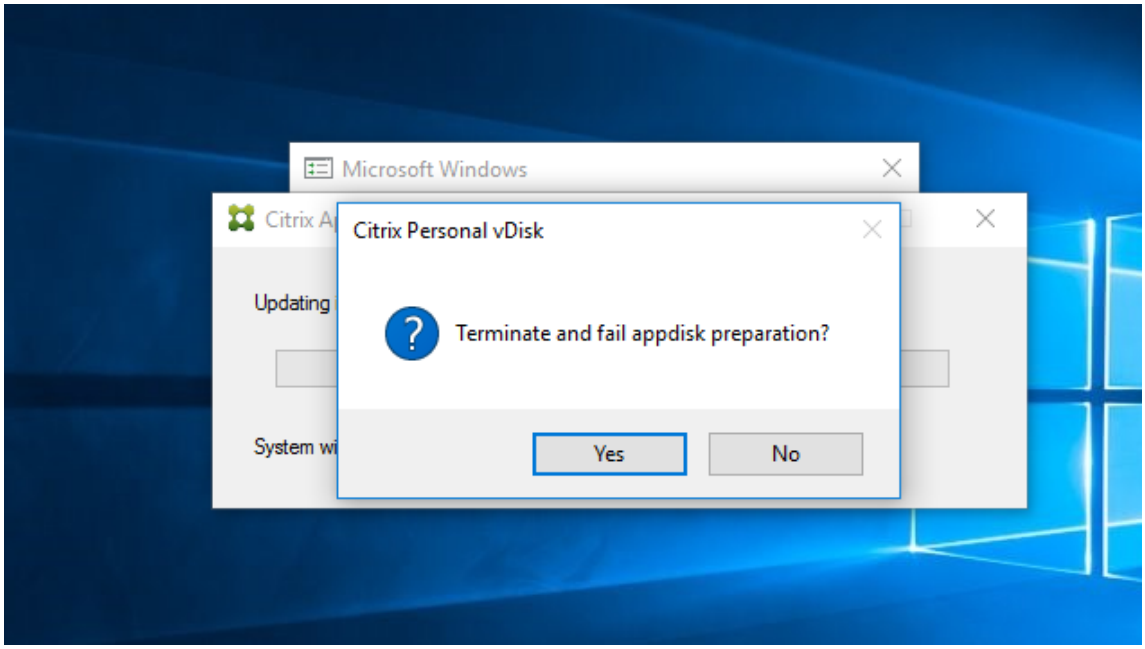
Abbrechen der AppDisk-Vorbereitung und -Versiegelung

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 unter 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.

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.

Wichtige Überlegungen zu Windows-Updates:

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.

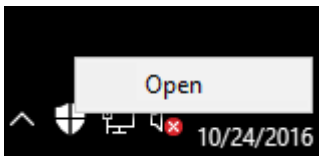
Dieser Abschnitt enthält Informationen zum Hinzufügen von Ausnahmen für folgende Antivirus-Anwendungen:

- Windows Defender (für Windows 10)
- OfficeScan (Version 11.0)
- Symantec (Version 12.1.16)
- McAfee (Version 4.8)

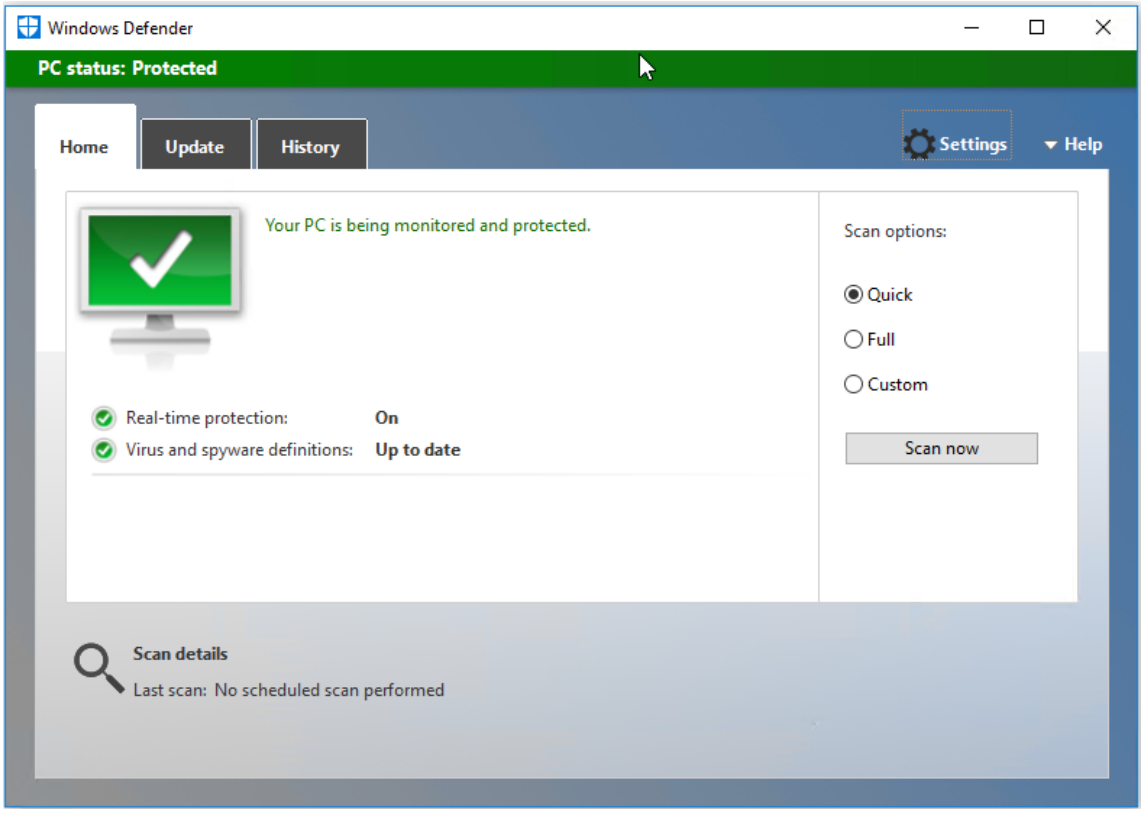
Windows Defender

Gehen Sie wie folgt vor, wenn auf der Basis-VM Windows Defender (Version 10) ausgeführt wird:

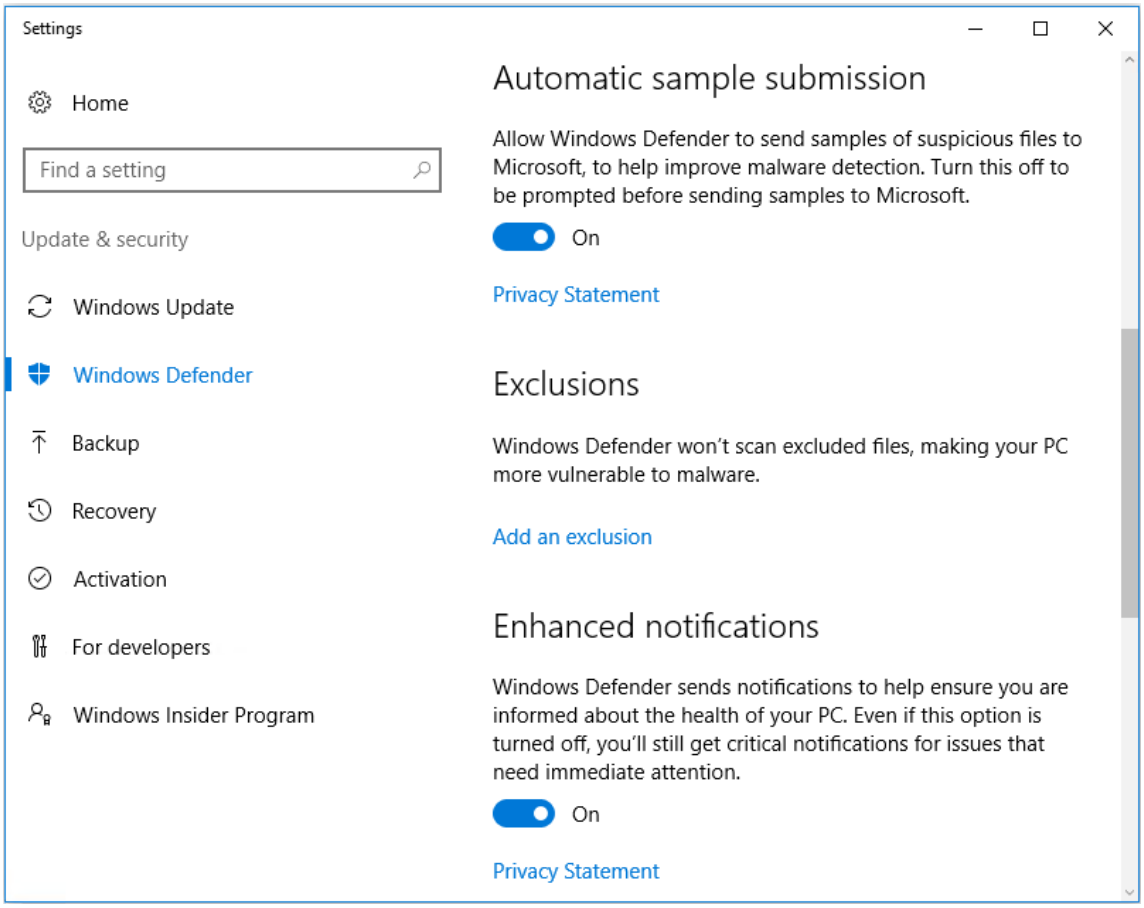
1. Melden Sie sich bei dem Computer als lokaler Administrator an.
2. Klicken Sie mit der rechten Maustaste auf das Windows Defender-Symbol, um die Schaltfläche **Öffnen** anzuzeigen:



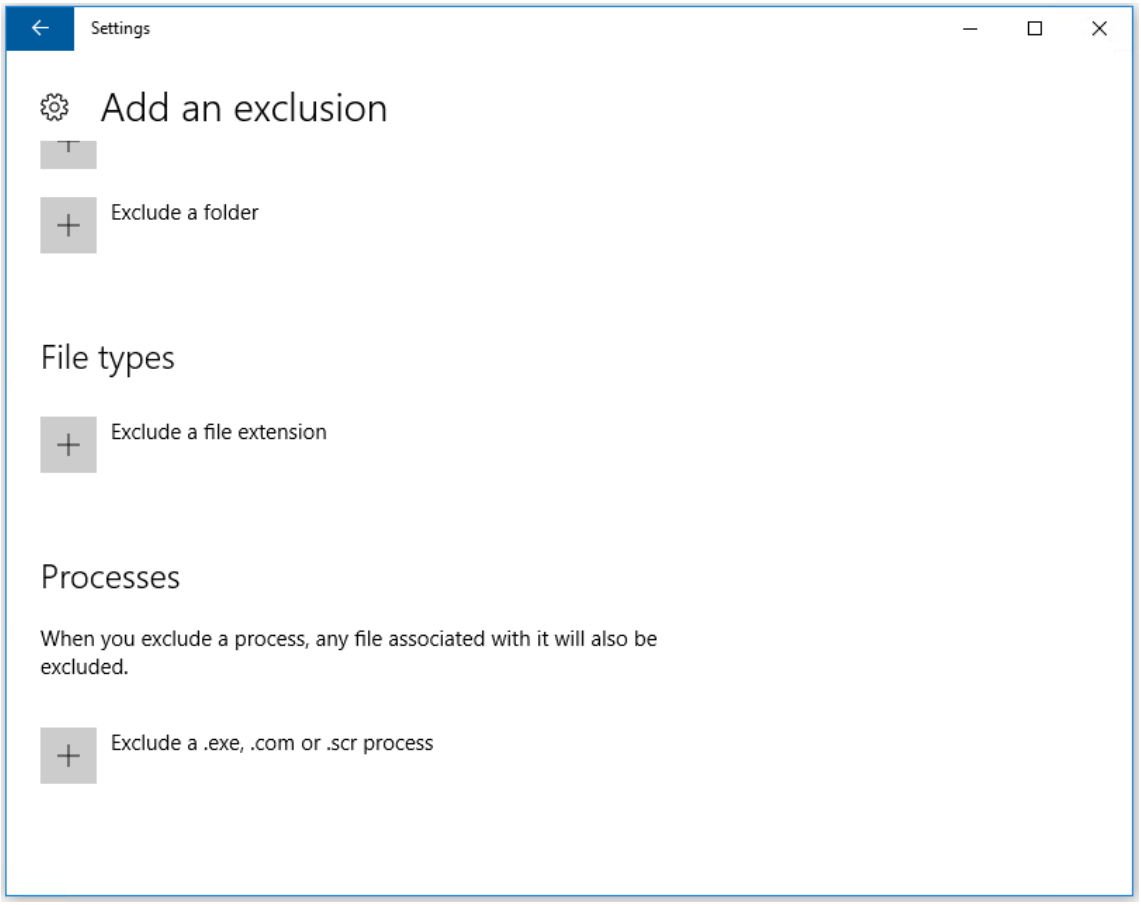
3. Wählen Sie in der Windows Defender-Konsole rechts oben **Einstellungen**:



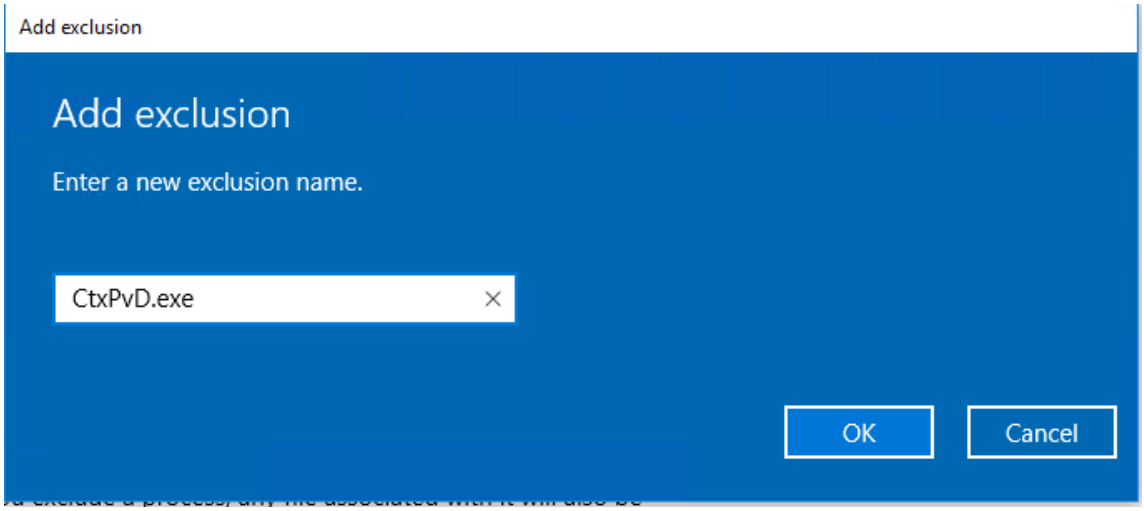
4. Klicken Sie im Bereich **Ausschlüsse** auf **Ausschluss hinzufügen**:



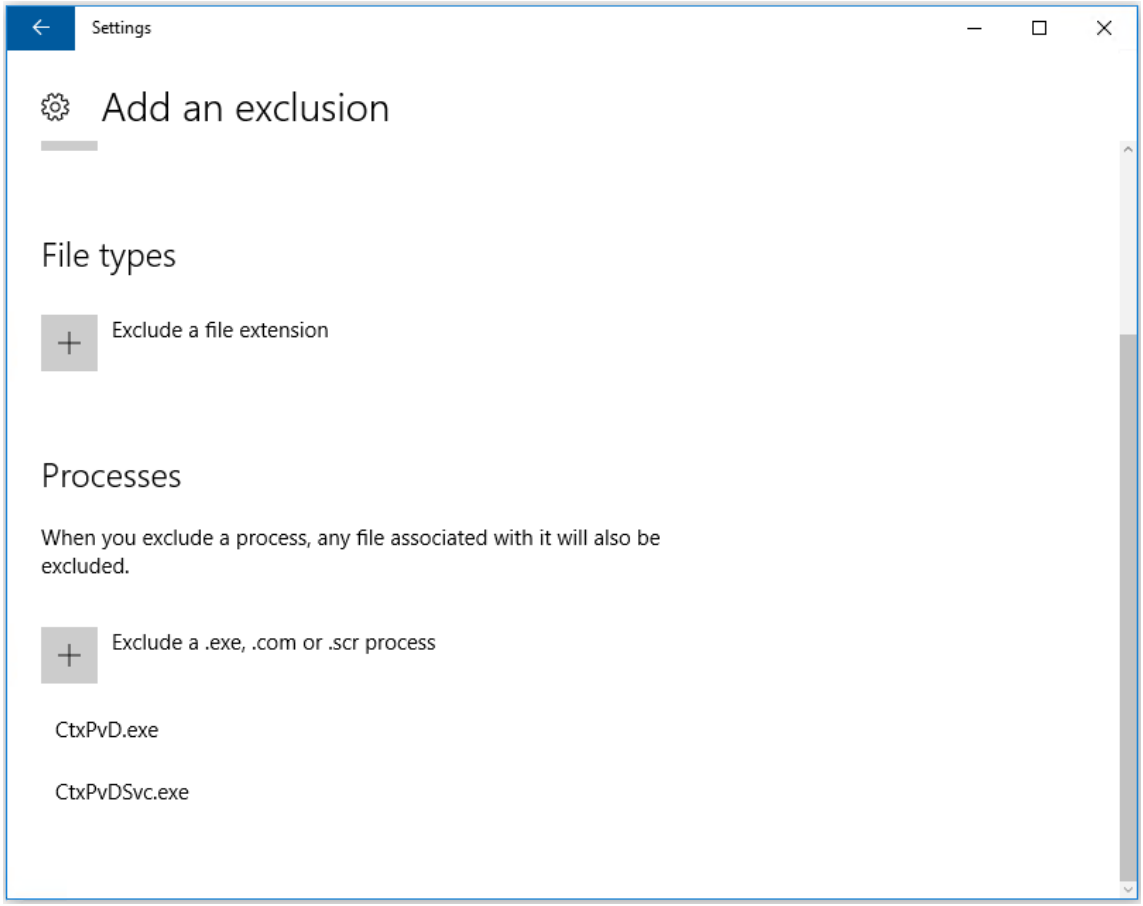
5. Wählen Sie im Bildschirm **Ausschluss hinzufügen** die Option **EXE-, COM- oder SCR-Prozess ausschließen**:



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**:



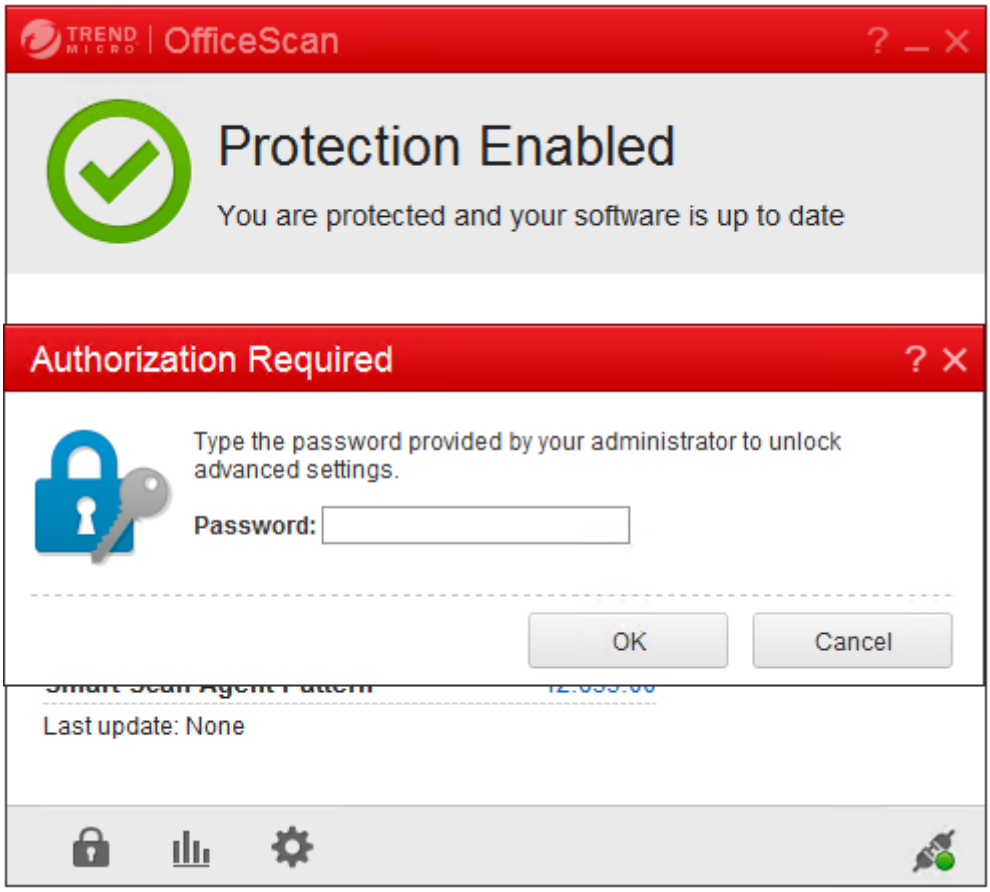
Nach dem Hinzufügen der Ausschlüsse erscheinen sie in der Liste der ausgeschlossenen Prozesse auf dem Bildschirm **Einstellungen**:



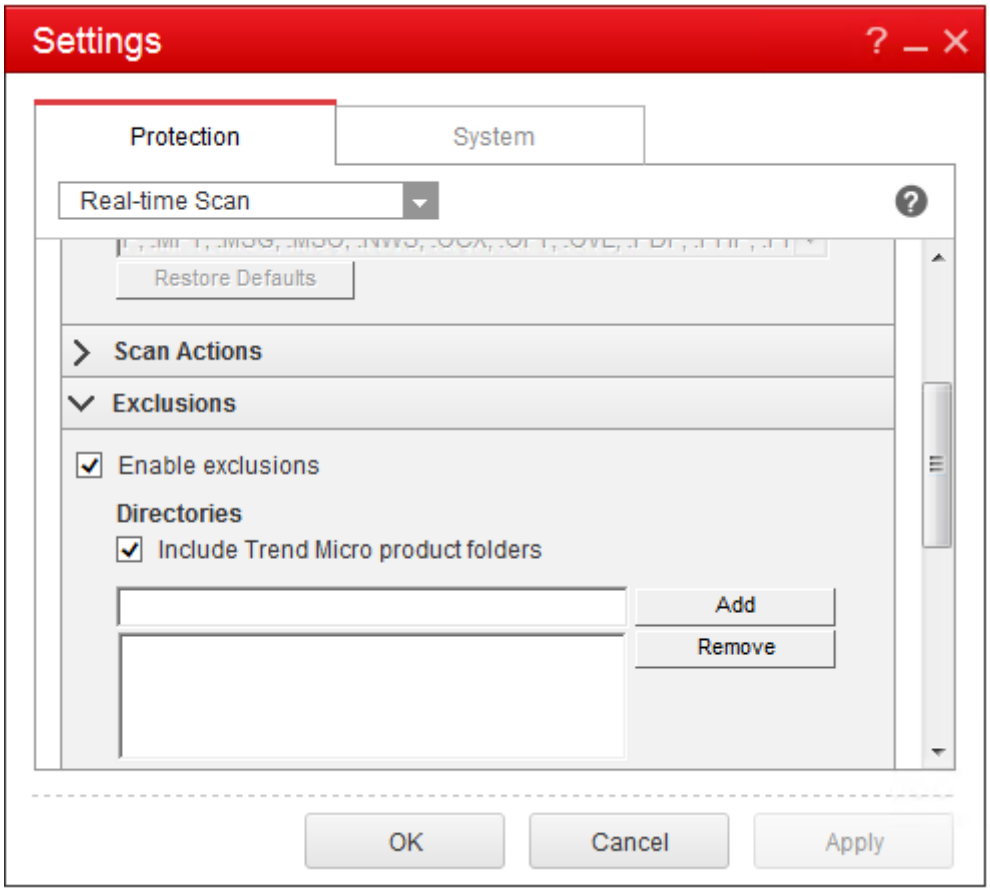
OfficeScan

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:



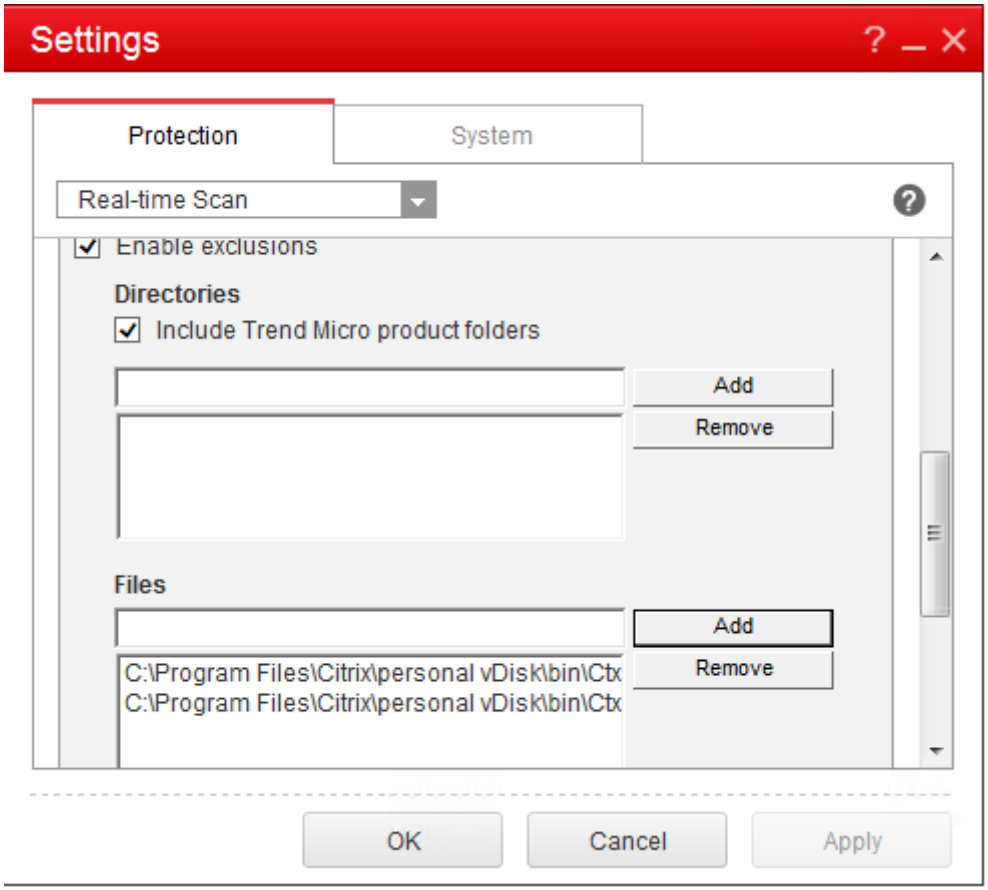
3. Klicken Sie auf das Symbol **Settings**, um die Konfigurationsoptionen anzuzeigen.
4. Wählen Sie im Bildschirm mit den Einstellungen die Registerkarte **Protection**.
5. Scrollen Sie auf der Registerkarte nach unten zum Abschnitt **Exclusions**.



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
   ```

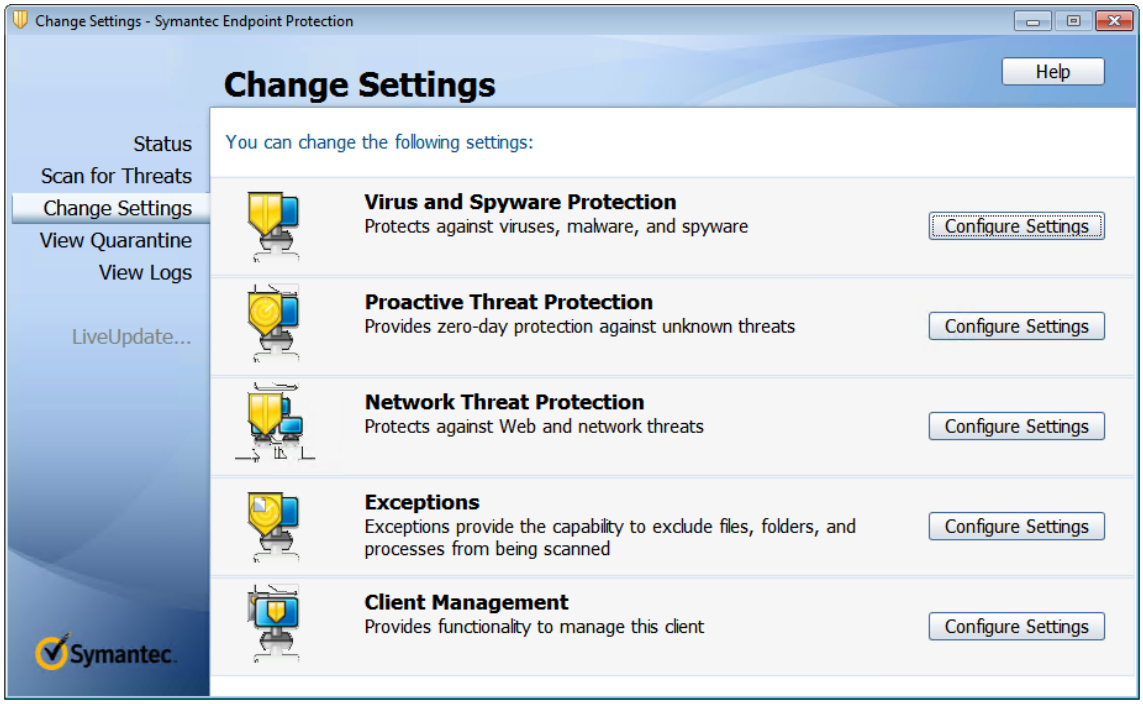



7. Klicken Sie auf **Apply** und dann auf **OK**, um die Ausschlüsse hinzuzufügen.

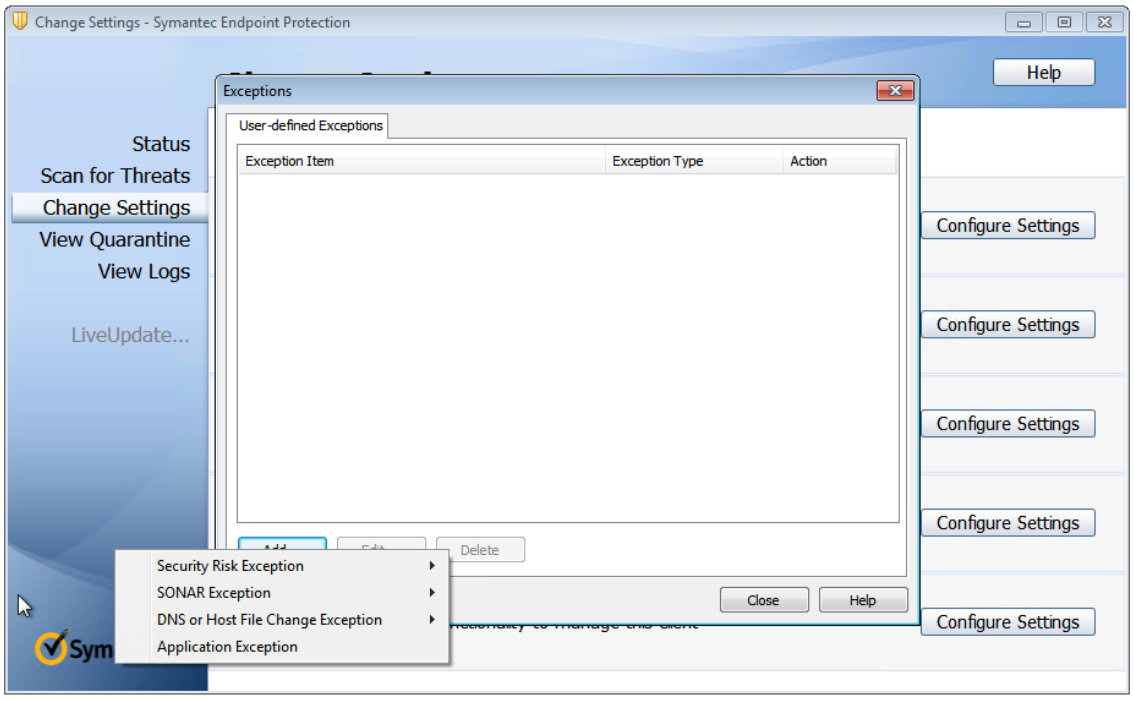
Symantec

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**:



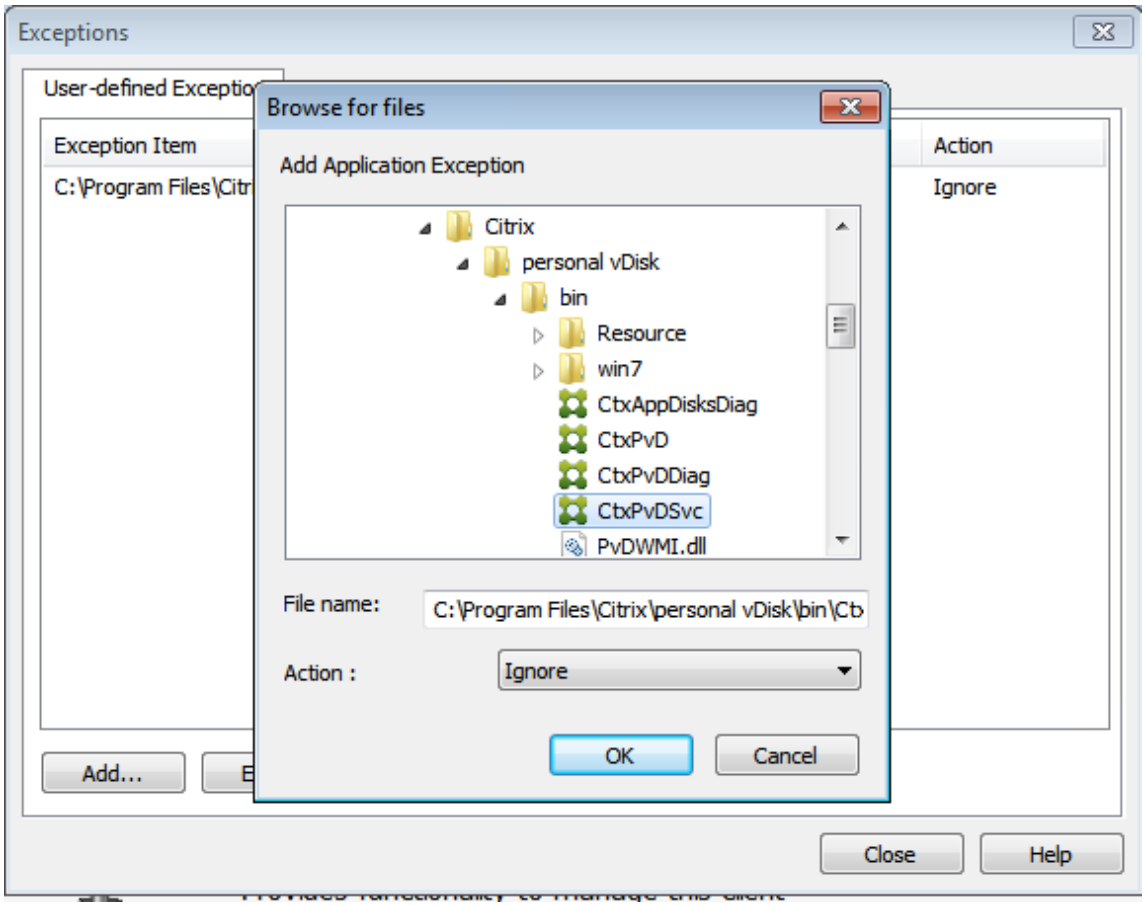
4. Klicken Sie im Bildschirm "Configure Settings"auf **Add**.
5. Es wird nun ein Kontextmenü zum Angeben des Typs "Anwendung"angezeigt. Wählen Sie **Application Exception**:



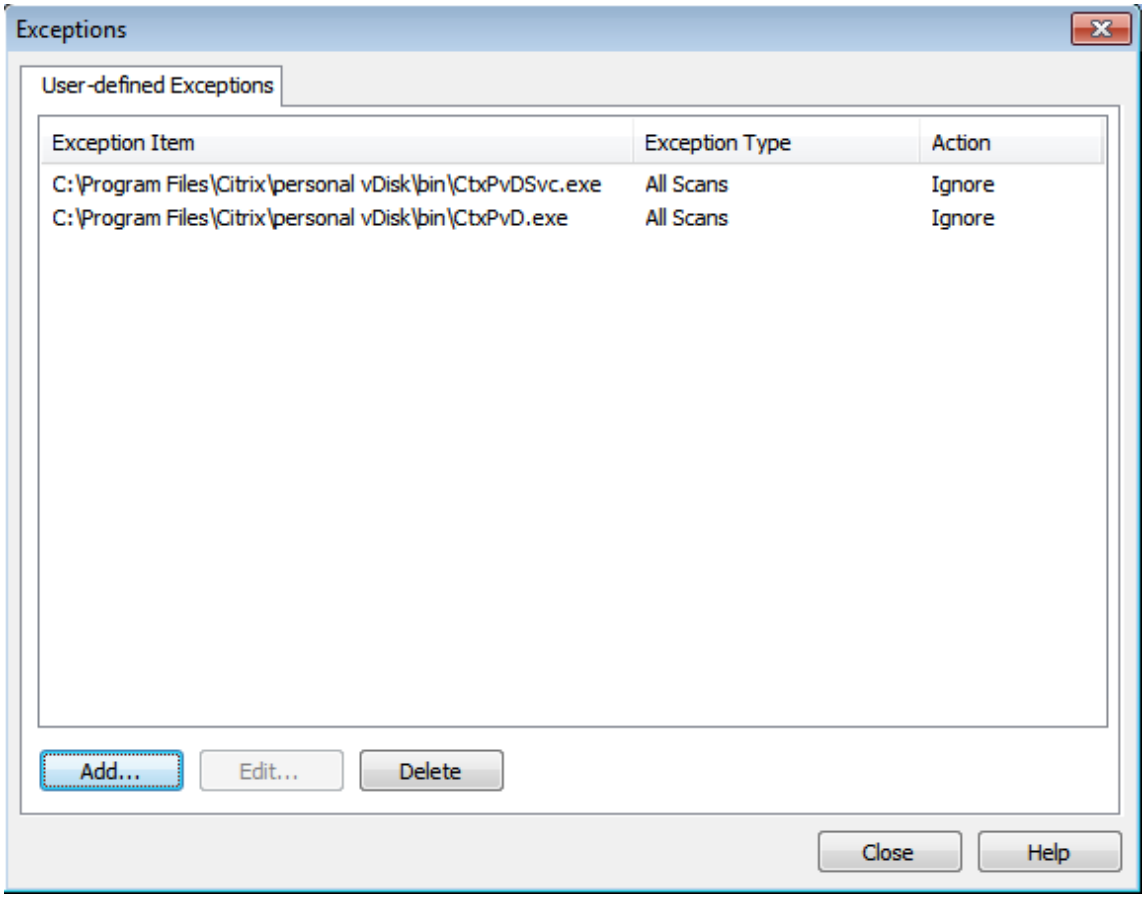
6. Geben Sie im Bildschirm "Exceptions"die folgenden AppDisk-Dateipfade ein und wählen Sie als Aktion **Ignore**:


```
C:\Program Files\Citrix\personal vDisk\bin\CtxPvD.exe
```

```
C:\Program Files\Citrix\personal vDisk\bin\CtxPvDSvc.exe
```



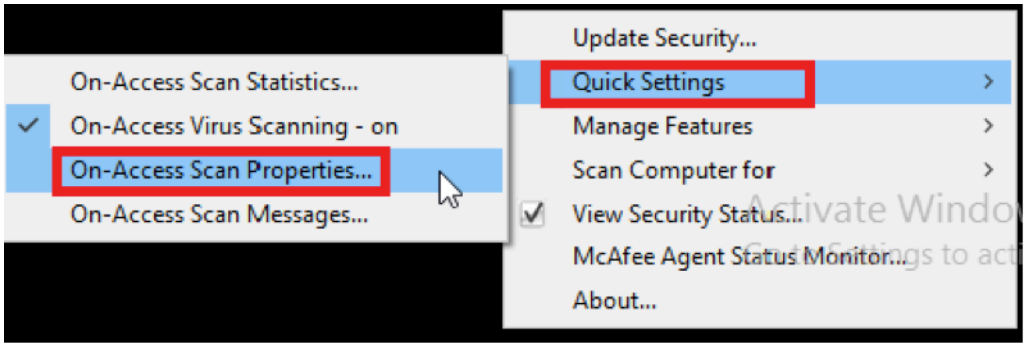
Die Ausnahmen werden der Liste hinzugefügt. Schließen Sie das Fenster, um die Änderungen anzuwenden.



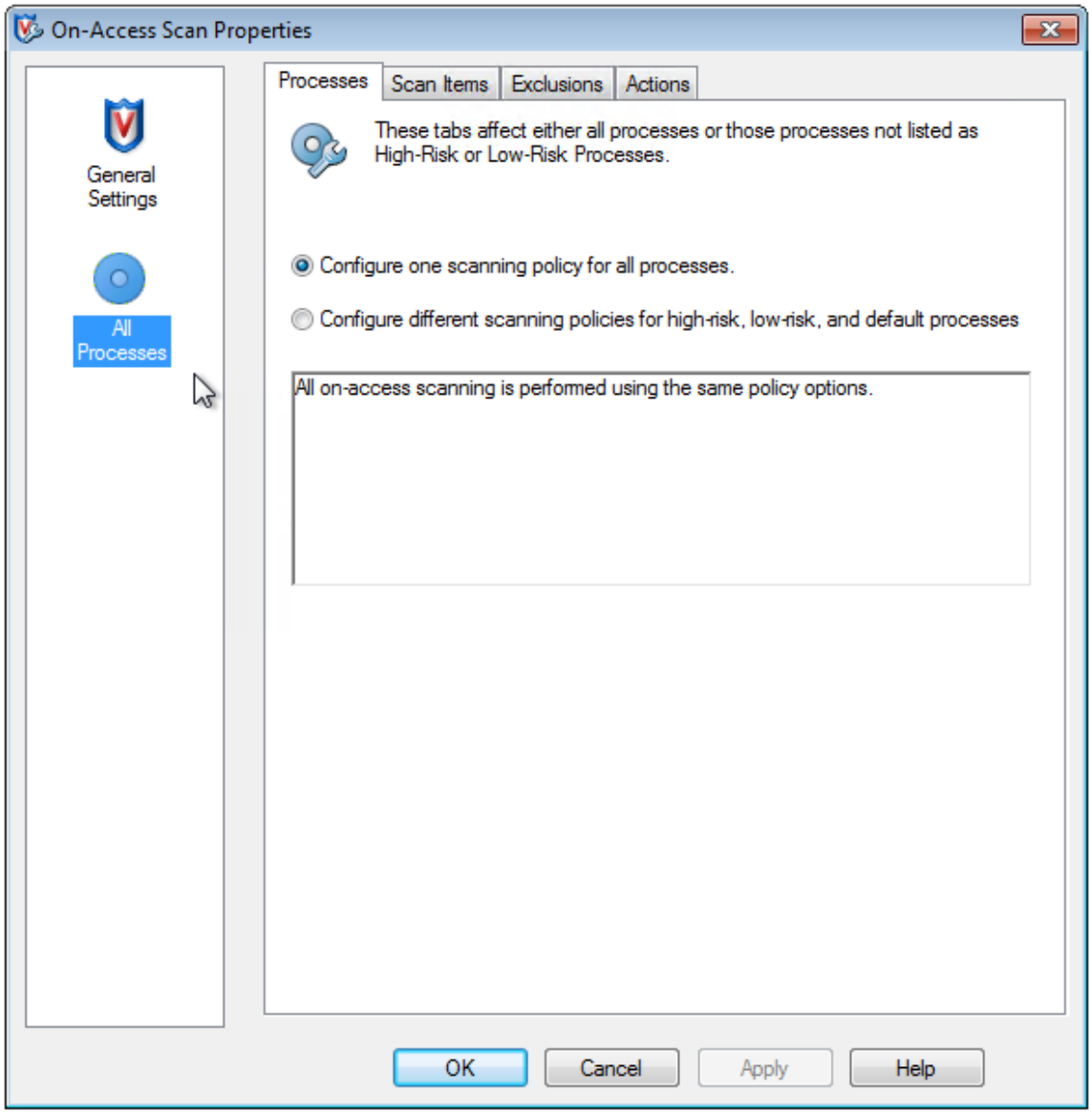
McAfee

Gehen Sie wie folgt vor, wenn auf der Basis-VM McAfee (Version 4.8) ausgeführt wird:

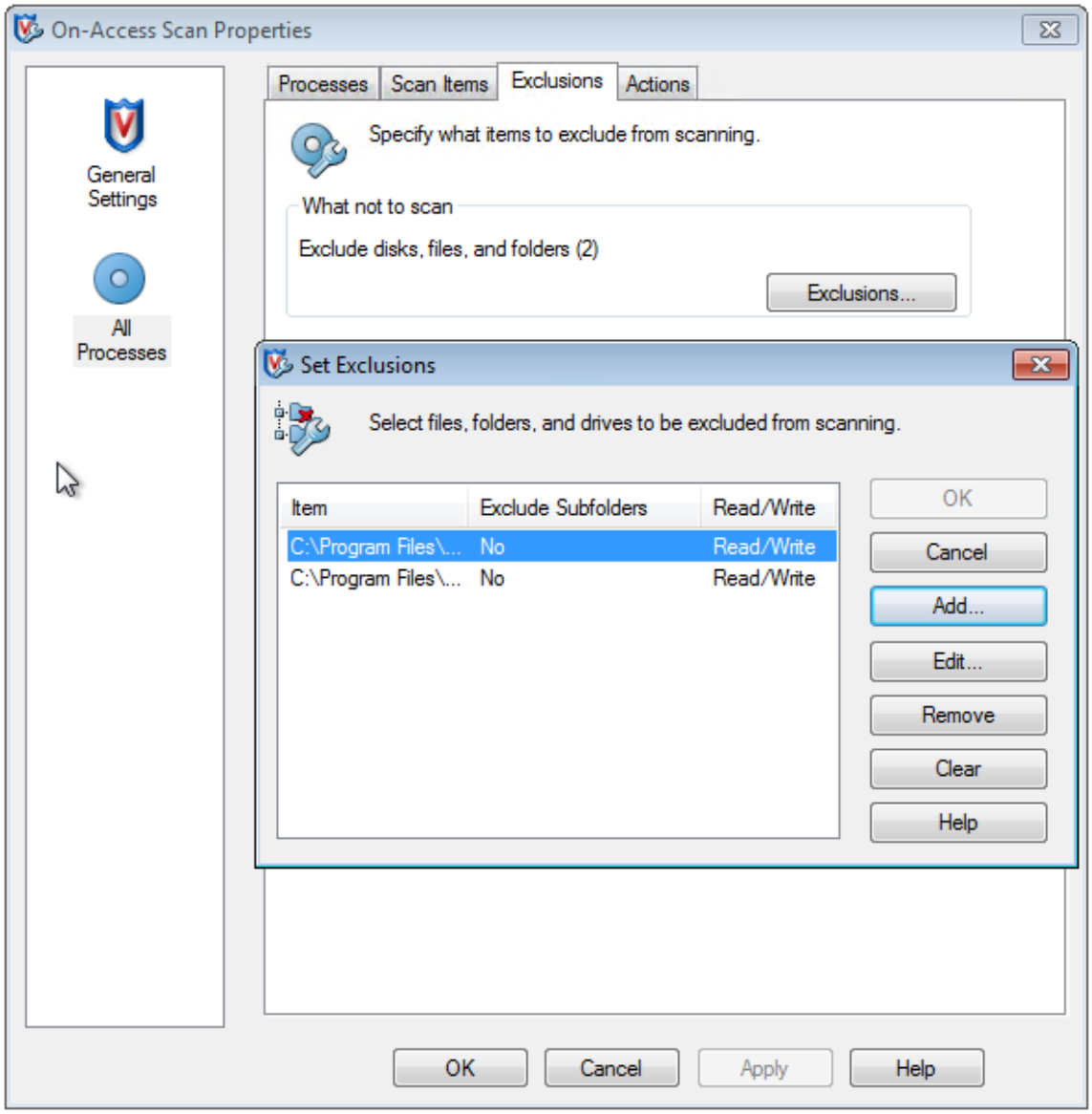
1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol und erweitern Sie die Option **Quick Settings**.
2. Wählen Sie **On-Access Scan Properties**:



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**.

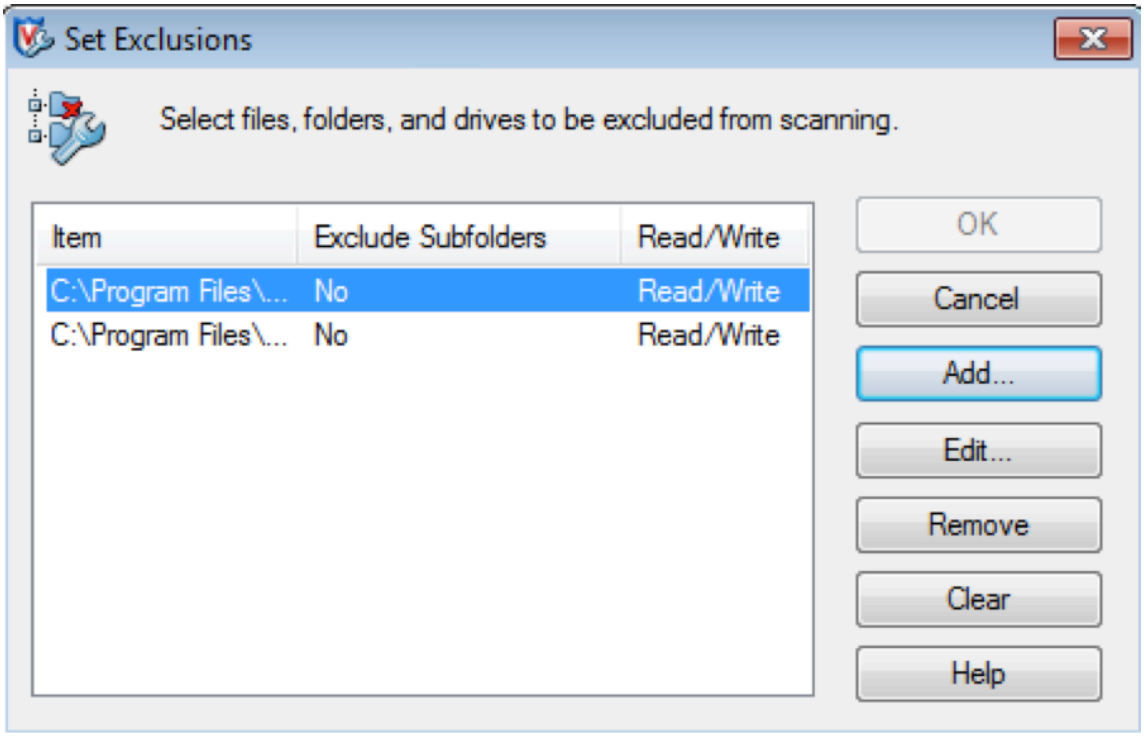


7. Wählen Sie im Bildschirm **Add Exclusion Item** die Option **By name/location (can include wild-cards * or ?)**. Klicken Sie auf **Browse**, um die ausführbaren Dateien zu suchen:

   ```
   C:\Program Files\Citrix\personal vDisk\bin\CtxPvD.exe
   ```

   ```
   C:\Program Files\Citrix\personal vDisk\bin\CtxPvDSvc.exe
   ```

8. Klicken Sie auf **OK**.
9. In dem Bildschirm **Set Exclusions** werden jetzt die hinzugefügten Ausschlüsse angezeigt. Klicken Sie auf **OK**, um die Änderungen anzuwenden:



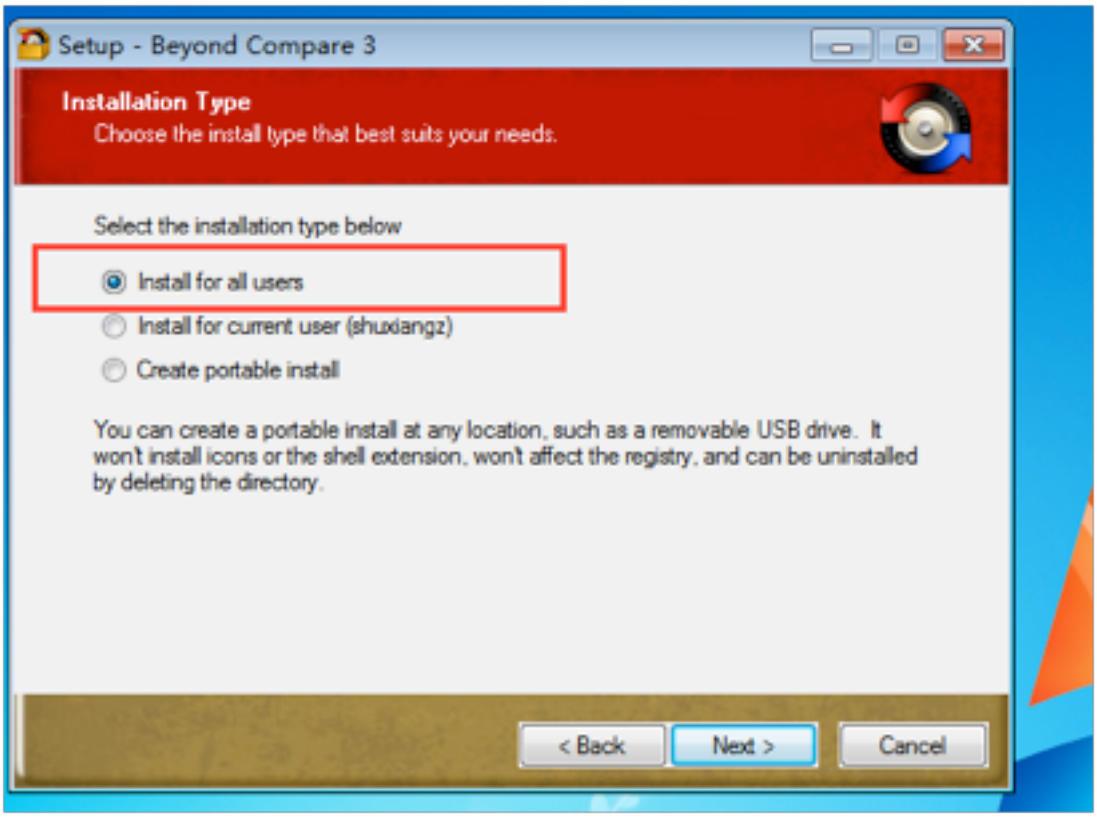
Wenn Sie die Ausschlüsse konfiguriert haben, erstellen Sie die AppDisk.

Anzeige von Anwendungen im Startmenü

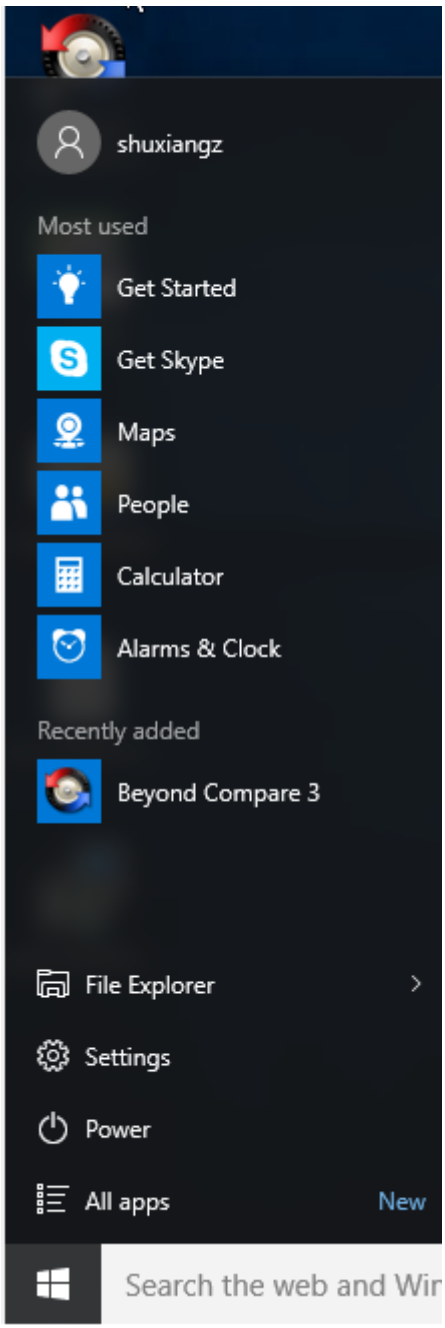
Wenn Sie eine neue AppDisk erstellen und eine Anwendung für alle Benutzer verfügbar machen, wird die AppDisk dem Desktop angefügt und eine Verknüpfung mit der Anwendung im Startmenü angezeigt. Wenn Sie eine AppDisk erstellen und nur für den aktuellen Benutzer installieren und die AppDisk dem Desktop angefügt wird, wird keine Verknüpfung mit der Anwendung im Startmenü angezeigt.

Beispiel für das Erstellen einer neuen Anwendung mit Bereitstellung für alle Benutzer:

1. Installieren Sie eine Anwendung auf der AppDisk (in diesem Beispiel *Beyond Compare*):

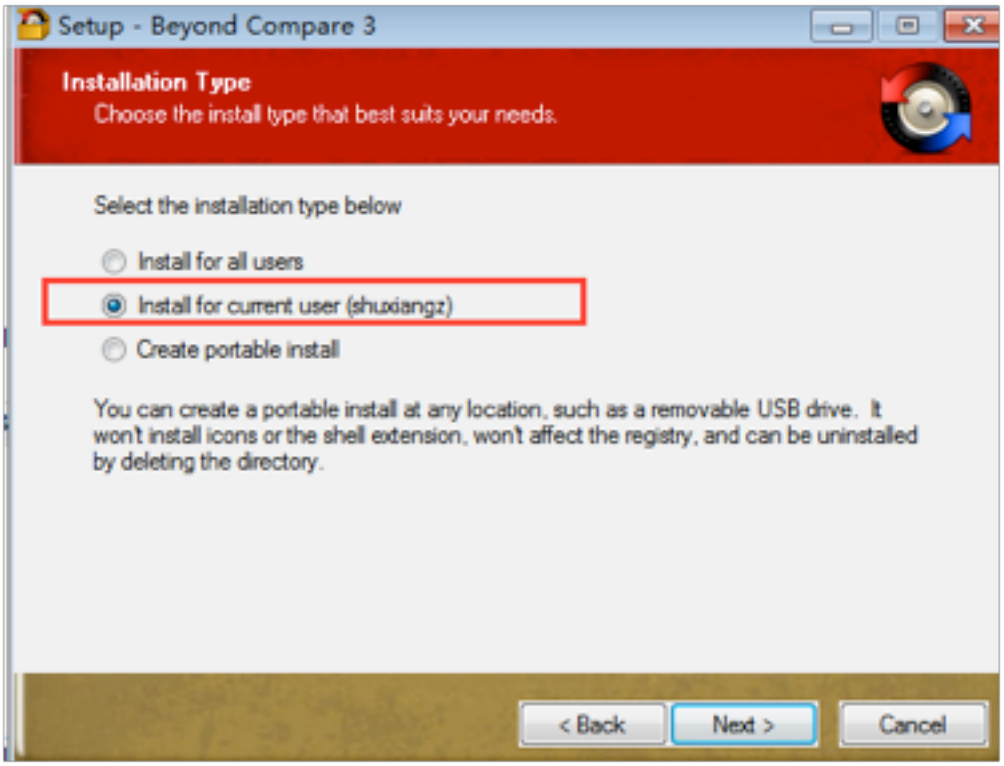


2. Fügen Sie die AppDisk dem Desktop an. Die Verknüpfung für das neu installierte *Beyond Compare* erscheint nun im Startmenü:

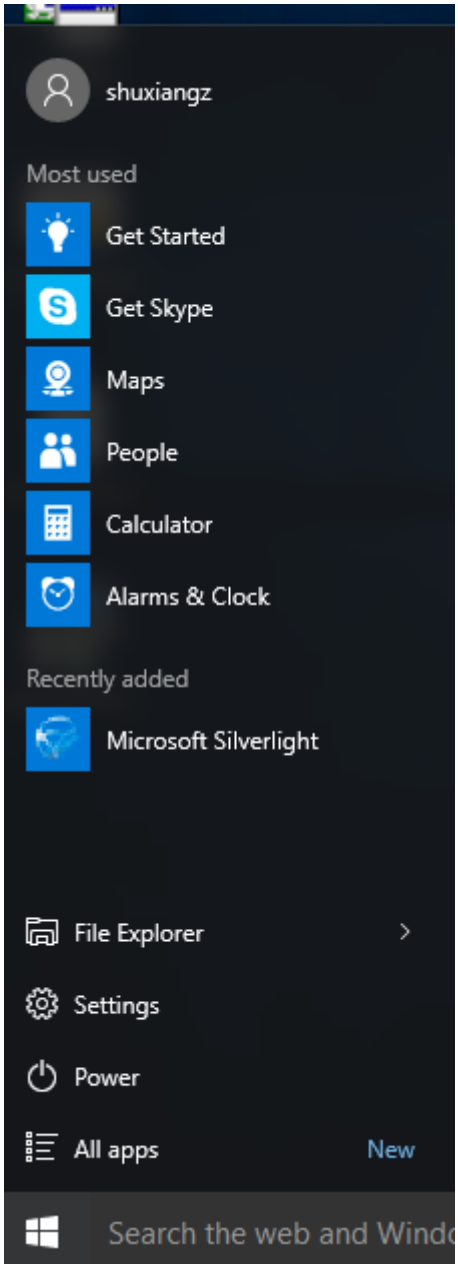


Ausschließliches Installieren der Anwendung für den aktuellen Benutzer:

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:



AppDisk-Protokollierung

AppDisk-Benutzer können Diagnoseinformationen abrufen und optional auf die Citrix Insight Services (CIS)-Website hochladen.

Funktionsweise

Für die Funktion wird ein skriptbasiertes 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 strukturierten Einzeldatei komprimiert und dann die Option zum lokalen Speichern der Datei bzw. 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 CIS-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

Die Skripts sind im Ordner C:\Programme\Citrix\personal vdisk\bin\scripts. Die PowerShell-Skripts müssen als Administrator ausgeführt werden.

Upload-AppDDiags.ps1 Verwenden Sie dieses Skript zum Sammeln von Diagnosedaten für AppDisk und optional zum manuellen Hochladen der Daten auf die CIS-Website.

```
Upload-AppDDiags [[-OutputFile] <string>] [-help] [<CommonParameters
>]
```

`-OutputFile`: lokaler Pfad für die ZIP-Datei statt Hochladen in CIS. Wenn `–OutputFile` nicht angegeben wird, erfolgt der Upload. Wird `–OutputFile` angegeben, erstellt das Skript eine ZIP-Datei, die Sie später manuell hochladen können.

Beispiele:

- `Upload-AppDDiags`: lädt die Diagnosedaten auf die Citrix CIS-Website unter Verwendung der vom interaktiven Benutzer eingegebenen Anmeldeinformationen hoch.
- `Upload-AppDDiags -OutputFile C:\MyDiags.zip`: speichert AppDisk-Diagnosedaten in der angegebenen ZIP-Datei. Sie können später auf https://cis.citrix.com/ zugreifen, um sie hochzuladen.

Upload-PvDDiags.ps1 Verwenden Sie dieses Skript zum Sammeln von Diagnosedaten für PvD und optional zum manuellen Hochladen der Daten auf die CIS-Website.


```
Upload-PvDDiags [[-OutputFile] <string>] [-help] [<CommonParameters>]
```

-OutputFile: lokaler Pfad für die ZIP-Datei statt Hochladen in CIS. Wenn –OutputFile nicht angegeben wird, erfolgt der Upload. Wird –OutputFile angegeben, erstellt das Skript eine ZIP-Datei, die Sie später manuell hochladen können.

Beispiele:

- Upload-PvDDiags: lädt die PvD-Diagnosedaten auf die Citrix CIS-Website unter Verwendung der vom interaktiven Benutzer eingegebenen Anmeldeinformationen hoch.
- Upload-PvDDiags -OutputFile C:\MyDiags.zip: speichert PvD-Diagnosedaten in der angegebenen ZIP-Datei. Sie können später auf https://cis.citrix.com/ zugreifen, um sie hochzuladen.

Veröffentlichen von Inhalten

September 21, 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.

Der veröffentlichte Inhalt erscheint wie andere Anwendungen in StoreFront und der Citrix Workspace-App. Die Benutzer greifen auf dieselbe Weise darauf 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.)

```
1 New-BrokerApplication –ApplicationType PublishedContent -
     CommandLineExecutable location -Name app-name -DesktopGroup delivery
     -group-name
2 <!--NeedCopy-->
```

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. http://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 or \\\\\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 Virtual Apps and Desktops Service-Bereitstellungen laden Sie das Citrix Virtual Apps and Desktops Remote PowerShell SDK herunter und installieren Sie es.
- Verwenden Sie bei lokalen Citrix Virtual Apps and Desktops-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
```

Wenn Sie Citrix Virtual Apps and Desktops 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.

```
1 $citrixUrl = "https://www.citrix.com/"
2 $appName = "Citrix Home Page"
3
4 New-BrokerApplication –ApplicationType PublishedContent –
     CommandLineExecutable $citrixURL –Name $appName –DesktopGroup $dg.
     Uid
5 <!--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.

```
1 $rtfUNC = "\GMSXJ-EDGE0.xd.local\PublishedResources\PublishedRTF.rtf"
2 $rtfAppName = "PublishedRTF"
3
```



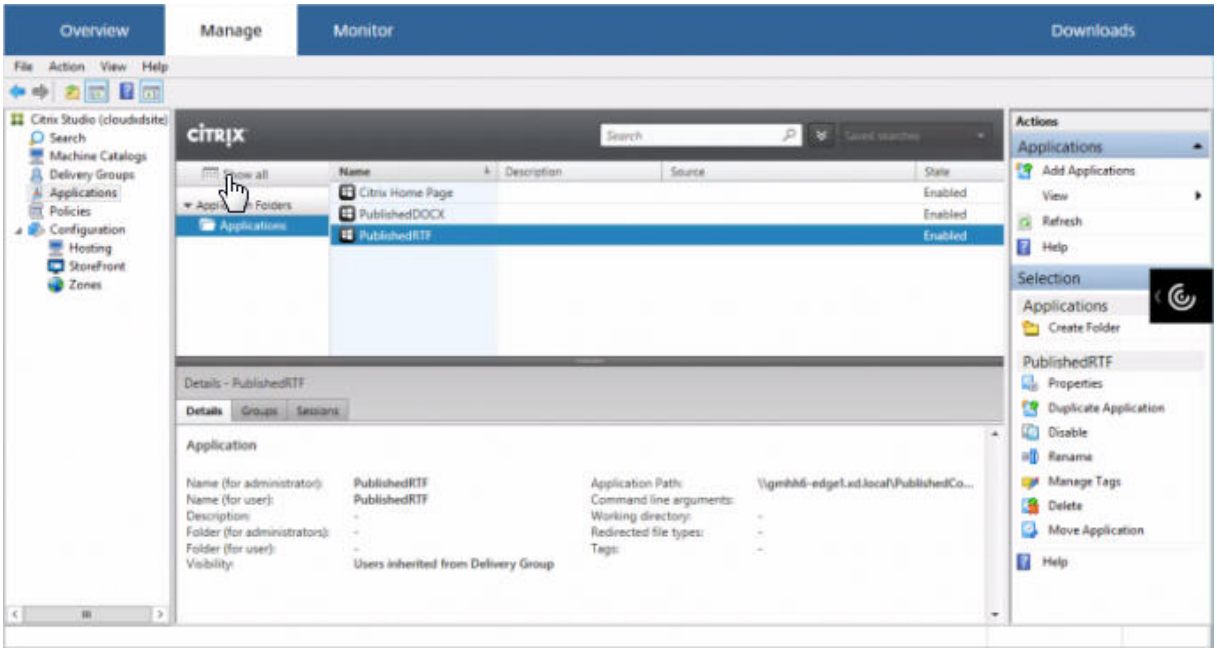
```
New-BrokerApplication –ApplicationType PublishedContent
–CommandLineExecutable $rtfUNC -Name $rtfAppName
-DesktopGroup $dg.Uid

$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

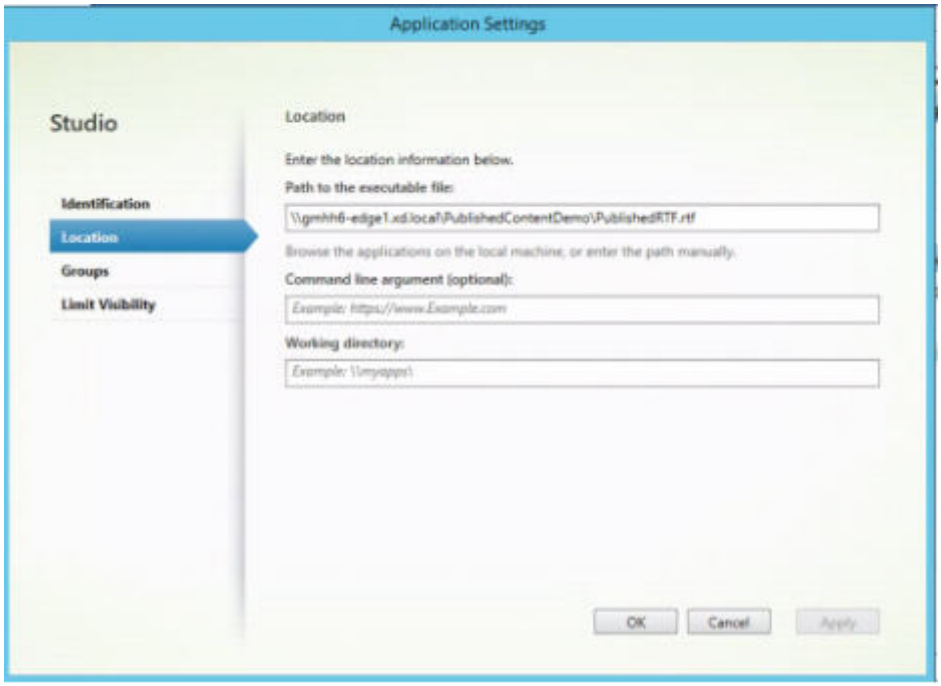
- Aktualisieren Sie Ihr StoreFront-Fenster, um die neu veröffentlichten Dokumente anzuzeigen.
- Klicken Sie auf die Anwendungen **PublishedRTF** und **PublishedDOCX**. Beide Dokumente werden in einer lokal ausgeführten WordPad-Instanz geöffnet.

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.

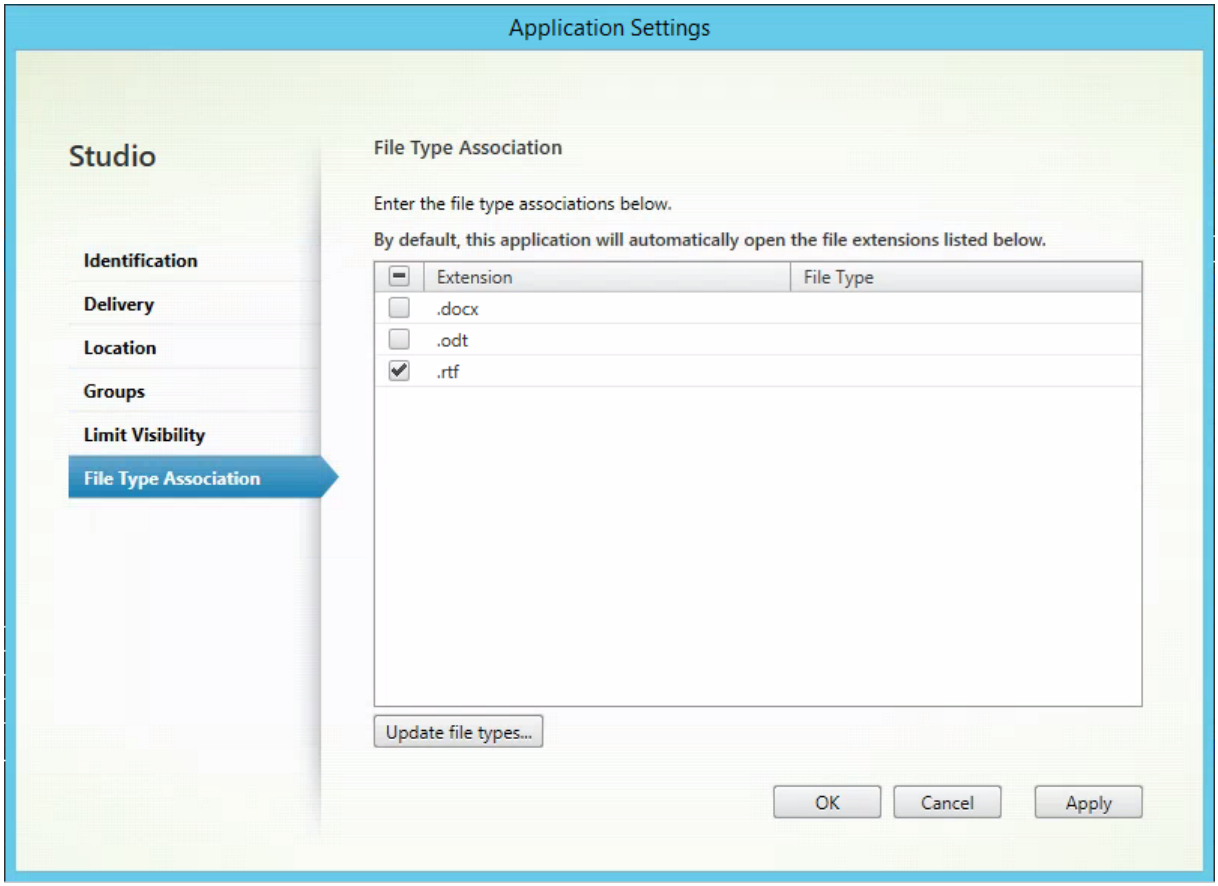


Anwendungseigenschaften (z. B. Benutzersichtbarkeit, Gruppenzuordnung und Verknüpfung) gelten für die veröffentlichten Inhalte. Befehlszeilenargumente und Arbeitsverzeichnis können Sie auf der Seite **Speicherort** jedoch nicht ändern. Zum Ändern der Ressource ändern Sie das Feld **Pfad zur ausführbaren Datei** auf dieser Seite.

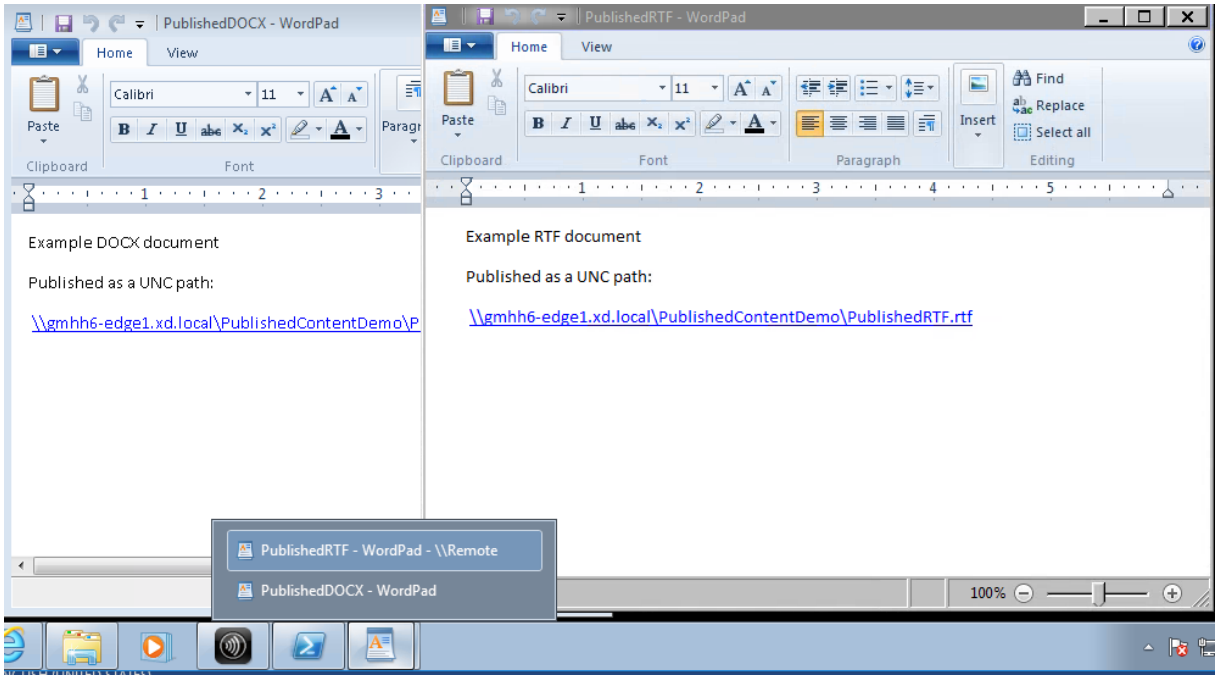


Um anstatt einer lokalen Anwendung eine veröffentlichte Anwendung zum Öffnen einer PublishedContent-Anwendung zu verwenden, bearbeiten Sie die Eigenschaft **Dateitypzuordnung** der veröffentlichten Anwendung. In diesem Beispiel wurde der veröffentlichten WordPad-Anwendung die Dateitypzuordnung für RTF-Dateien zugewiesen.

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 von App-Eigenschaften

Server-VDI

September 21, 2021

Verwenden Sie das Server-VDI-Feature (Virtual Desktop Infrastructure), um einen Desktop von einem Serverbetriebssystem einem einzelnen Benutzer bereitzustellen.

- Enterprise-Administratoren können Serverbetriebssysteme als VDI-Desktops bereitstellen. Dies ist für Benutzer, z. B. Techniker und Designer, nützlich.
- Dienstanbieter können Desktops von der Cloud anbieten. Diese Desktops entsprechen dem Microsoft Services Provider License Agreement (SPLA).

Mit der Citrix Richtlinieneinstellung "Enhanced Desktop Experience"können Sie das Serverbetriebssystem wie ein Desktopbetriebssystem aussehen lassen.

Die folgenden Features können nicht mit der Server-VDI verwendet werden:

- Personal vDisks
- Gehostete Anwendungen
- Lokaler App-Zugriff
- Direkte (nicht vermittelte) Desktopverbindungen
- Remote-PC-Zugriff

Server-VDI wird derzeit unter Windows Server 2019 und Windows Server 2016 unterstützt.

Damit die Server-VDI mit TWAIN-Geräten wie etwa Scannern funktioniert, muss das Windows-Feature Desktopdarstellung installiert werden.

Installieren und Konfigurieren von Server-VDI

1. Vorbereiten des Windows-Servers für die Installation

   - Stellen Sie mit dem Windows-Server-Manager sicher, dass die Rollendienste für Remotedesktopdienste nicht installiert sind. Wenn sie installiert sind, entfernen Sie die Dienste. Die VDA-Installation schlägt fehl, wenn diese Rollendienste installiert sind.
   - Stellen Sie sicher, dass die Eigenschaft "Nur eine Sitzung pro Benutzer zulassen"aktiviert ist. Bearbeiten Sie auf der Windows Server-Maschine die Terminalservereinstellung der Registrierung:
     - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer
     - DWORD fSingleSessionPerUser = 1

2. Installieren Sie einen VDA über die Befehlszeilenschnittstelle des Citrix Virtual Apps and Desktops-Installationsprogramms mit den Optionen "/quiet"und "/servervdi"auf einem unterstützten Server oder einem Servermasterimage. (In der Standardeinstellung blockiert die grafische Benutzeroberfläche des Installationsprogramms den VDA für Windows-Einzelsitzungs-OS auf einem Serverbetriebssystem. Durch die Verwendung der Befehlszeile kann dieses Verhalten überbrückt werden.) Verwenden Sie einen der folgenden Befehle:

   - Citrix Virtual Apps and Desktops-Bereitstellungen:
     - `XenDesktopVdaSetup.exe /quiet /servervdi`
     - `VDAWorkstationSetup.exe /quiet /servervdi`
   - Citrix Virtual Apps and Desktops Service-Bereitstellungen:
     - `VDAWorkstationSetup.exe /quiet /servervdi`

   Andere Optionen:

   - Sie können den Delivery Controller oder Cloud Connector mit der Option "controllers" angeben.

- Öffnen Sie mit der Option `enable_hdx_ports` Ports in der Firewall, wenn diese nicht manuell konfiguriert wird.
- Fügen Sie die Option `mastermcsimage` oder `masterimage` hinzu, wenn Sie den VDA auf einem Image installieren, und verwenden Sie MCS zum Erstellen von Server-VMs von diesem Image.
- Schließen Sie keine Optionen für Features ein, die nicht mit Server-VDI unterstützt werden, u. a. "baseimage"(für persönliche vDisks).
- Informationen zu allen Optionen finden Sie unter Installieren über die Befehlszeile.

3. Erstellen Sie einen Maschinenkatalog für Server-VDI. Im Assistenten für die Katalogerstellung:

   - Wählen Sie auf der Seite **Betriebssystem** die Option **Einzelsitzungs-OS**.
   - Geben Sie auf der Seite **Zusammenfassung** einen Maschinenkatalognamen und eine Beschreibung für Administratoren an, die klar auf Server-VDI hinweisen. Dies ist die einzige Angabe in Studio, dass der Katalog Server-VDI unterstützt.

   Wenn Sie eine Suche in Studio durchführen, wird der Server-VDI-Katalog auf der Registerkarte **Maschinen mit Betriebssystemen für Einzelsitzungen** angezeigt, obwohl der VDA auf einem Server installiert wurde.

4. Erstellen Sie eine Bereitstellungsgruppe und wählen Sie den zuvor erstellten Server-VDI-Katalog zu.

Wenn Sie bei der VDA-Installation keine Delivery Controller oder einen Cloud Connector angegeben haben, holen Sie das anschließend nach. Informationen hierzu finden Sie unter VDA-Registrierung.

Benutzerpersonalisierungslayer

March 15, 2022

Der Benutzerpersonalisierungslayer ist ein Feature für Citrix Virtual Apps and Desktops, das die Funktionen nicht persistenter Maschinenkataloge erweitert. Benutzerpersonalisierungslayer speichern Benutzerdaten und lokal installierte Anwendungen über Sitzungen hinweg. Das Feature wird von Citrix App Layering unterstützt und ersetzt die persönliche vDisk (PvD).

Wie PvD funktioniert der Benutzerpersonalisierungslayer mit Citrix Provisioning und Maschinenerstellungsdiensten (MCS) in einem nicht persistenten Maschinenkatalog. Die Komponenten des Features werden zusammen mit dem VDA (Virtual Delivery Agent) im Windows 10-Masterimage installiert.

Die Anwendungen und Daten, die Benutzer erstellen, werden auf der eigenen virtuellen Benutzerlayer-Festplatte in einer VHD-Datei gespeichert, die auf dem Image bereitgestellt wird.

Dieses Dokument enthält Anweisungen zum Bereitstellen und Konfigurieren des Benutzerpersonalisierungslayers. Es werden die Anforderungen für eine erfolgreiche Bereitstellung sowie Einschränkungen und bekannte Probleme beschrieben.

Um den Benutzerpersonalisierungslayer zu verwenden, müssen Sie ihn zunächst über die im Artikel beschriebene Schrittfolge bereitstellen. Erst dann steht Ihnen dieses Feature zur Verfügung.

Anwendungsunterstützung

Bis auf folgende Ausnahmen werden alle Anwendungen, die ein Benutzer lokal auf dem Desktop installiert, im Benutzerpersonalisierunglayer unterstützt.

Ausnahmen

Die folgenden Anwendungen werden *nicht* im Benutzerpersonalisierungslayer unterstützt:

- Unternehmensanwendungen wie MS Office und Visual Studio.
- Anwendungen, die den Netzwerkstapel oder die Hardware ändern. Beispiel: ein VPN-Client.
- Anwendungen mit Treibern auf Startebene. Beispiel: ein Virenscanner.
- Anwendungen mit Treibern, die den Treiberspeicher verwenden. Beispiel: ein Druckertreiber.

  > **Hinweis:**
  >
  > Sie können Drucker über Windows-Gruppenrichtlinienobjekte zur Verfügung stellen.

Nicht unterstützte Anwendungen dürfen *nicht* von Benutzern lokal installiert werden. Installieren Sie diese Anwendungen direkt auf dem Masterimage.

Anwendungen mit erforderlichem lokalen Benutzer- oder Administratorkonto

Wenn ein Benutzer eine Anwendung lokal (auf seinem Benutzerlayer) installiert und dann einen dafür benötigten lokalen Benutzer oder eine Gruppe hinzufügen oder bearbeiten möchte, werden die Änderungen des Benutzers oder der Gruppe *nicht* übernommen.

> **Wichtig:**
>
> Fügen Sie alle erforderlichen lokalen Benutzer oder Gruppen im Masterimage hinzu.

Anforderungen

Der Benutzerpersonalisierungslayer erfordert folgende Komponenten:

- Citrix Virtual Apps and Desktops 7 1909 oder höher
- Virtual Delivery Agent (VDA), Version 1912
- Citrix Provisioning, Version 1909 oder höher
- Windows-Dateifreigabe (SMB)
- Windows 10 Enterprise x64, Version 1607 oder höher

> **Wichtig:**
>
> - Bei installierter Preview-Version des Benutzerpersonalisierungslayers deinstallieren Sie sie und starten Sie das Masterimage neu, bevor Sie diese Version installieren.
> - Wie weiter unten beschrieben, müssen Sie die Richtlinien in Studio definieren und sie der Bereitstellungsgruppe zuweisen, die an den Maschinenkatalog mit bereitgestelltem Benutzerpersonalisierungslayer gebunden ist. Wenn kein Benutzerpersonalisierungslayer auf dem Masterimage konfiguriert ist, bleiben die Dienste inaktiv und beeinträchtigen nicht die Erstellungsaktivitäten. Wenn Sie die Richtlinien im Masterimage festlegen, versuchen die Dienste im Benutzerpersonalisierungslayer, einen Benutzerlayer im Masterimage auszuführen und bereitzustellen. Da diese Umgebung dazu dient, Änderungen am Image vorzunehmen, kann dies zu unerwartetem Verhalten und zu Instabilität im Masterimage führen.

Empfehlungen

Befolgen Sie die Empfehlungen in diesem Abschnitt, um den Benutzerpersonalisierungslayer fehlerfrei bereitzustellen.

Profilverwaltungslösung

Wir empfehlen, den Benutzerpersonalisierungslayer mit einer Profilverwaltungslösung wie Citrix Profilverwaltung zu verwenden.

Bei Verwendung der Profilverwaltung müssen Sie das Löschen der Benutzerinformationen bei der Abmeldung deaktivieren. Je nach gewählter Bereitstellung können Sie die Löschfunktion entweder mit einem Gruppenrichtlinienobjekt (GPO) oder mit der Richtlinie auf dem Delivery Controller (DDC) deaktivieren.

Einzelheiten zu den verfügbaren Profilverwaltungsrichtlinien finden Sie unter Beschreibungen der Richtlinien der Profilverwaltung und deren Standardwerte.

Microsoft System Center Configuration Manager

Wenn Sie den Benutzerpersonalisierungslayer mit SCCM verwenden, sollten Sie die bewährten Microsoft-Methoden zur Image-Vorbereitung in einer VDI-Umgebung nutzen. Weitere Informationen finden Sie in diesem Microsoft TechNet-Artikel .

Maximale Benutzerlayergröße

Wir empfehlen mindestens 10 GB für den Benutzerlayer.

> **Hinweis:**
>
> Bei der Installation führt der Wert Null (0) zum Verwenden des Standardwerts von 10 GB für den Benutzerlayer.

Ein in Windows festgelegtes Kontingent kann die maximale Größe des Benutzerlayers überschreiben Um die in Studio festgelegte maximale Benutzerlayergröße zu überschreiben, definieren Sie ein Kontingent für die Benutzerlayer-Dateifreigabe. Bei einem definierten Kontingent wird für den Benutzerlayer das Maximum der Kontingentgröße konfiguriert.

Verwenden Sie eines der folgenden Microsoft-Kontingenttools, um eine harte Kontingentgrenze für die Benutzerlayergröße festzulegen:

- Ressourcen-Manager für Dateiserver (FSRM)
- Kontingentmanager

Das Kontingent muss im Benutzerlayerverzeichnis “Benutzer”festgelegt werden.

> **Hinweis:**
>
> Das Erhöhen oder Verringern des Kontingents wirkt sich nur auf neue Benutzerlayer aus. Die maximale Größe vorhandener Benutzerlayer wird dadurch nicht geändert. Ihr Höchstwert bleibt unverändert, wenn das Kontingent aktualisiert wird.

Bereitstellen eines Benutzerpersonalisierungslayers

Führen Sie diese Schrittfolge aus, um das Benutzerpersonalisierungslayer-Feature bereitzustellen:

- Schritt 1: Überprüfen Sie die Verfügbarkeit einer Citrix Virtual Apps and Desktops-Umgebung.
- Schritt 2: Bereiten Sie Ihr Masterimage vor.
- Schritt 3: Erstellen Sie einen Maschinenkatalog.
- Schritt 4: Erstellen Sie eine Bereitstellungsgruppe.
- Schritt 5: Erstellen Sie benutzerdefinierte Richtlinien für die Bereitstellungsgruppe.

Schritt 1: Überprüfen der Verfügbarkeit einer Citrix Virtual Apps and Desktops-Umgebung

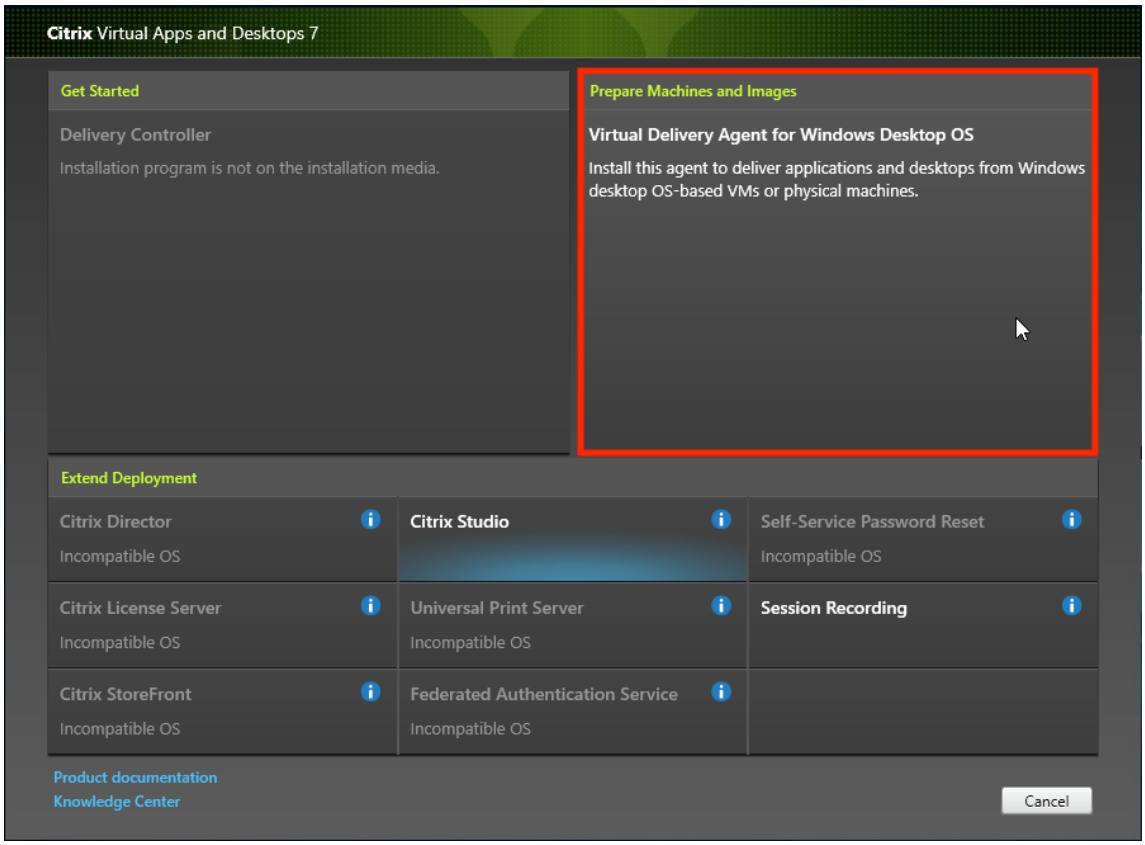
Stellen Sie sicher, dass Ihre Citrix Virtual Apps and Desktops-Umgebung mit diesem neuen Feature verwendet werden kann. Details zum Einrichten finden Sie unter "Installieren und Konfigurieren von Citrix Virtual Apps and Desktops".

Schritt 2: Vorbereiten Ihres Masterimages

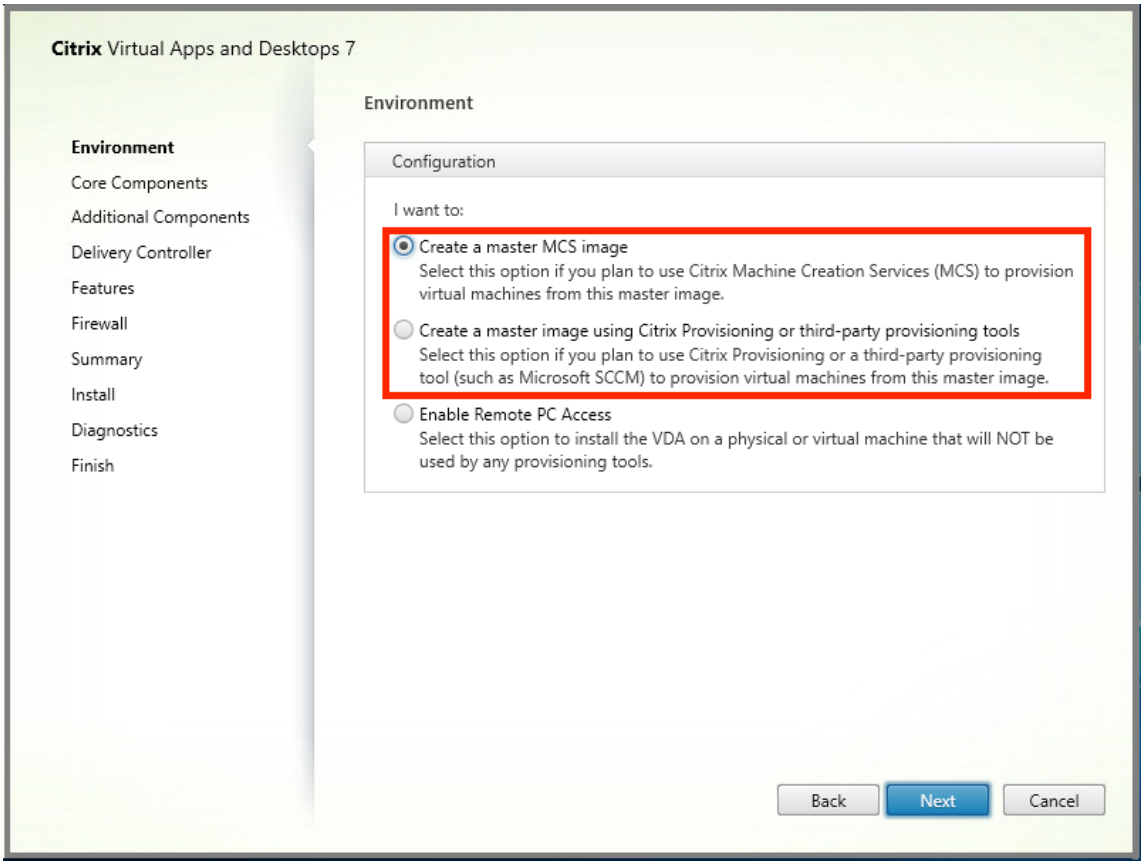
Zum Vorbereiten des Masterimages führen Sie folgende Schritte aus:

1. Suchen Sie das Masterimage. Installieren Sie die Unternehmensanwendungen Ihrer Organisation und alle übrigen Apps, die für Benutzer von Nutzen sein könnten.
2. Installieren Sie den Virtual Delivery Agent (VDA) 1912. Wenn bereits eine ältere VDA-Version vorhanden ist, deinstallieren Sie diese zunächst. Achten Sie bei der Installation der neuen Version darauf, die optionale Komponente Citrix User Personalization Layer wie folgt auszuwählen und zu installieren:

    a) Klicken Sie auf die Kachel **Virtual Delivery Agent für Windows-Desktopbetriebssysteme**.

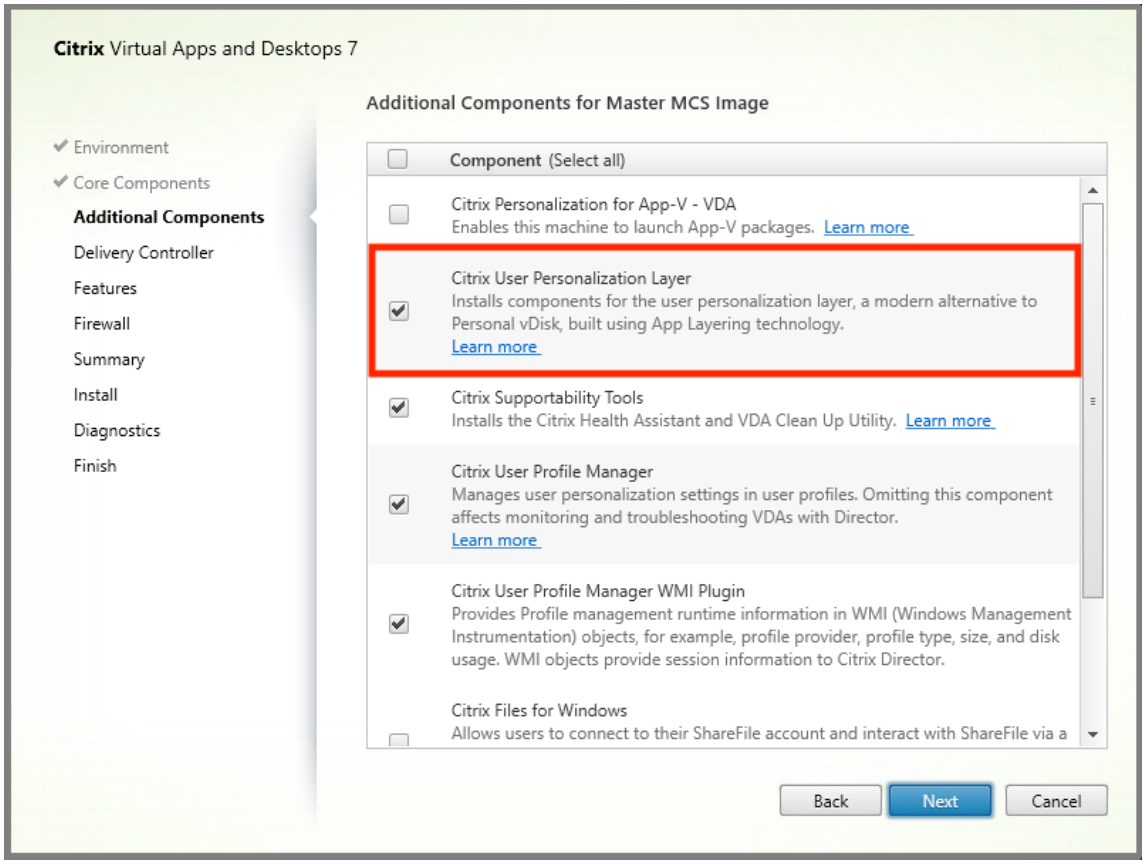


    a) **Umgebung:** Wählen Sie entweder "MCS-Masterimage erstellen"oder "Masterimage mit Citrix Provisioning oder Bereitstellungstools von Drittanbietern erstellen".



a) **Kernkomponenten:** Klicken Sie auf **Weiter**.

b) **Zusätzliche Komponenten:** Aktivieren Sie **Citrix User Personalization Layer**.



a) Konfigurieren Sie den VDA auf den restlichen Installationsbildschirmen nach Bedarf und klicken Sie auf “Installieren”. Das Image wird während der Installation mehrmals neu gestartet.

3. Lassen Sie **Windows-Updates** deaktiviert. Das Installationsprogramm für den Benutzerpersonalisierungslayer deaktiviert Windows-Updates auf dem Image. Lassen Sie die Updatefunktion deaktiviert.

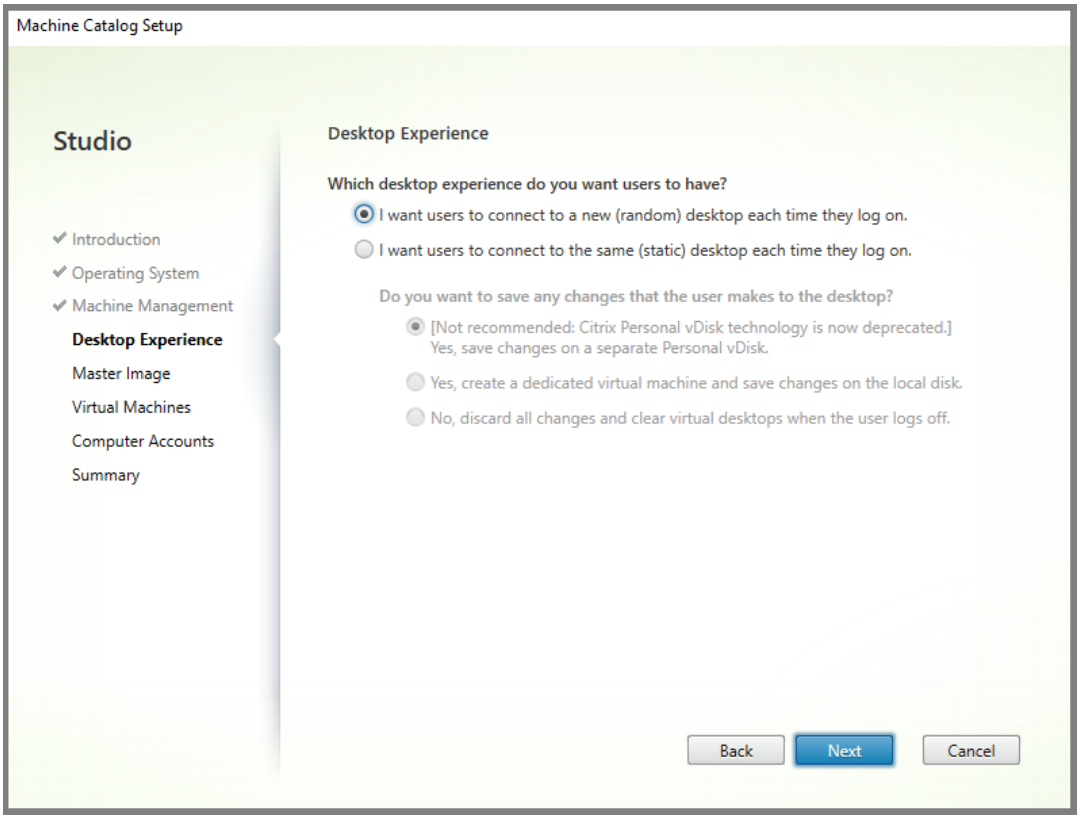
Das Image kann nun in Studio hochgeladen werden.

Schritt 3: Erstellen eines Maschinenkatalogs

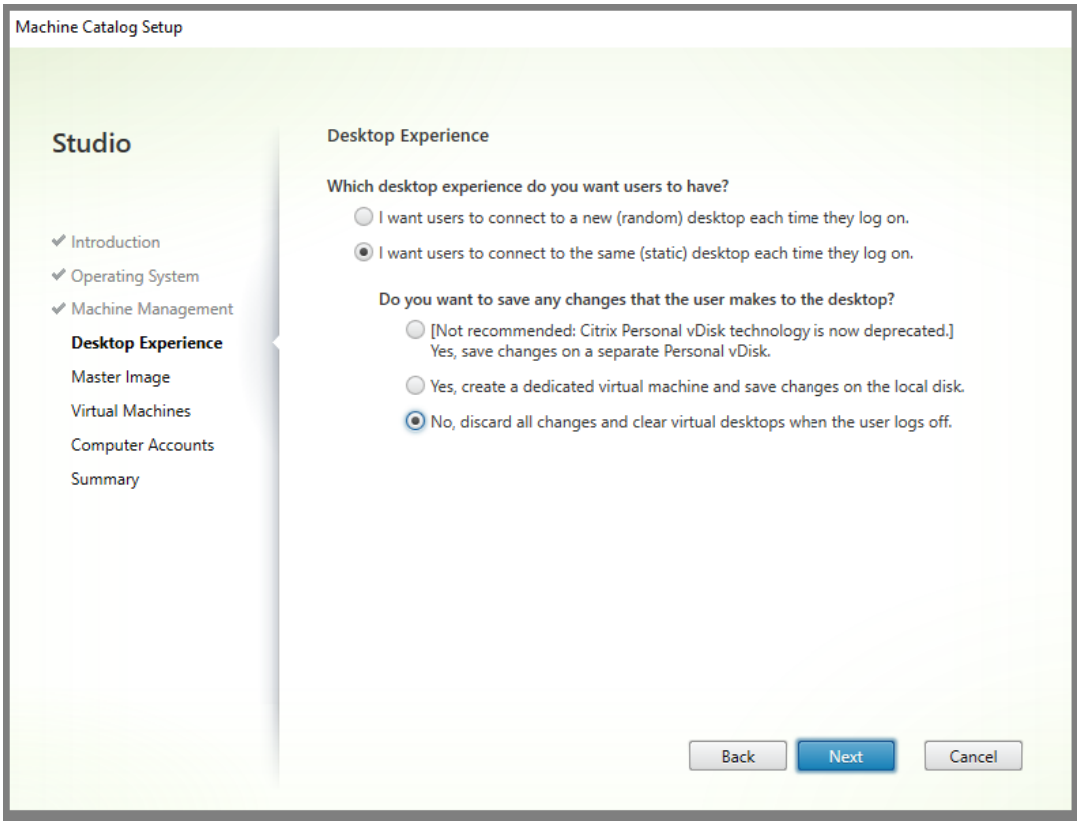
Führen Sie in Studio folgende Schritte aus, um einen Maschinenkatalog zu erstellen. Verwenden Sie die folgenden Optionen während der Katalogerstellung:

1. Wählen Sie unter **Betriebssystem** die Einstellung **Betriebssystem für Einzelsitzungen**.
2. Wählen Sie unter **Maschinenverwaltung** die Einstellung **Maschinen mit Energieverwaltung**. Zum Beispiel virtuelle Maschinen oder Blade-PCs.
3. Wählen Sie unter **Desktoperfahrung** den Katalogtyp **Gepoolt-zufällig** oder **Gepoolt-statisch**, wie in den folgenden Beispielen angegeben:

- **Gepoolt-zufällig:**



- **Gepoolt-statisch:** Bei Auswahl der gepoolt-statischen Einstellung legen Sie fest, dass beim Abmelden des Benutzers alle Änderungen verworfen und virtuelle Desktops gelöscht werden, wie im folgenden Screenshot angezeigt:



> **Hinweis:**
>
> Der Benutzerpersonalisierungslayer unterstützt keine gepoolt-statischen Kataloge, die zur Verwendung der persönlichen Citrix vDisk konfiguriert oder als dedizierte virtuelle Maschinen zugewiesen wurden.

4. Bei Verwendung von MCS wählen Sie **Masterimage** und den Snapshot für das im vorherigen Abschnitt erstellte Image.
5. Konfigurieren Sie die übrigen Katalogeigenschaften nach Bedarf für Ihre Umgebung.

Schritt 4: Erstellen einer Bereitstellungsgruppe

Erstellen und konfigurieren Sie eine **Bereitstellungsgruppe**, einschließlich der Maschinen aus dem erstellten Maschinenkatalog. Weitere Informationen finden Sie unter Erstellen von Bereitstellungsgruppen.

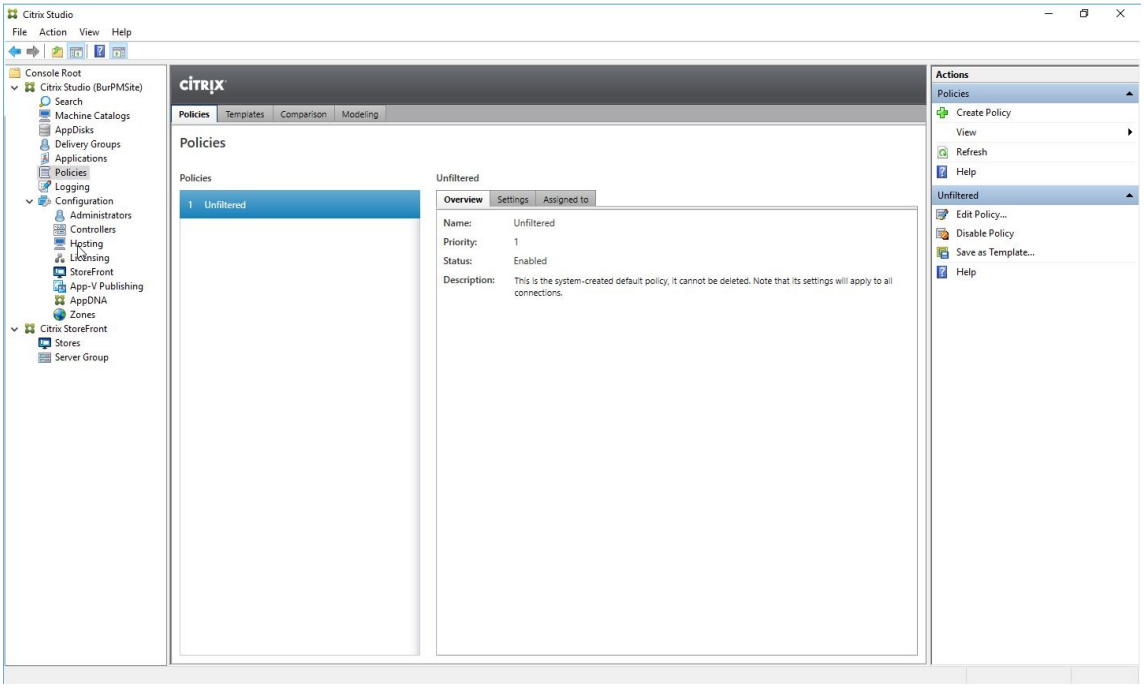
Schritt 5: Erstellen benutzerdefinierter Richtlinien für die Bereitstellungsgruppe

Um die Bereitstellung von Benutzerlayern in Virtual Delivery Agents zu aktivieren, verwenden Sie Konfigurationsparameter, um Folgendes zu definieren:

- Wo im Netzwerk auf die Benutzerlayer zugegriffen werden soll.
- Die maximale Größe der Datenträger für die Benutzerlayer.

Die folgende Schrittfolge zeigt, wie Sie die Parameter als benutzerdefinierte Citrix Richtlinien in Studio definieren und dann Ihrer Bereitstellungsgruppe zuweisen.

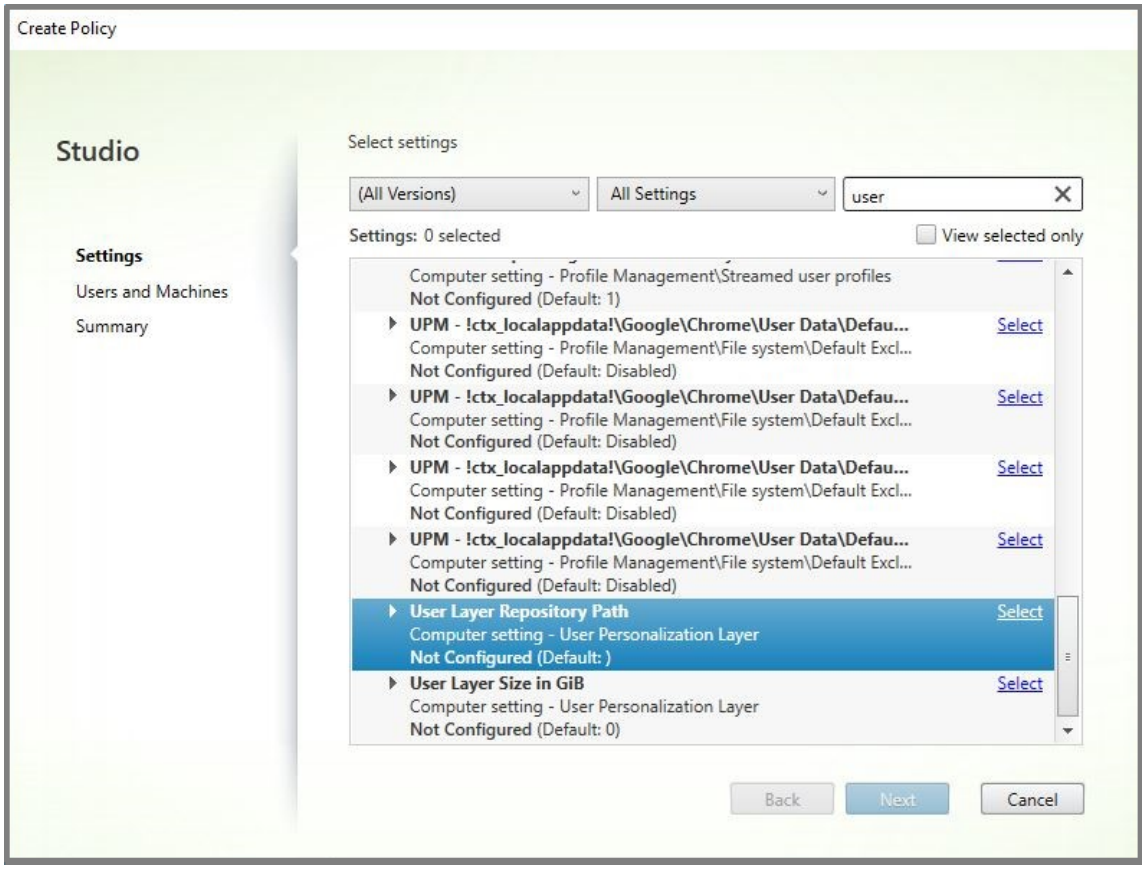
1. Wählen Sie im Studio-Navigationsbereich "Richtlinien"aus.



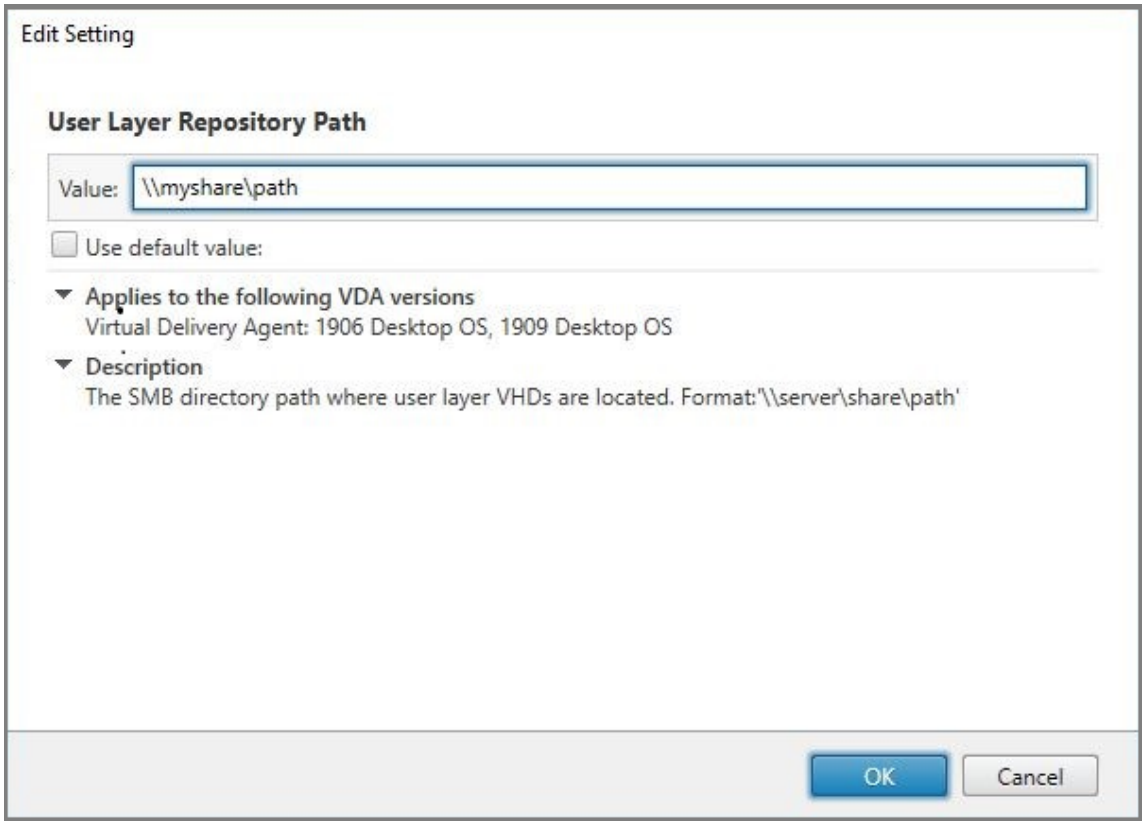
2. Wählen Sie im Aktionsbereich Richtlinie erstellen. Das Fenster "Richtlinie erstellen"wird angezeigt.
3. Geben Sie in das Suchfeld den Begriff "Benutzerlayer"ein. Zwei Richtlinien werden in der Liste der verfügbaren Richtlinien angezeigt:
   - Repositorypfad für Benutzerlayer
   - Größe von Benutzerlayer in GB

   > **Hinweis:**
   >
   > Durch das Ändern der Benutzerlayergröße in der Richtlinie wird die Größe vorhandener Layer nicht geändert.

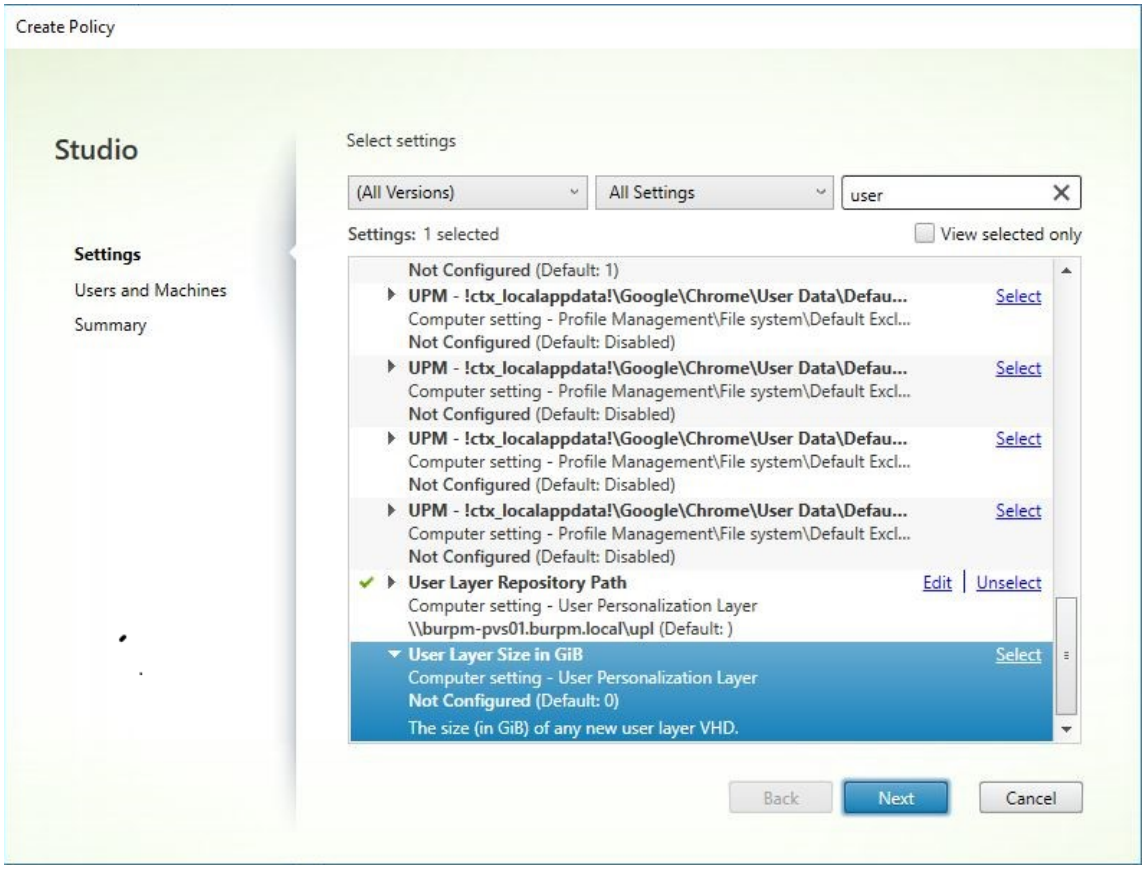
4. Klicken Sie neben "Repositorypfad für Benutzerlayer"auf **Auswählen**. Das Fenster "Einstellung bearbeiten"wird angezeigt.



5. Geben Sie einen Pfad im Format `\\server name or address\folder name` in das Feld “Wert”ein und klicken Sie auf **OK**:



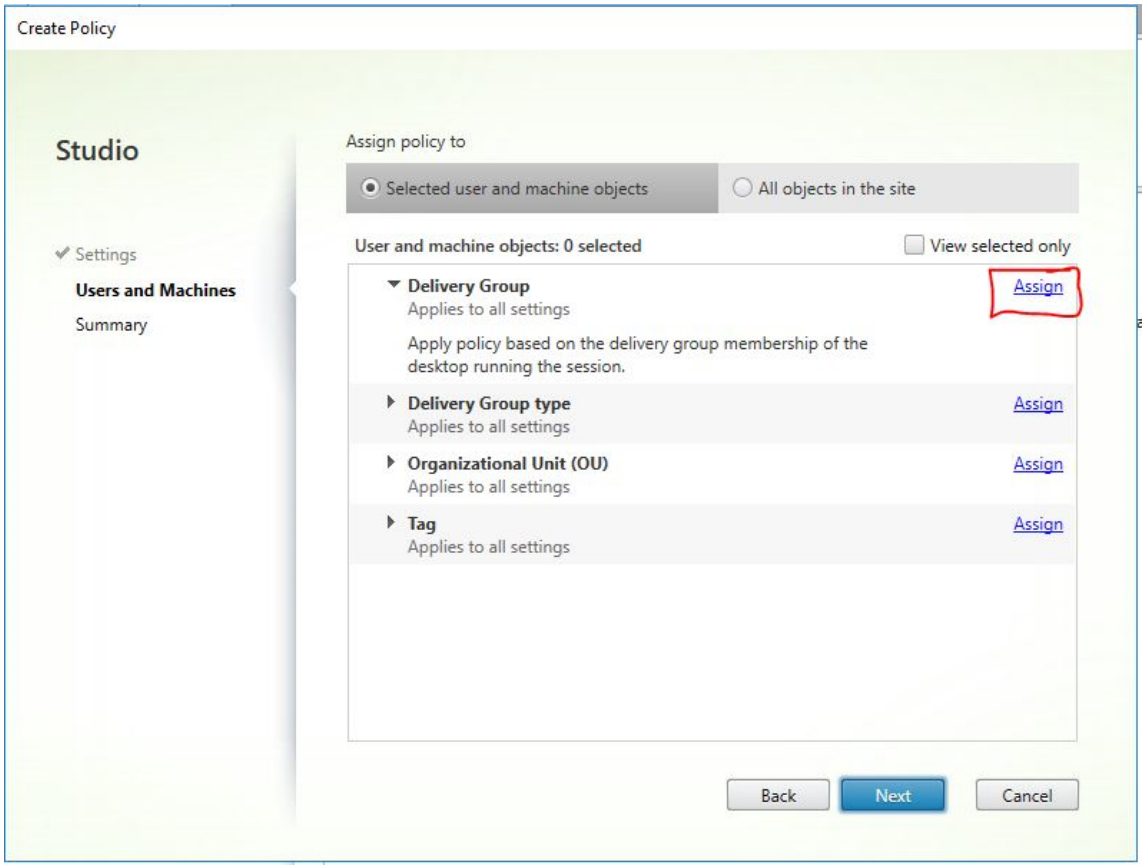
6. Optional: Klicken Sie neben “Größe von Benutzerlayer in GB”auf **Auswählen**:



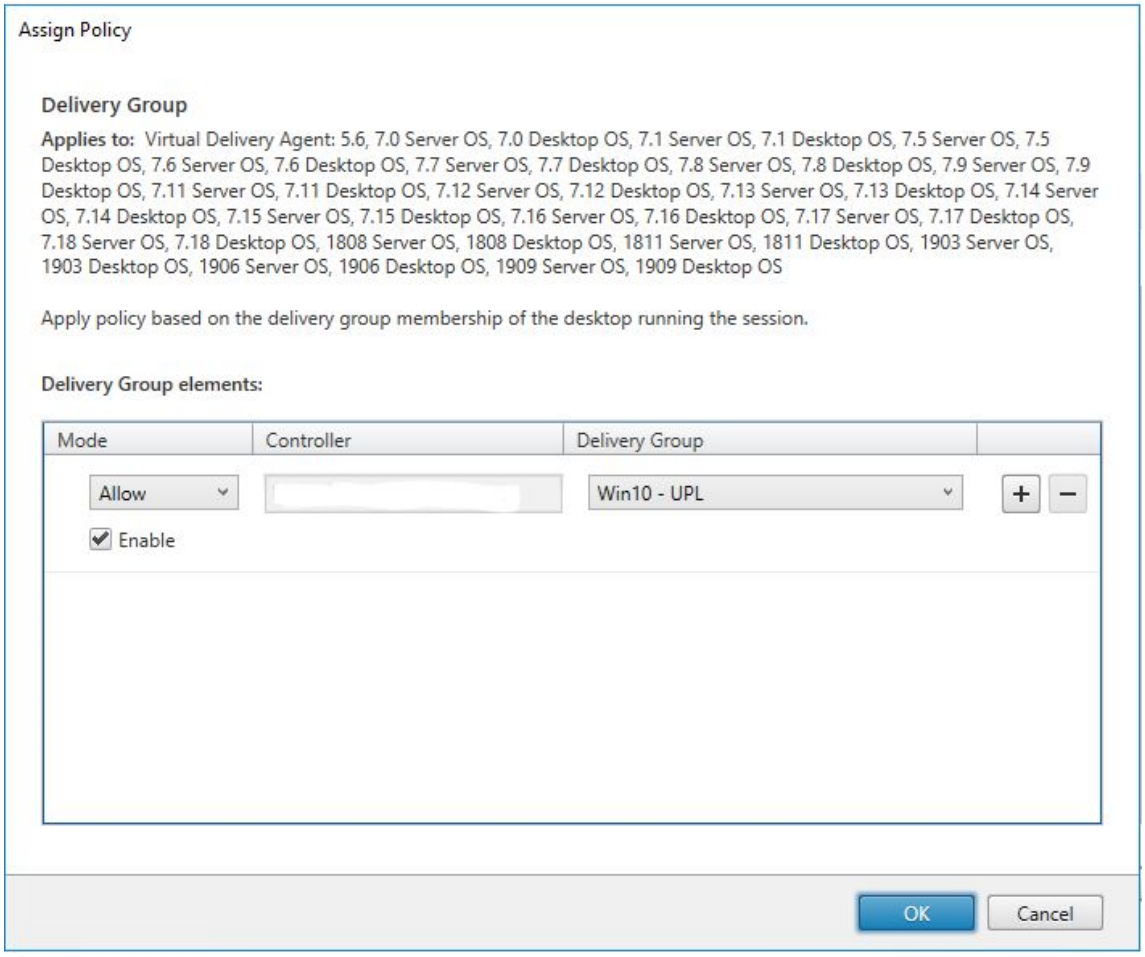
7. Das Fenster “Einstellungen bearbeiten”wird angezeigt.
8. Ändern Sie den Standardwert 0 auf die maximale Größe (in GB), die der Benutzerlayer erreichen darf. Klicken Sie auf OK.

   > **Hinweis:**
   >
   > Wenn Sie den Standardwert beibehalten, beträgt die maximale Benutzerlayergröße 10 GB.

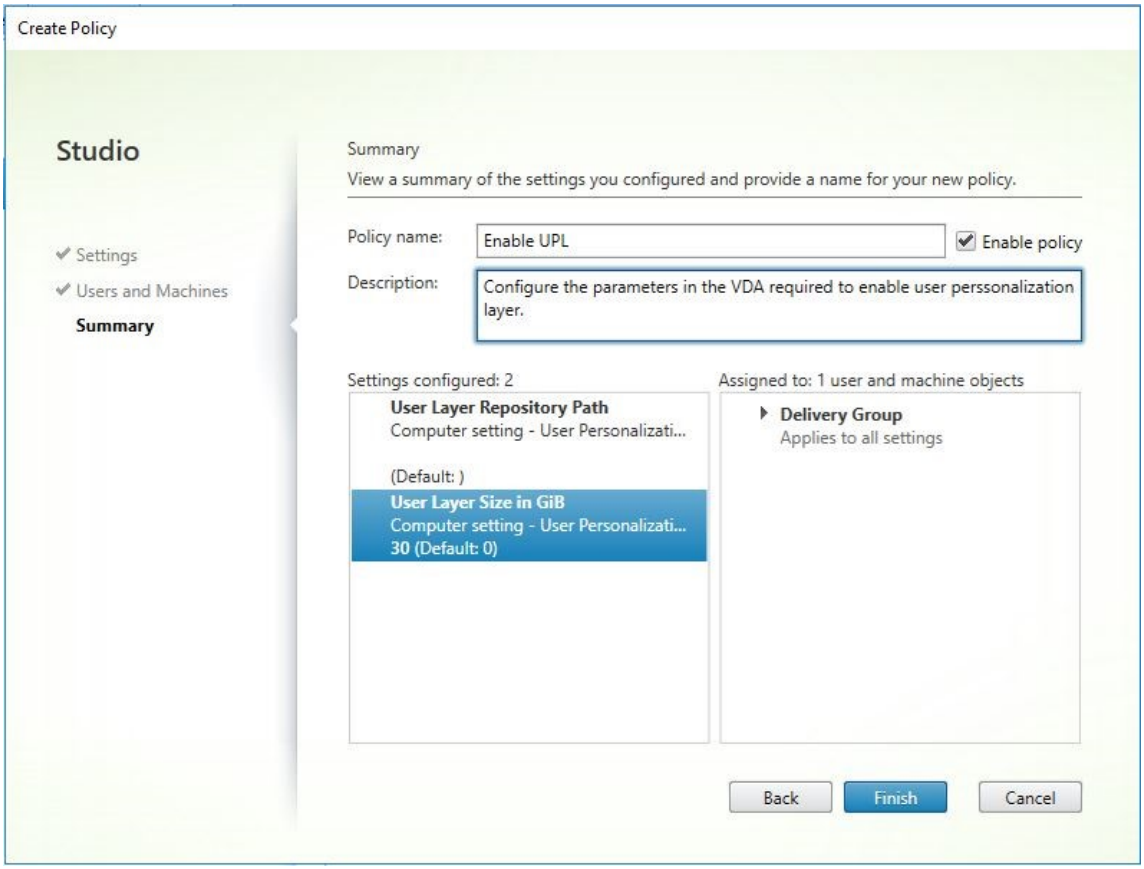
9. Klicken Sie auf Weiter, um Benutzer und Maschinen zu konfigurieren. Klicken Sie neben “Bereitstellungsgruppe”auf den Link “Zuweisen”(im Bild markiert):



10. Wählen Sie im Bereitstellungsgruppenmenü die im vorherigen Abschnitt erstellte Bereitstellungsgruppe aus. Klicken Sie auf OK.



11. Geben Sie einen Namen für die Richtlinie ein. Klicken Sie auf das Kontrollkästchen, um die Richtlinie zu aktivieren, und klicken Sie auf Fertig stellen.



Konfigurieren von Sicherheitseinstellungen im Benutzerlayerordner

Als Domänenadministrator können Sie mehrere Speicherorte für Ihre Benutzerlayer angeben. Erstellen Sie für jeden Speicherort (einschließlich des Standardspeichers) einen Unterordner `\Users` und sichern Sie diesen Speicherort mit folgenden Einstellungen.

Einstellungsname	Wert	Anwenden auf
Ersteller-Besitzer	Ändern	Nur Unterordner und Dateien
Besitzerrechte	Ändern	Nur Unterordner und Dateien
Benutzer oder Gruppe	Ordner erstellen/Daten anhängen; Ordner durchsuchen/Datei ausführen; Ordner auflisten/Daten lesen; Attribute lesen	Nur ausgewählter Ordner
System	Vollzugriff	Ausgewählter Ordner sowie Unterordner und Dateien

Einstellungsname	Wert	Anwenden auf
Domänenadministratoren und ausgewählte Administratorgruppe	Vollzugriff	Ausgewählter Ordner sowie Unterordner und Dateien

Benutzerlayermeldungen

Wenn ein Benutzer auf seinen Benutzerlayer nicht zugreifen kann, erhält er eine der folgenden Benachrichtigungen.

- *Benutzerlayer wird verwendet*

  Wir konnten Ihren Benutzerlayer nicht anhängen, da er bereits verwendet wird. Geänderte Anwendungseinstellungen oder Daten werden nicht gespeichert. Speichern Sie Ihre Arbeit auf einem freigegebenen Netzwerkspeicherort.

- *Benutzerlayer nicht verfügbar*

  Wir konnten Ihren Benutzerlayer nicht anhängen. Geänderte Anwendungseinstellungen oder Daten werden nicht gespeichert. Speichern Sie Ihre Arbeit auf einem freigegebenen Netzwerkspeicherort.

- *System wird nach der Benutzerabmeldung nicht zurückgesetzt*

  Das System wurde nicht ordnungsgemäß heruntergefahren. Melden Sie sich sofort ab und wenden Sie sich an Ihren Systemadministrator.

Protokolldateien für die Fehlerbehebung

Die Protokolldatei ulayersvc.log enthält die Ausgabe der Benutzerpersonalisierungslayer-Software, in der Änderungen erfasst werden.

```
C:\ProgramData\Unidesk\Logs\ulayersvc.log
<!--NeedCopy-->
```

Einschränkungen

Berücksichtigen Sie folgende Einschränkungen bei der Installation und Verwendung des Benutzerpersonalisierung Features.

- Konfigurieren Sie den Benutzerpersonalisierungslayer *nicht* mit persistenten Maschinenkatalogen.

- Verwenden Sie *keine* Sitzungshosts.
- Aktualisieren Sie den Maschinenkatalog *nicht* mit einem Image mit neu installiertem Betriebssystem (gilt auch für dieselbe Version von Windows 10). Es wird empfohlen, Betriebssystemaktualisierungen in dem Masterimage anzuwenden, das beim Erstellen des Maschinenkatalogs verwendet wurde.
- Verwenden Sie *keine* Starttreiber oder anderen Personalisierungen, die am Startbeginn aktiv werden.
- Migrieren Sie *keine* Daten einer persönlichen vDisk auf den Benutzerpersonalisierungslayer.
- Migrieren Sie *keine* vorhandenen Benutzerlayer vom vollständigen App Layering-Produkt auf den Benutzerpersonalisierungslayer.
- Ändern Sie *nicht* den Benutzerlayer-SMB-Pfad, um auf Benutzerlayer zuzugreifen, die mit einem anderen Betriebssystem-Masterimage erstellt wurden.
- Aktivieren Sie *nicht* Secure Boot in virtuellen Maschinen mit Benutzerpersonalisierungslayer. Dies wird derzeit nicht unterstützt.
- Microsoft SCCM Software Center kann eine auf dem Benutzerlayer installierte App als nicht verfügbar anzeigen, obwohl sie zuvor installiert wurde. Das Problem tritt auf, wenn ein Benutzer sich von einer Sitzung abmeldet und auf einer anderen Maschine im Pool erneut anmeldet. Dieses Verhalten basiert auf einer SCCM-Eigenschaft in einer VDI-Umgebung. Das Softwarecenter zeigt nur Anwendungen an, die der Benutzer auf der aktuellen Maschine installiert hat. Die Anwendungen sind jedoch weiterhin installiert und voll funktionsfähig.

  Um die Installation einer Anwendung zu überprüfen, kann der Benutzer die Anwendung im Softwarecenter auswählen und auf **Installieren** klicken. Wenn die Anwendung bereits im Benutzerlayer installiert ist, aktualisiert SCCM den Status auf "Installiert"und listet die App mit den installierten Anwendungen auf.
- Gelegentlich wird das Softwarecenter auf einem VDA mit aktiviertem Benutzerpersonalisierungslayer unmittelbar nach dem Start beendet. Um dieses Problem zu vermeiden, befolgen Sie die Empfehlungen von Microsoft zum Implementieren von SCCM in einer XenDesktop VDI-Umgebung. Stellen Sie auch sicher, dass der ccmexec-Dienst ausgeführt wird, bevor Sie das Softwarecenter starten.
- Gruppenrichtlinien (Computerkonfigurationen): Benutzerlayereinstellungen überschreiben die Einstellungen für das Masterimage. Daher sind die Änderungen, die unter "Computereinstellungen"mit einem Gruppenrichtlinienobjekt vorgenommen werden, bei der nächsten Sitzungsanmeldung nicht immer für den Benutzer vorhanden.

  Um dieses Problem zu umgehen, erstellen Sie ein Benutzeranmeldeskript, das folgenden Befehl ausgibt:


```
gpupdate /force
```

Ein Kunde hat beispielsweise festgelegt, dass folgender Befehl bei jeder Benutzeranmeldung ausgeführt wird:

```
gpudate /Target:Computer /force
```

Optimale Ergebnisse erzielen Sie, wenn Sie Änderungen unter "Computereinstellungen"direkt auf den Benutzerlayer anwenden, nachdem der Benutzer sich angemeldet hat.

Personal vDisk

September 21, 2021

> **Hinweis:**
>
> Persönliche vDisk ist veraltet. Das Benutzerpersonalisierungslayer-Feature behandelt die Benutzerpersistenz.

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.

Neue Features in Personal vDisk 7.6.1

Dieses Release enthält folgende Verbesserungen:

- Diese Version von Personal vDisk enthält Leistungsverbesserungen, durch die die zum Anwenden eines Imageupdates auf einen Personal vDisk-Katalog benötigte Zeit verkürzt wird.

Die folgenden Probleme wurden in diesem Release behoben:

- Bei dem Versuch, eine Basis-VM mit einem direkten Upgrade von Microsoft Office 2010 auf Microsoft Office 2013 zu aktualisieren, wurde dem Benutzer ein Konfigurationsfenster gefolgt von der folgenden Fehlermeldung angezeigt: "Error 25004. The product key you entered cannot be used on this machine."Zuvor wurde in diesem Fall empfohlen, Office 2010 auf der Basis-VM zu deinstallieren und danach Office 2013 zu installieren. Jetzt ist es nicht mehr nötig, Office 2010 beim Durchführen eines direkten Upgrades auf der Basis-VM zu deinstallieren (#391225).
- Wenn während eines Imageupdates eine höhere Version von Microsoft .NET auf der persönlichen vDisk des Benutzers gefunden wurde, wurde diese vom Basisimage mit einer niedrigeren Version überschrieben. Dies führte für Benutzer zu Problemen beim Ausführen bestimmter, auf ihrer persönlichen vDisk installierter Anwendungen, die eine höhere Version, z. B. Visual Studio, benötigten (#439009).
- Ein mit Provisioning Services bereitgestellter Datenträger, auf dem Personal vDisk installiert und aktiviert ist, kann nicht zum Erstellen eines nicht-Personal vDisk-Maschinenkatalogs verwendet werden. Diese Einschränkung wurde entfernt (#485189).

Info zu Personal vDisk 7.6

Neue Features in Version 7.6:

- Verbesserte Fehlerbehandlung und Berichterstellung für Personal vDisk. Wenn Sie in Studio PvD-aktivierte Maschinen in einem Katalog anzeigen, können Sie auf der Registerkarte "PvD" den Überwachungsstatus während Imageupdates sowie die geschätzte Abschlusszeit und den Fortschritt verfolgen. Außerdem wurden die Zustandsanzeigen verbessert.
- Ein Überwachungstool für PvD-Imageupdates ist für frühere Versionen auf dem ISO-Medium verfügbar (ISO\Support\Tools\Scripts\PvdTool). Überwachungsfunktionen wurden auch in früheren Releases unterstützt, jedoch sind die Berichterstellungsfunktionen nicht so robust wie im aktuellen Release.
- Im Provisioning Services-Testmodus können Sie Maschinen mit einem aktualisierten Image in einem Testkatalog starten. Nachdem Sie die Stabilität überprüft haben, können Sie die Testversion der persönlichen vDisk auf "Production"hochstufen.
- Mit einer neuen Funktion können Sie das Delta (die Differenz) zwischen zwei Beständen während einer Bestandsaktualisierung berechnen statt sie für jeden PvD-Desktop einzeln berechnen zu müssen. Es sind neue Befehle zum Exportieren und Importieren eines vorherigen Bestands für MCS-Kataloge verfügbar. (Provisioning Services-Master-vDisks haben bereits den vorherigen Bestand.)

Bekannte Probleme aus Version 7.1.3, die in Version 7.6 behoben wurden:

- Unterbrechen des Upgrades einer Personal vDisk-Installation kann dazu führen, dass eine vorhandene Personal vDisk-Installation beschädigt wird. [#424878]

- Ein virtueller Desktop reagiert möglicherweise nicht mehr, wenn die persönliche vDisk über einen langen Zeitraum ausgeführt wird und es zu einem Speicherverlust im nicht-ausgelagerten Speicher kommt. [#473170]

Neue bekannten Probleme in Version 7.6:

- 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 PROCESS-Ausschlussliste des Antivirenprodukts hinzufügen. Diese Dateien befinden sich im Ordner C:\Programme\Citrix\personal vdisk\bin. [#326735]
- Feste Links zwischen Dateien, die vom Masterimage geerbt wurden, bleiben in persönlichen vDisk-Katalogen nicht erhalten. [#368678]
- Nach dem Upgrade von Office 2010 auf 2013 auf dem Personal vDisk-Masterimage kann Office nicht auf virtuellen Maschinen gestartet werden, da der KMS-Lizenzierungsproduktschlüssel von Office beim Upgrade entfernt wurde. Als Workaround können Sie Office 2010 deinstallieren und Office 2013 auf dem Masterimage neu installieren. [#391225]
- Personal vDisk-Kataloge unterstützen keine VMware Paravirtual SCSI (PVSCSI)-Controller. Verwenden Sie den Standardcontroller, um dieses Problem zu vermeiden. [#394039]
- Für virtuelle Desktops, die mit Personal vDisk Version 5.6.0 erstellt wurden und auf 7 aktualisiert werden, finden Benutzer, die sich an der Master-VM anmelden, nicht alle Dateien in der gepoolten VM. Dieses Problem tritt auf, da ein neues Benutzerprofil erstellt wird, wenn sich Benutzer an der gepoolten VM anmelden. Für dieses Problem gibt es kein Workaround. [#392459]
- Personal vDisks, die unter Windows 7 ausgeführt werden, können das Feature "Sichern und Wiederherstellen"nicht verwenden, wenn der Windows-Systemschutz aktiviert ist. Wenn der Systemschutz deaktiviert ist, wird ein Backup des Benutzerprofils aber nicht der Datei userdata.v2.vhd erstellt. Citrix empfiehlt, den Systemschutz zu deaktivieren und ein Backup des Benutzerprofils mit dem Feature "Sichern und Wiederherstellen"zu erstellen. [#360582]
- Beim Erstellen einer VHD-Datei auf der Basis-VM mit dem Datenträgerverwaltungstool können Sie die virtuelle Festplatte (VHD) möglicherweise nicht bereitstellen. Um dieses Problem zu umgehen, kopieren Sie die VHD auf das PvD-Volume. [#355576]
- Office 2010-Verknüpfungen bleiben auf virtuellen Desktops erhalten, nachdem diese Software entfernt wurde. Um dieses Problem zu umgehen, löschen Sie die Verknüpfungen. [#402889]
- Wenn Sie Microsoft Hyper-V verwenden, können Sie mit Maschinen mit persönlichen vDisks keinen Katalog erstellen, wenn die Maschinen lokal gespeichert sind und die vDisks auf freigegebenen Clustervolumes (CSVs) gespeichert sind. Die Katalogerstellung schlägt fehl und ein Fehler wird angezeigt. Um dieses Problem zu umgehen, verwenden Sie einen anderen Speicherort für die vDisks. [#423969]
- Wenn Sie sich das erste Mal bei einem virtuellen Desktop anmelden, der von einem Provisioning Services-Katalog erstellt wurde, werden Sie aufgefordert, den Desktop neu zu starten, wenn die persönliche vDisk zurückgesetzt wurde (mit dem Befehl "ctxpvd.exe -s reset"). Um dieses

Problem zu lösen, starten Sie den Desktop neu, wenn Sie dazu aufgefordert werden. Es handelt sich hier um eine einmalige Zurücksetzung, die bei erneuter Anmeldung nicht erforderlich ist. [#340186]

- Wenn Sie .NET 4.5 auf einer persönlichen vDisk installieren und .NET 4.0 bei einem späteren Update des Images installiert oder bearbeitet wird, schlagen Anwendungen, die von .NET 4.5 abhängig sind, fehl. Um dieses Problem zu umgehen, stellen Sie .NET 4.5 vom Basisimage aus als Imageupdate bereit.
- Weitere Informationen finden Sie unter Bekannte Probleme in der Dokumentation zu XenApp und XenDesktop 7.6.

Info zu Personal vDisk 7.1.3

Bekannte Probleme aus Version 7.1.1, die in Version 7.1.3 behoben wurden:

- Direkte Upgrades von Personal vDisk 5.6.0 auf Personal vDisk 7.x können zu Fehlern bei Personal vDisk führen. [#432992]
- Benutzer können möglicherweise nur zeitweilig Verbindungen zu virtuellen Desktops mit persönlichen vDisks herstellen. [#437203]
- Wenn das Update eines Personal vDisk-Images während der Aktualisierung von Personal vDisk 5.6.5 oder höher auf Personal vDisk 7.0 oder höher unterbrochen wird, können spätere Updates fehlschlagen. [#436145]

Info zu Personal vDisk 7.1.1

Bekannte Probleme aus Version 7.1, die in Version 7.1.1 behoben wurden:

- Nach der Aktualisierung auf Symantec Endpoint Protection 12.1.3 über ein Imageupdate meldet symhelp.exe beschädigte Antivirus-Definitionen. [#423429]
- Personal vDisk kann den Neustart gepoolter Desktops verursachen, wenn der Dienststeuerungs-Manager (services.exe) abstürzt. [#0365351]

Neue bekannten Probleme in Version 7.1.1: Keine

Info zu Personal vDisk 7.1

Neu in Version 7.1:

- Sie können Personal vDisk nun auch auf Desktops unter Windows 8.1 verwenden und die Ereignisprotokollierung wurde verbessert.

- Copy-on-Write (CoW) wird nicht mehr unterstützt. Beim Upgrade von Personal vDisk Version 7.0 auf 7.1 gehen alle von CoW verwalteten Datenänderungen verloren. CoW war ein Feature, das in XenDesktop 7 bewertet wurde und standardmäßig deaktiviert war. Wenn Sie es nicht aktiviert haben, sind Sie nicht betroffenen.

Bekannte Probleme aus Version 7.0.1, die in Version 7.1 behoben wurden:

- Wenn der Wert des Personal vDisk-Registrierungsschlüssels EnableProfileRedirection auf 1 oder ON eingestellt ist, und Sie den Wert beim Aktualisieren des Images in 0 oder OFF ändern, wird der ganze Personal vDisk-Speicherplatz u. U. den vom Benutzer installierten Anwendungen zugeordnet, sodass kein Platz für Benutzerprofile vorhanden ist, die auf der vDisk bleiben. Wenn die Profilumleitung für einen Katalog deaktiviert ist und Sie die Profilumleitung während eines Imageupdates aktivieren, können sich Benutzer u. U. nicht bei ihren virtuellen Desktops anmelden. [#381921]
- Der Desktopdienst protokolliert nicht den richtigen Fehler in der Ereignisanzeige, wenn das Update des Personal vDisk-Bestands fehlschlägt. [#383331]
- Beim Upgrade auf Personal vDisk 7.x bleiben geänderte Regeln nicht erhalten. Dieses Problem wurde für das Upgrade von Version 7.0 auf Version 7.1 behoben. Beim Upgrade von Version 5.6.5 auf Version 7.1 müssen Sie die Regeldatei zuerst speichern und die Regeln nach dem Upgrade erneut anwenden. [#388664]
- Personal vDisks, die unter Windows 8 ausgeführt werden, können keine Anwendungen vom Windows Store installieren. Eine Fehlermeldung gibt an, dass der Kauf nicht abgeschlossen werden konnte. Wenn Sie den Windows Update-Dienst aktivieren, wird das Problem nun behoben. Von Benutzern installierte Anwendungen müssen jedoch nach dem Neustart des Systems neu installiert werden. [#361513]
- Einige symbolische Verknüpfungen fehlen auf gepoolten Windows 7-Desktops mit persönlichen vDisks. Daher werden Symbole, die von Anwendungen unter C:\Benutzer\Alle Benutzer gespeichert werden, nicht im Startmenü angezeigt. [#418710]
- Der Start einer persönlichen vDisk schlägt fehl, wenn ein USN-Journalüberlauf aufgrund zahlreicher Systemänderungen nach einer Bestandsaktualisierung auftritt. [#369846]
- Der Start einer persönlichen vDisk schlägt fehl und der Statuscode 0x20 sowie Fehlercode 0x20000028 werden angezeigt. [#393627]
- Symantec Endpoint Protection 12.1.3 zeigt die Fehlermeldung “Proactive Threat Protection is malfunctioning”an und der Liveupdatestatus dieser Komponente ist nicht verfügbar. [#390204]

Neue bekannte Probleme in Version 7.1: siehe die Dokumentation zu bekannten Problemen in XenDesktop 7.1.

Info zu Personal vDisk 7.0.1

Neu in Version 7.0.1: Personal vDisk ist jetzt robuster bei Änderungen der Umgebung. Virtuelle Desktops mit persönlichen vDisks werden jetzt beim Delivery Controller registriert, selbst wenn das Imageupdate fehlschlägt, und das Herunterfahren von unsicheren Systemen setzt die vDisks in einen permanent deaktivierten Zustand. Darüber hinaus können Sie nun während einer Bereitstellung Dateien und Ordner mit Regeldateien von vDisks ausschließen.

Bekannte Probleme aus Version 5.6.13, die in Version 7.0.1 behoben wurden:

- Änderungen an der Mitgliedschaft einer Gruppe, die von einem Benutzer an einem gepoolten virtuellen Desktop vorgenommen wurden, gehen u. U. nach einem Imageupdate verloren. [#286227]
- Imageupdates schlagen u. U. mit einer Fehlermeldung fehl, dass der Speicherplatz auf dem Datenträger niedrig ist, selbst wenn die persönliche vDisk genug Speicherplatz hat. [#325125]
- Die Installation einiger Anwendungen schlägt auf virtuellen Desktops mit einer persönlichen vDisk fehl, und eine Meldung weist auf einen erforderlichen Neustart hin. Grund ist eine ausstehende Umbenennung. [#351520]
- Symbolische Links, die im Masterimage erstellt wurden, funktionieren nicht auf virtuellen Desktops mit persönlichen vDisks. [#352585]
- In Umgebungen mit der Citrix Profilverwaltung und Personal vDisk funktionieren Anwendungen, die Benutzerprofile auf einem Systemvolume überprüfen u. U. nicht richtig, wenn die Profilumleitung aktiviert ist. [#353661]
- Die Bestandsaktualisierung schlägt auf Masterimages fehl, wenn der Bestand größer als 2 GB ist. [#359768]
- Imageupdates schlagen mit einem Fehlercode 112 fehl und persönliche vDisks sind beschädigt, selbst wenn die vDisks ausreichend Speicherplatz für das Update haben. [#363003]
- Das Skript für das Ändern der Größe schlägt für Kataloge fehl, die mehr als 250 Desktops haben. [#363365]
- Benutzerseitige Änderungen einer Umgebungsvariablen gehen bei einer Aktualisierung des Images verloren. [#372295]
- Lokale Benutzer, die auf einem virtuellen Desktop mit einer persönlichen vDisk erstellt wurden, gehen bei einer Aktualisierung des Images verloren. [#377964]
- Der Start einer persönlichen vDisk schlägt u. U. fehl, wenn ein USN-Journalüberlauf aufgrund zahlreicher Systemänderungen nach einer Bestandsaktualisierung auftritt. Erhöhen Sie die USN-Journalgröße im Masterimage auf mindestens 32 MB und aktualisieren Sie das Image, um dieses Problem zu vermeiden. [#369846]
- Ein Problem wurde mit Personal vDisk festgestellt, das ein richtiges Funktionieren der Registrierungsstrukturaktionen des AppSense-Umgebungs-Managers verhindert, wenn AppSense im Ersetzenmodus verwendet wird. Citrix und AppSense arbeiten an der Behebung des Problems, das mit dem Verhalten der RegRestoreKey-API zusammenhängt, wenn Personal

vDisk installiert ist. [#0353936]

Release-unabhängige bekannte Probleme

- Wenn Windows Store- und Metro-Apps auf dem Masterimage aktualisiert werden, kann dies zu Konflikten bei PvD-aktivierten Zielgeräten nach dem Upgrade der persönlichen vDisk auf Test oder Produktion führen. Außerdem können Metro-Apps möglicherweise nicht gestartet werden, wobei Fehler im Anwendungsereignisprotokoll verzeichnet werden. Citrix empfiehlt, Windows Store- und Metro-Apps für PvD-aktivierte Zielgeräte deaktivieren.
- 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 Masterimage 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]

Installation und Upgrade

March 9, 2022

Personal vDisk 7.x wird von der aktuellen Version von Citrix Virtual Apps and Desktops (und früheren Versionen ab XenDesktop 5.6) unterstützt. Für jede Version werden in der Dokumentation unter "Systemanforderungen"die unterstützten Betriebssysteme für Virtual Delivery Agents (VDAs) sowie die unterstützten Versionen von Hosts (Virtualisierungsressourcen) und Citrix Provisioning (zuvor "Provisioning Services") aufgelistet. Weitere Informationen zu Citrix Provisioning-Aufgaben finden Sie in der aktuellen Dokumentation.

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 Citrix Virtual Apps and Desktops-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 Citrix Provisioning 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 Citrix Virtual Desktops-Version. Nehmen Sie anschließend den PvD-Bestand auf.

Deinstallieren von PvD

Sie können die PvD-Software mit einer der folgenden beiden Methoden deinstallieren:

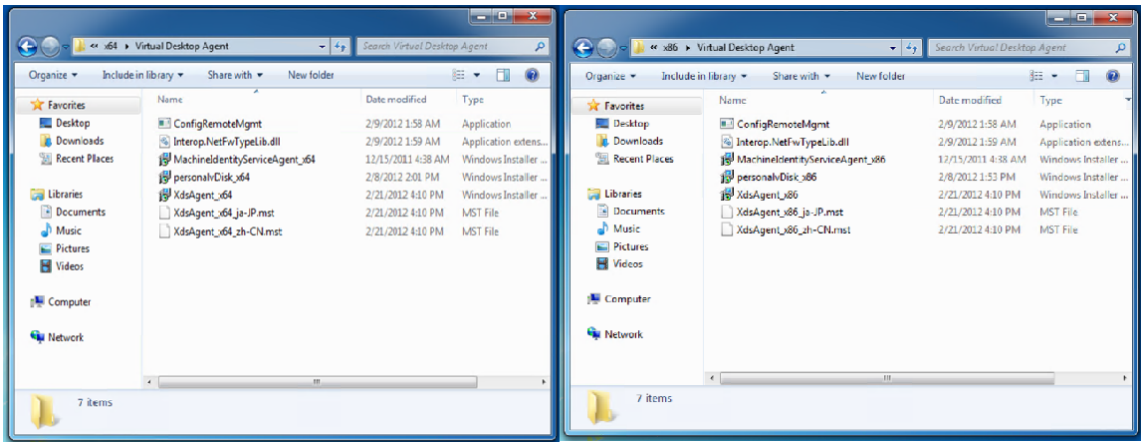
- Deinstallieren Sie den VDA. Dabei wird die PvD-Software ebenfalls entfernt.
- Wenn Sie PvD mit der PvD-MSI aktualisiert haben, können Sie es über die Liste der Programme deinstallieren.

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.

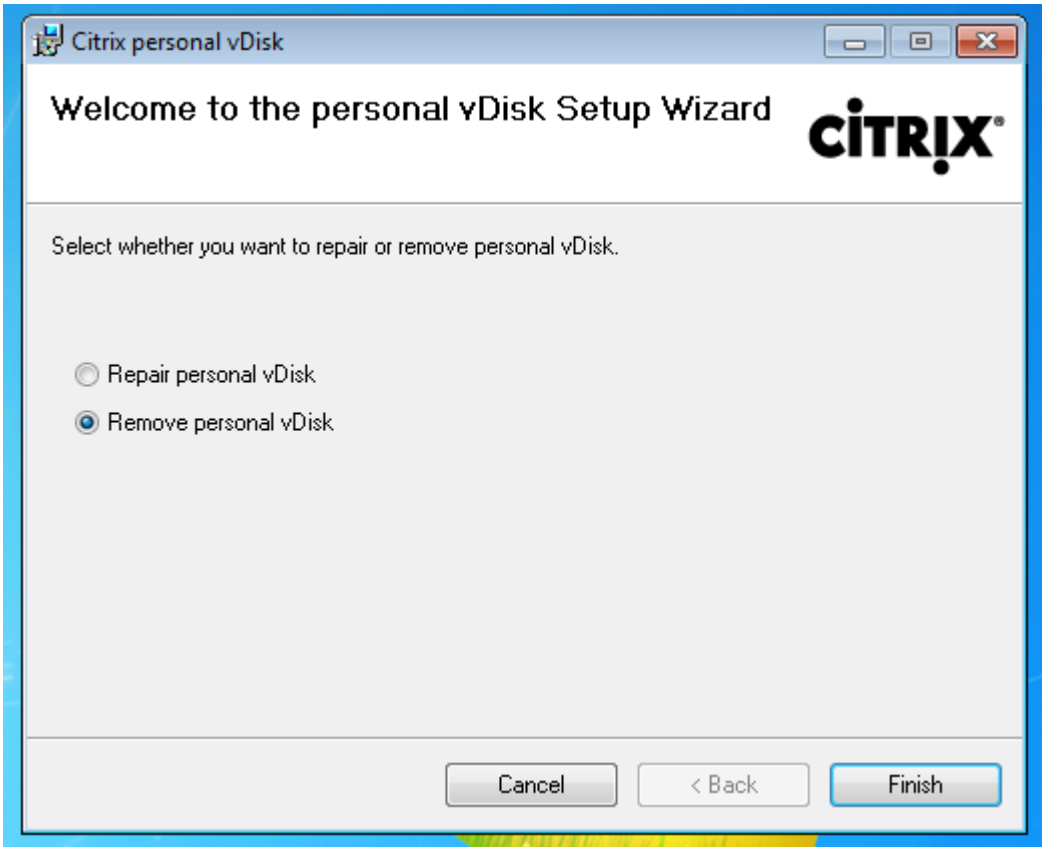
Die Deinstallation kann fehlschlagen, wenn eine persönliche vDisk mit Windows 7 (64 Bit) im Basisimage installiert ist. Um dieses Problem zu beheben, empfiehlt Citrix, die persönliche vDisk vor der Aktualisierung zu entfernen.

1. Wählen Sie die geeignete Kopie des vDisk-Installationsprogramms unter den Citrix Virtual Apps and Desktops-Medien. Suchen Sie die aktuelle Version des MSI-Installationspakets für Personal vDisk in einem der folgenden Verzeichnisse (je nachdem, ob die aktualisierte VM ein 32- oder 64-Bit-System ist):

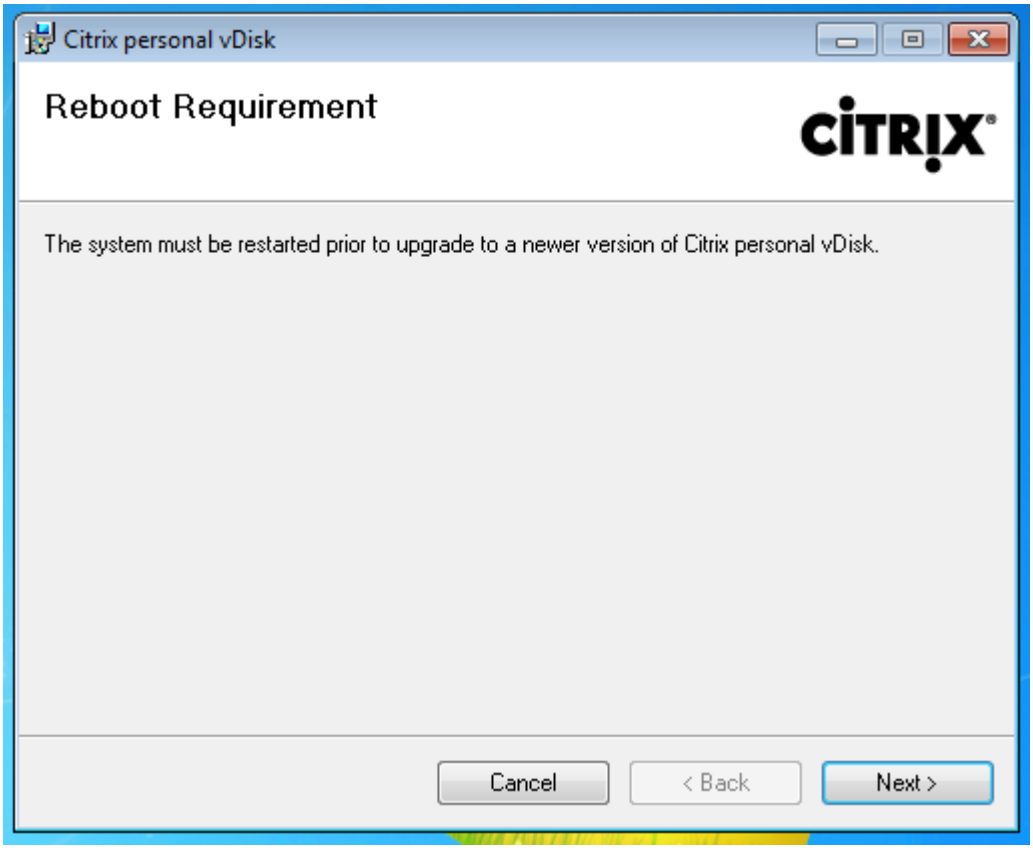
    - 32-Bit: XA and XD\x86\Virtual Desktop Components\personalvDisk_x86.msi
    - 64-Bit: XA and XD\x64\Virtual Desktop Components\personalvDisk_x64.msi



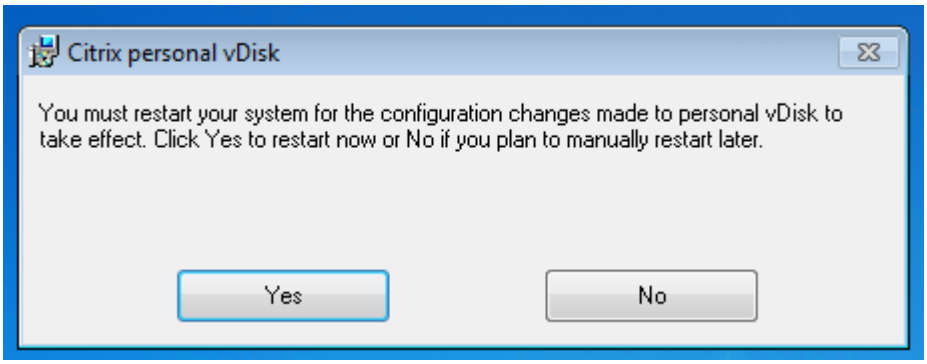
2. Entfernen Sie die installierte persönliche vDisk. Wählen Sie das MSI-Installationspaket für Personal vDisk, das in Schritt 1 gefunden wurde. Der Setupbildschirm für Personal vDisk wird angezeigt.
3. Wählen Sie **Personal vDisk entfernen**.
4. Klicken Sie auf **Fertig stellen**.



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

March 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-Poolstatistikskript (auf dem Citrix Virtual Apps and Desktops-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 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. Spätere Versionen verwenden dafür die delegierte Administration.

Weitere Einstellungen:

- **Windows Update-Dienst:** Stellen Sie sicher, dass im Masterimage für Windows Updates die Einstellung "Never Check for Updates"und für den Windows Update-Dienst die Einstellung "Disabled"ausgewählt ist. Außerdem empfiehlt Citrix, dass Sie Updates und Features von Windows Store- und Metro-Apps deaktivieren.
- **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 Workspace-App)
- 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 Citrix Provisioning

Wenn Sie Citrix Provisioning 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 Citrix Provisioning-vDisk auf "Production"hochgestuft wird.
- Das Versionsverwaltungsfeature von Citrix Provisioning 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 Citrix Provisioning-Schreibcachedatenträger sein, da Citrix Provisioning sonst fälschlicherweise die persönliche vDisk als Schreibcache nehmen könnte.
- Nach dem Erstellen einer Bereitstellungsgruppe können Sie die persönliche vDisk mit dem resize- und dem poolstats-Skript (`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 Citrix Provisioning-Schreibcache verringern. Wenn PvD jedoch nicht aktiv ist, z. B. während Imageupdatevorgängen, kann ein kleiner Citrix Provisioning-Schreibcache schnell voll sein und den Absturz von Maschinen verursachen.

Citrix empfiehlt, dass Sie die Größe des Citrix Provisioning-Schreibcache entsprechend den Empfehlungen für Citrix Provisioning 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 Citrix Provisioning einen Katalog mit PvD-aktivierten Maschinen bereitstellen:

- Folgen Sie den Anweisungen in der Dokumentation zu Citrix Provisioning.
- Sie können die Drosselungseinstellungen für Energieaktionen ändern, indem Sie die Verbindung in Studio bearbeiten.
- Zum Aktualisieren der Citrix Provisioning-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 Citrix Provisioning 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 Produktdokumentation.
- 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 resize- und dem poolstats-Skript (`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".
- Die gleichzeitige Auswahl von PVD und MCS-E/A-Caching ist nicht möglich. Wenn Sie PVD installieren, können Sie keinen Katalog mit aktiviertem MCS-E/A-Caching erstellen.

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:** Die 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

September 21, 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 Citrix Virtual Apps and Desktops-Installationsmedium.

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.

- 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:

```
1  C:\Program Files\Citrix\personal vDisk\bin> .\CtxPvDSvc.exe
       exportinventory
2  \share location\ExportedInventory
3  Current inventory source location C:\CitrixPvD\Settings\Inventory
       \VER-LAS
4  ...
5  Exporting current inventory to location \ ….
```



```
6  ...
7  Deleting any pre-existing inventory folder at \ ....
8  .Successfully exported current inventory to location \ ....  Error
      code = OPS
9  <!--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>"
```

<path to exported inventory> muss der vollständige Pfad für die Bestandsdateien sein; in der Regel ist das <network location\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:

```
1  C:\Program Files\Citrix\personal vDisk\bin> .\CtxPvDSvc.exe
      importinventory
2  \share location\ExportedInventory\ExportedPvdInventory
3  Importing inventory \share location\ExportedInventory\
      ExportedPvdInventory
4  ...
5  Successfully added inventory \share location\ExportedInventory\
      ExportedPvdInventory to the
6  store at c:\ProgramData\Citrix\personal vDisk\InventoryStore
7  <!--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

February 6, 2020

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:\\Program Files\\Citrix\\personal vDisk\\bin\\CtxPvdDiag.exe` 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 zwei 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 in "UserData.V2.vhd"unter "\ProgramData\CitrixPvD\Settings\Inventory\
  LAST"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 tritt häufig auf, weil Software 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 Desk-

top 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.

Fehlercode	Beschreibung
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.
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.

Ereignis-ID	Beschreibung
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.

Migrieren von PvD zu App Layering

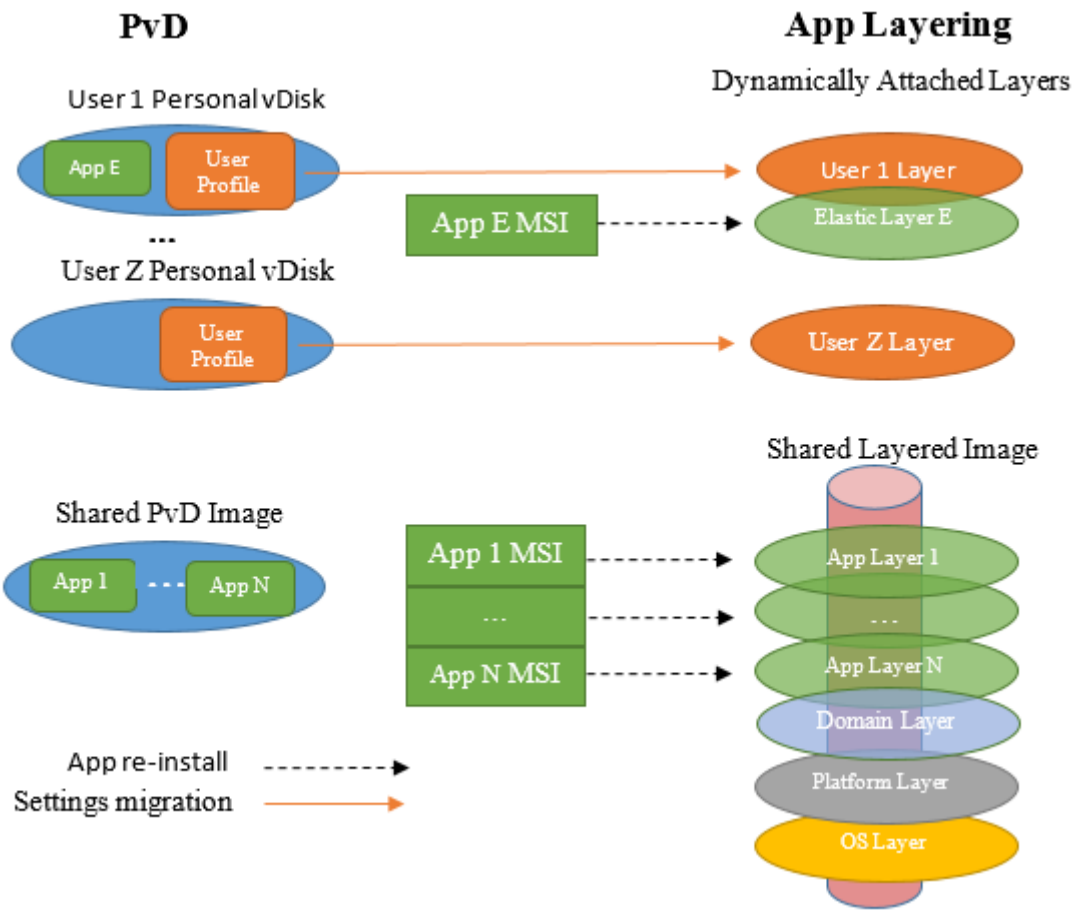
September 21, 2021

Citrix ersetzt PvD (persönliche vDisk) durch die Citrix App Layering-Technologie. Anhand der Informationen in diesem Artikel können Sie eine App Layering-VM erstellen, die funktionell einer PvD-basierten VM entspricht.

Informationen zu Layern und zum Erstellen und Veröffentlichen von Imagevorlagen finden Sie in der Dokumentation zu Citrix App Layering.

Eine PvD-VM besteht in der Regel aus einem freigegebenen Image und einer persönlichen vDisk. Das freigegebene Image wird an mehrere Benutzer verteilt, von denen jeder seine eigene persönliche vDisk hat. Eine App Layering-VM besteht in der Regel aus mehreren Layern, einschließlich Betriebssystem-, Plattform- und einem oder mehreren Anwendungslayern. Die VM wird von mehreren Benutzern genutzt, von denen jeder seinen eigenen Benutzerlayer hat.

Bei der Migration einer Gruppe von Benutzern, die sich eine PvD-Image-VM teilen, wird eine funktional gleichwertige App Layering-VM mit freigegebenem Image erstellt. Das Profil und die Einstellungen der einzelnen Benutzer werden von deren persönlicher vDisk in ihren jeweiligen App Layering-Benutzerlayer migriert:



Der Ansatz zur Migration der persönlichen Daten eines Benutzers im vorliegenden Artikel unterscheidet sich von dem zur Anwendungsmigration. Für persönliche Daten werden Tools zum Kopieren von einer persönlichen vDisk zu einem Benutzerlayer empfohlen. Für Anwendungen wird das Kopieren nicht empfohlen. Stattdessen wird die Neuinstallation persönlicher Daten in einem App-Layer empfohlen. Darüber hinaus wird von Folgendem ausgegangen:

- Auf der PvD-VM wird Windows 7 ausgeführt. Die Migration ist bei anderen Betriebssystemversionen, sofern sie von App Layering unterstützt werden, ähnlich. App Layering unterstützt beispielsweise Windows XP nicht.
- Als Hypervisor wird Citrix Hypervisor verwendet und Sie sind mit dessen Verwaltung über XenCenter vertraut.
- Für die Bereitstellung wird Maschinenerstellungsdienste (MCS) oder Citrix Provisioning (zuvor "Provisioning Services") verwendet. Für MCS bzw. Citrix Provisioning benötigen Sie das Cit-

rix Virtual Apps and Desktops-ISO. Für Citrix Provisioning benötigen Sie das ProvisioningServicesxxx.iso.
- Citrix Virtual Desktops wird zum Verwalten der generierten App Layering-VMs verwendet.

Bei Verwendung eines anderen Hypervisors oder Bereitstellungsdiensts gelten ähnliche Verfahren wie hier beschrieben.

Bei den Beispielen in diesem Artikel wird davon ausgegangen, dass der Benutzer Mitglied einer Active Directory-Domäne ist.

PvD und App Layering im Vergleich

App Layering fördert die saubere Trennung von Anwendungen und benutzerspezifischen Informationen. Anwendungen befinden sich in App-Layern (oft eine App pro Layer) und benutzerspezifische Informationen in einem Benutzerlayer. Als bewährte Methode würde ein Benutzer eine Anwendung nicht in seinem Benutzerlayer installieren, wenn er davon ausgeht, dass sie für die Allgemeinheit nützlich ist. Stattdessen würde er sie in einem elastischen App-Layer installieren, der dynamisch an die VMs von Benutzern bei deren Anmeldung angefügt wird.

PvD unterstützt diese saubere Trennung nicht, da es nur zwei Ebenen gibt: das freigegebene, von mehreren Benutzern gemeinsam genutzte Image und eine benutzerspezifische vDisk. Die Benutzer installieren hier häufig eine Anwendung in ihrer persönlichen vDisk, wenn sie im freigegebenen Image nicht verfügbar ist.

Für die Migration eines freigegebenen PvD-Images in App Layering müssen Sie ermitteln, welche Anwendungen das Image enthält. Für jede Anwendung (bzw. jede Gruppe verwandter Anwendungen) erstellen Sie einen App-Layer. Beachten Sie Folgendes:

- Wenn die Anwendung allgemeinen Nutzen hat, fügen Sie den App-Layer einer Imagevorlage an, die dann in einem Layerimage veröffentlicht wird.
- Ist die Anwendung für eine kleinere Benutzergruppe geeignet, weisen Sie sie dieser Gruppe zu. Wenn sich Mitglieder dieser Gruppe dann bei der VM anmelden, wird sie dynamisch als elastischer App-Layer angefügt.
- Wenn eine Anwendung nur für einen Benutzer geeignet ist, installieren Sie sie in dessen Benutzerlayer.

Artefakte beim App Layering

Beim Erstellen einer App Layering-VM werden diverse App Layering-spezifische Artefakte erstellt, darunter Verpackungs-VMs, Connectors, Agents und VM-Vorlagen. Diese Elemente gibt es nur beim App Layering. Sie werden nachfolgend kurz beschrieben. Ausführliche Beschreibungen finden Sie in der App Layering-Dokumentation.

Verpackungs-VMs

Die App Layering-Methode zum Anpassen des Inhalts von Plattformlayern und App-Layern besteht in der Erstellung einer *Packaging-VM* (oder auch *Installationsmaschine*). Das Erstellen eines Layers erfolgt in sechs Schritten:

1. In Enterprise Layer Manager (ELM) erstellen Sie den Layer und geben dessen Namen sowie andere Informationen an.
2. ELM generiert eine Packaging-VM und kopiert sie (normalerweise) auf den Hypervisor.
3. Sie starten die Packaging-VM über den Hypervisor und passen sie an.
4. Wenn Sie fertig sind, klicken Sie auf das Symbol **Shutdown to Finalize** auf dem Desktop der Packaging-VM. Es erfolgt nun eine Layer-Integritätsprüfung, die sicherstellt, dass keine Neustarts anstehen und dass ngen nicht ausgeführt wird. Der Abschluss erfolgt erst, wenn diese Tasks abgeschlossen sind.
5. In ELM klicken Sie dann auf die Aktion **Finalize**.
6. ELM schließt die Erstellung des Layers basierend auf Ihrer angepassten Packaging-VM ab und löscht dann die Packaging-VM.

Beim App Layering wird zum Erstellen des Betriebssystemlayers keine Packaging-VM verwendet. Stattdessen erstellen Sie eine VM und passen sie nach Bedarf an. Die VM wird dann in ELM importiert.

Connectors und Agents

ELM kommuniziert mit mehreren Entitäten (Hypervisors, Dateifreigaben und Provisioningtools). Es erstellt VMs, führt weitere Aufgaben an den Entitäten aus und kopiert verschiedene Arten von Daten (z. B. VHDs und Dateien) zu oder von den Entitäten.

Ein Connector ist ein Objekt, das ELM für die Kommunikation mit einer anderen Entität zur Ausführung von Aufgaben verwendet. Seine Konfiguration enthält den Namen oder die IP-Adresse der Entität, die Anmeldeinformationen für den Zugriff auf die Entität und alle anderen zur Ausführung der Aufgaben erforderlichen Informationen. Beispiel: ein Dateipfad in der Entität, an dem Daten gelesen oder geschrieben werden.

Folgende Elemente erstellen Connectors:

- Citrix Hypervisor-Connector: ELM verwendet den Connector zum Erstellen und Löschen von VMs (z. B. Packaging-VMs) auf dem bzw. vom Citrix Hypervisor.
- Netzwerkdateifreigabe-Connector: Dieser Connector wird auf der Registerkarte “System” auf der Unterregisterkarte “Settings and Configurations”im Abschnitt “Network File Share” konfiguriert. ELM und VMs verwenden den Prozess zum Erstellen von Dateien in einer Netzwerkdateifreigabe.

- Citrix MCS für Citrix Hypervisor-Connector: Wenn Sie MCS als Provisioningdienst verwenden, wird dieser Connector erstellt. ELM verwendet ihn, um Layerimages auf Citrix Hypervisor zu kopieren, nachdem Treiber entfernt wurden, die von MCS nicht benötigt werden.
- Citrix Provisioning Connector: Wenn Sie Citrix Provisioning als Provisioningdienst verwenden, erstellen Sie diesen Connector. ELM verwendet ihn zum Kopieren der Layerimage-VHD auf den Citrix Provisioning-Server. Es wird dort eine vDisk erstellt, nachdem nicht von Citrix Provisioning benötigte Treiber entfernt wurden.

VM-Vorlage

Wenn Sie Citrix Hypervisor als Hypervisor verwenden, wird basierend auf Ihrer Betriebssystemlayer-VM eine VM-Vorlage erstellt. Diese Vorlage enthält Informationen zum Betriebssystem, z. B. Netzwerkschnittstellen und die Zahl der Prozessoren. Sie wird nach dem Betriebssystemlayer erstellt. Sie wird bei der Erstellung eines Citrix Hypervisor-Connectors verwendet.

Installation des Unidesk-Agents auf dem Citrix Provisioning-Server

Wenn Sie Citrix Provisioning bereitstellen, müssen Sie den Unidesk-Agent auf dem Citrix Provisioning-Server installieren. Dadurch kann ELM Befehle auf dem Citrix Provisioning-Server ausführen.

Informationen hierzu finden Sie unter “Install the App Layering Agent (required for Citrix Provisioning and Connector Scripts)”in der App Layering-Dokumentation.

Migration freigegebener Images

Zur Migration eines freigegebenen Images in App Layering erstellen Sie ein freigegebenes Layerimage, das funktional dem PvD-Image entspricht. Das freigegebene Layerimage wird durch Veröffentlichung einer Imagevorlage erstellt. Für die Imagevorlage erstellen Sie einen Betriebssystemlayer, einen Plattformlayer und mindestens einen App-Layer. Die entsprechenden Verfahren werden nachfolgend beschrieben.

Betriebssystemlayer

Gehen Sie zum Erstellen des Betriebssystemlayers wie nachfolgend beschrieben vor.

In XenCenter:

Erstellen Sie eine VM in Citrix Hypervisor. Diese bildet die Grundlage für den Betriebssystemlayer und die VM-Vorlage.

Die Betriebssystemversion der VM muss mit der des freigegebenen PvD-Images, das Sie migrieren, übereinstimmen. In diesen Anweisungen wird davon ausgegangen, dass Sie Windows 7 ausführen.

Auf der Betriebssystemlayer-VM:

Melden Sie sich mit dem lokalen Administratorkonto an.

Installieren Sie alle ausstehenden Windows-Updates.

Treffen Sie die in der App Layering-Dokumentation unter "Prepare a Windows 7 image"aufgeführten Vorbereitungen.

In XenCenter:

Erstellen Sie eine Kopie der Betriebssystemlayer-VM. Löschen Sie jeglichen lokalen Speicher. Konvertieren Sie die VM in eine Vorlage. Die VM-Vorlage verwenden Sie beim Erstellen eines Citrix Hypervisor-Connectors.

In ELM:

Klicken Sie auf der Registerkarte **Layers** auf **Create OS Layer**.

Wenn Sie Citrix Hypervisor verwenden und noch keinen Citrix Hypervisor-Connector erstellt haben, tun Sie dies jetzt. Geben Sie für "Virtual Machine Template"die zuvor erstellte VM-Vorlage an.

Wählen Sie für "Select Virtual Machine"die Betriebssystemlayer-VM aus.

Nachdem Sie ein Symbol zugewiesen und ggf. weitere Detailinformationen angegeben haben, klicken Sie auf "Create Layer". Dadurch wird die Betriebssystemlayer-VM in den ELM-Speicher kopiert und der Betriebssystemlayer wird generiert.

Der Betriebssystemlayer ist damit erstellt und kann bereitgestellt werden.

Plattformlayer

Nach Erstellung des Betriebssystemlayers können Sie mit dem Erstellen eines Plattformlayers für das freigegebene Image fortfahren.

Ein Schritt beim Einrichten des Plattformlayers besteht im Beitritt zur Active Directory-Domäne der Benutzer. Sind die Benutzer Mitglied mehrerer Domänen, müssen Sie für jede Domäne einen eigenen Plattformlayer erstellen. In diesem Artikel wird davon ausgegangen, dass alle Benutzer Mitglied einer Einzeldomäne sind.

In ELM:

1. Klicken Sie auf der Registerkarte **Layers** auf **Create Platform Layer**.
2. Wählen Sie im Fenster "OS Layers"den zuvor erstellten Betriebssystemlayer aus.

3. Wählen Sie im Fenster "Connector"den zuvor erstellten Citrix Hypervisor-Connector aus. ELM verwendet diese Informationen beim Schreiben der Packaging-VM für den Plattformlayer in Citrix Hypervisor.
4. Wählen Sie im Fenster "Platform Types"die Option "This platform will be used for publishing Layered Images".
5. Wählen Sie den Hypervisor aus. In diesem Artikel wird davon ausgegangen, dass Sie Citrix Hypervisor verwenden.
6. Wählen Sie den Provisioningdienst aus. Es wird davon ausgegangen, dass Sie Citrix MCS oder Citrix PVS (mit Citrix Provisioning) verwenden.
7. Wählen Sie für "Connection Broker""Citrix XenDesktop".

Nachdem Sie ein Symbol zugewiesen und ggf. weitere Detailinformationen angegeben haben, klicken Sie auf **Create Layer**. Dadurch wird eine Packaging-VM für den Plattformlayer erstellt. Nach Abschluss des Vorgangs wird die Statusangabe "Action Required"angezeigt.

In XenCenter:

Wenn die Packaging-VM für den Plattformlayer erstellt ist, wird sie in XenCenter angezeigt. Führen Sie folgende Schritte aus:

1. Starten Sie die VM.
2. Melden Sie sich auf der Packaging-VM für den Plattformlayer mit dem lokalen Administratorkonto an.
3. Wenn Sie dazu aufgefordert werden, führen Sie einen Neustart aus und melden Sie sich erneut an.
4. Verbinden Sie die Active Directory-Domäne der Benutzer wie gewohnt. **Systemsteuerung** > **System> Einstellungen ändern > Ändern**. Starten Sie die Maschine neu und melden Sie sich mit dem lokalen Administratorkonto an.

Installieren Sie den Citrix Virtual Delivery Agent (VDA):

1. Stellen Sie das Citrix Virtual Apps and Desktops-ISO bereit.
2. Führen Sie AutoSelect.exe aus, wenn kein automatischer Start stattfindet.
3. Klicken Sie neben Citrix Virtual Desktops auf **Start**.
4. Klicken Sie auf **Virtual Delivery Agent for Desktop OS**.

   Wählen Sie mit folgenden Ausnahmen die Standardeinstellungen in den folgenden Dialogfeldern aus. Allerdings:

   - Sie können Ihren Delivery Controller angeben, wenn Sie dazu aufgefordert werden, oder "Später (erweitert)"auswählen.
   - Stellen Sie sicher, dass "Persönliche vDisk"nicht ausgewählt ist.

   Wenn der VDA installiert ist, wird die Packaging-VM für den Plattformlayer neu gestartet.

Melden Sie sich erneut an.

Wenn Sie Citrix Provisioning als Provisioningdienst verwenden, müssen Sie die Zielgerätesoftware installieren. Gehen Sie dazu folgendermaßen vor:

1. Stellen Sie ProvisionServicesxxx.iso bereit.
2. Führen Sie AutoSelect.exe aus, wenn kein automatischer Start stattfindet.
3. Klicken Sie auf "Target Device Installation".
4. Klicken Sie erneut auf "Target Device Installation", um den Installationsassistenten zu starten. Das Installationsprogramm installiert Citrix Diagnostic Facility (CDF) und die Citrix Provisioning Services-Zielgerätesoftware.
5. In den folgenden Dialogfeldern wählen Sie in der Regel die Standardeinstellungen aus.
6. Deaktivieren Sie zum Abschluss der Installation "Launch Imaging Wizard"und klicken Sie auf "Finish".
7. Warten Sie den Neustart der VM ab und melden Sie sich an.
8. Führen Sie das Hilfsprogramm Citrix Provisioning Optimizer aus.

Nach Installation und Anpassung der plattformbezogenen Software klicken Sie auf das Desktop-Symbol "Shutdown to Finalize".

In ELM:

Wählen Sie das Symbol für den Plattformlayer aus (der Status müsste "Editing"lauten) und klicken Sie auf **Finalize**.

App-Layer

Nach Erstellung des Betriebssystemlayers können Sie mit dem Erstellen von App-Layern aus dem freigegebenen PvD-Image fortfahren. Ermitteln Sie, welche Anwendungen im freigegebenen PvD-Image installiert sind. Dazu gibt es mehrere Möglichkeiten:

- Wenn Sie eine startbare Version des freigegebenen PvD-Images haben, starten Sie diese und wählen Sie in der Systemsteuerung "Programme und Features".
- Erstellen Sie andernfalls über Citrix Virtual Desktops mit dem freigegebenen PvD-Image eine PvD-VM für einen Pseudobenutzer. Da die persönliche vDisk des Pseudobenutzers leer ist, sind alle unter "Programme und Features"angezeigten Anwendungen auf dem freigegebenen PvD-Image installiert.

Ermitteln Sie über **Programme und Features** die Liste der erforderlichen Anwendungen.

Alternativ können Sie das unter "Migrationstools"beschriebene Programm PCmover verwenden. Dieses stellt eine gute Möglichkeit zur Ermittlung der Anwendungen auf einem Computer dar. Es erkennt ad hoc installierte Programme, die nicht unter "Programme und Features"aufgeführt

werden. Bei Verwendung des Programms zu diesem Zweck lassen Sie die Analyse ohne tatsächliche Übertragungen durchführen. Wenn Sie nach Abschluss der Analyse alle Anwendungen des freigegebenen Images notiert haben, können Sie PCmover einfach mit "Abbrechen"schließen. Weitere Informationen finden Sie weiter unten im Abschnitt **Ermitteln erforderlicher Anwendungen mit PCmover**.

> **Tipp:**
>
> Wenn Sie mehrere PvD-VMs migrieren, wäre nun ein guter Zeitpunkt, jede zu starten, um eine Liste der von den Benutzern installierten Anwendungen aufzustellen. Alle Anwendungen, die Sie über die im freigegebenen Image gefundenen Anwendungen hinaus finden, sind benutzerinstalliert.

Nachdem Sie eine vollständige Liste der erforderlichen Anwendungen erstellt haben, erstellen Sie einen oder mehrere App-Layer und installieren Sie eine oder mehrere der erforderlichen Anwendungen in jedem App-Layer. Sie können beispielsweise verwandte Anwendungen im selben App-Layer installieren. Anwendungen, die von mehreren Benutzern verwendet werden, können Sie in einem elastischen App Layer installieren. Anwendungen, die nur von einem Benutzer verwendet werden, können Sie in dessen Benutzerlayer installieren. Bei vielen Anwendungen ist es einfach, einen App-Layer zu erstellen, andere erfordern eine spezielle Vorbereitung.

Bei vielen Anwendungen ist die Erstellung des App-Layers einfach, andere erfordern eine spezielle Vorbereitung. Informieren Sie sich über die verschiedenen Konfigurationen, die von den Citrix Solution Architects und der App Layering-Community entwickelt wurden. Einige Anwendungen können beispielsweise nur in einem Benutzerlayer und nicht in einem App-Layer installiert werden.

Schritte in ELM für jeden App-Layer:

1. Klicken Sie auf der Registerkarte **Layers** auf **Create App Layer**.
2. Geben Sie im Abschnitt **Layer Details** den Namen und die Version des Layers an.
3. Wählen Sie unter "OS Layer"den zuvor erstellten Betriebssystemlayer aus.
4. Ist die Anwendung von Anwendungen in einem anderen App-Layer abhängig, geben Sie diese unter "Prerequisite Layers"an. Dadurch wird die Reihenfolge bestimmt, in der die App-Layer erstellt werden.
5. Wählen Sie unter "Connector"den zuvor erstellten Citrix Hypervisor-Connector aus. ELM verwendet den Connector zum Schreiben der Packaging-VM für den App-Layer in Citrix Hypervisor. Mit XenCenter können Sie diese dann starten und anpassen.
6. Wenn alle Optionen angegeben sind, klicken Sie auf **Create Layer**. Dadurch wird eine Packaging-VM für den App-Layer erstellt. Nach Abschluss des Vorgangs wird die Statusangabe "Action Required"angezeigt. In diesem Beispiel ist kein Plattformlayer erforderlich, da davon ausgegangen wird, dass der App-Layer auf dem Hypervisor bereitgestellt wird, der beim Erstellen des Betriebssystemlayers ausgewählt wurde.

In XenCenter:

Wenn die Packaging-VM für den App-Layer erstellt ist, wird sie in XenCenter angezeigt. Führen Sie die folgenden Aufgaben aus:

1. Starten Sie die VM.
2. Melden Sie sich auf der Packaging-VM für den App-Layer mit dem lokalen Administratorkonto an.
3. Wenn sofort ein Neustart erforderlich ist, führen Sie ihn aus und melden Sie sich erneut an.
4. Installieren Sie die Anwendungen für den App-Layer und nehmen Sie die erforderlichen Anpassungen vor. Da der Layer von mehreren Benutzern verwendet wird, nehmen Sie keine benutzerspezifischen Anpassungen und Einstellungen vor. Diese werden beim Migrieren der persönlichen vDisk von Benutzern durchgeführt (siehe weiter unten).
5. Nach Installation und Anpassung der Anwendungen für den Layer klicken Sie auf das Desktop-Symbol **Shutdown to Finalize**.

In ELM:

1. Wählen Sie das Symbol für den App-Layer aus (der Status müsste *Editing* lauten).
2. Klicken Sie auf **Finalize**. Der App-Layer ist damit erstellt und kann bereitgestellt werden.
3. Wiederholen Sie diesen Vorgang für jeden erforderlichen App-Layer.

Imagevorlage

Nach der Erstellung von Betriebssystemlayer, Plattformlayer und App-Layer(n) können Sie eine Imagevorlage erstellen. Entscheiden Sie, welche App-Layer in das Layerimage eingebunden und welche Benutzern dynamisch in Form elastischer App-Layer zugewiesen werden sollen. Berücksichtigen Sie dabei:

- Alle App-Layer, die Sie in die Imagevorlage einschließen, stehen allen Benutzern des freigegebenen Layerimages zur Verfügung.
- App-Layer, die Sie bestimmten Benutzern (oder AD-Gruppen) zuweisen, stehen nur diesen zur Verfügung. Sie können solche Zuweisungen später ändern und App-Layer anderen Benutzern oder Gruppen zur Verfügung stellen.

> **Wichtig:**
>
> Die beiden Alternativen schließen sich gegenseitig aus, d. h. Sie dürfen keinen App-Layer in eine Imagevorlage aufnehmen und ihn zugleich einem Benutzer zuweisen. Dies ist unnötig und wird nicht unterstützt.

Als Faustregel gilt, dass im freigegebenen PvD-Image installierte Anwendungen in die Imagevorlage aufgenommen werden sollten. Auf der persönlichen vDisk eines Benutzers installierte Anwendungen sollten als elastische App-Layer zugewiesen werden und solche, die nur von einem Benutzer verwendet werden, können in dessen Benutzerlayer installiert werden.

In ELM:

1. Klicken Sie auf der Registerkarte **Images** auf **Create Template**.
2. Geben Sie einen Namen und eine Version an.
3. Geben Sie den zuvor erstellten Betriebssystemlayer an.
4. Wählen Sie alle App-Layer aus, die Sie in die Imagevorlage einschließen möchten. Wählen Sie keine App-Layer aus, die Sie Benutzern oder AD-Gruppen als elastische App-Layer zuweisen möchten.
5. Wählen Sie eine Connector-Konfiguration. Dadurch wird festgelegt, wo das freigegebene Image bei der Veröffentlichung bereitgestellt wird. Erstellen Sie beim erstmaligen Verwenden eines neuen Bereitstellungsziels eine neue Connector-Konfiguration.

Bei Verwendung von Citrix Hypervisor haben Sie drei Bereitstellungstypen zur Auswahl:

- Citrix Hypervisor: Mit dem Citrix Hypervisor-Connector stellt ELM das veröffentlichte freigegebene Image als VM für Citrix Hypervisor bereit, wo Sie es mit XenCenter starten können. Normalerweise verwenden Sie jedoch Citrix Provisioning oder MCS.
- Citrix Provisioning: Das veröffentlichte freigegebene Image wird als vDisk auf einem Citrix Provisioning-Server bereitgestellt. Beim Erstellen dieser Art von Connector-Konfiguration müssen Sie den Namen des Citrix Provisioning-Servers angeben. Anmeldeinformationen eines Benutzers mit Berechtigung zum Verwalten von Citrix Provisioning. Ausführliche Informationen finden Sie unter "Connector Configuration & Optional Script (Citrix Provisioning)"in der Onlinedokumentation zu App Layering.
- Citrix MCS für Citrix Hypervisor: Das veröffentlichte freigegebene Image wird als VM auf Citrix Hypervisor bereitgestellt, wo Sie es zum Erstellen eines Maschinenkatalogs mit Citrix Virtual Desktops verwenden können.

Beim Erstellen dieser Art von Connector-Konfiguration müssen Sie die Citrix Hypervisor-Adresse und -Anmeldeinformationen angeben, damit ELM dort schreiben kann, sowie das Zielspeicherrepository. Geben Sie außerdem die zuvor erstellte VM-Vorlage an.

Darüber hinaus gilt Folgendes:

- Wählen Sie den zuvor erstellten Plattformlayer (MCS oder Citrix Provisioning) bzw. überspringen Sie diese Option, wenn Sie Citrix Hypervisor verwenden.
- Wenn im Fenster **Layered Image Disk** die Option "SysPrep"angezeigt wird, wählen Sie "Not Generalized".
- Wählen Sie für "Elastic Layering"die Option "Application and User Layers". Diese Einstellung hat zwei Auswirkungen.
  - Sie ermöglicht die Zuweisung zusätzlicher App-Layer zu Benutzern und AD-Gruppen, die dynamisch angefügt werden, wenn sich ein Benutzer anmeldet.
  - Außerdem wird ein neuer Benutzerlayer für Benutzer erstellt, wenn diese sich zum ersten Mal anmelden. (Bei App Layering Version 4.1 ist diese Option nur verfügbar, wenn sie

explizit aktiviert wird. Zum Aktivieren der Option wählen Sie in ELM auf der Unterregisterkarte "Settings and Configuration"der Registerkarte "System"im Fenster "Labs"das Kontrollkästchen "User Layers".)

Ein Benutzerlayer erfasst Profil, Einstellungen, Dokumente usw. eines Benutzers. Er ist das Migrationsziel aller benutzerspezifischen Informationen von der persönlichen vDisk des Benutzers (siehe "Migrationstools"unten).

Klicken Sie im Fenster **Confirm and Complete** auf **Create Template**. Die Erstellung müsste fast augenblicklich erfolgen.

Veröffentlichen des freigegebenen Layerimages

Im letzten Schritt zum Erstellen des freigegebenen Layerimages wählen Sie die **zuvor erstellte Imagevorlage** aus und klicken auf **Publish Layered Image**.

Das erstellte Layerimage wird dann als VM in Citrix Hypervisor (MCS) oder als vDisk auf dem Citrix Provisioning-Server (Citrix Provisioning) bereitgestellt.

Sie können nun mit den normalen MCS- oder Citrix Provisioning-Verwaltungstools einen Citrix Virtual Desktops-Maschinenkatalog und eine Bereitstellungsgruppe erstellen:

- Verwenden Sie für MCS Studio, um einen Maschinenkatalog zu erstellen, und importieren Sie die freigegebene Layerimage-VM.
- Verwenden Sie für Citrix Provisioning den Citrix Virtual Desktops-Setupassistenten, um einen Maschinenkatalog in Studio zu erstellen.

Der letzte Schritt beim Migrieren der PvD-VM eines Benutzers zu App Layering wird im folgenden Abschnitt beschrieben. Das Verfahren in der Vorschau: Sie führen gleichzeitig die ursprüngliche PvD-VM und die neue App Layering-VM aus, melden sich unter Verwendung des Kontos des PvD-Benutzers bei der App Layering-VM an und führen ein Migrationstool aus, um das Profil und die Einstellungen des Benutzers von der PvD in den Benutzerlayer von App Layering zu übertragen.

Migrationstools

Citrix empfiehlt die Verwendung von PCmover oder USMT zum Migrieren der persönlichen Informationen von der persönlichen vDisk eines Benutzers in dessen App Layering-Benutzerlayer.

- PCmover ist ein Programm von LapLink.com. Sie können die PvD-VM eines Benutzers und die App Layering-VM ausführen und die Einstellungen des Benutzers mit PCmover von PvD-VM auf die App Layering-VM übertragen. Die beiden VMs können gleichzeitig ausgeführt und die Informationen über ein Netzwerk übertragen werden oder Sie führen sie nacheinander aus und übertragen die Informationen in Form einer Datei.

PCmover bietet eine benutzerfreundliche Oberfläche, mit der Sie die übertragenen Informationen präzise steuern können. Wenn Sie mehrere PvD-VMs migrieren müssen, empfiehlt es sich ggf., den PCmover Policy Manager zum Erstellen einer Richtliniendatei zu verwenden. Mit einer Richtliniendatei können Sie Migrationen unter minimaler Interaktion durchführen.

Einzelheiten finden Sie im PCmover-Benutzerhandbuch.

- USMT ist eine Reihe von Programmen, die Microsoft als Teil von Windows Automation Installation Kit (AIK) zur Verfügung stellt. Ein Scanstate-Programm wird auf der PvD-VM ausgeführt, um eine Übertragungsdatei zu schreiben. Ein Loadstate-Programm wird auf der App Layering-VM ausgeführt, um die Übertragungsdatei zu lesen und anzuwenden. Welche Informationen übertragen werden, wird durch mehrere XML-Dateien bestimmt. Die Dateien können bearbeitet werden, wenn die Standardeinstellungen nicht Ihren Anforderungen entsprechen.

In diesem Artikel wird davon ausgegangen, dass Sie PCmover verwenden.

Migrieren von Benutzerinformationen

Es wird davon ausgegangen, dass Sie bereits aus dem ursprünglichen freigegebenen PvD-Image ein funktional äquivalentes, freigegebenes App Layering-Layerimage erstellt haben. Sie haben eine oder mehrere Benutzer-PvD-VMs mit jeweils einer persönlichen vDisk, die das Benutzerprofil und andere Informationen enthält, welche Sie in einen App Layering-Benutzerlayer migrieren möchten.

Für jeden Benutzer starten Sie dessen PvD-VM und das freigegebene Layerimage, melden sich bei beiden VMs mit den Domänenanmeldeinformationen des Benutzers an und führen PCmover aus.

Migrieren von Benutzerinformationen:

1. Installieren Sie PCmover in einer Freigabe, auf die sowohl von der PvD-VM als auch vom freigegebenen Layerimage aus zugegriffen werden kann.
2. Starten Sie in Studio die PvD-VM des Benutzers. Melden Sie sich als der betreffende Benutzer an. Deaktivieren Sie Firewalls.
3. Weisen Sie in ELM dem Benutzer sämtliche elastischen App-Layer zu, die dieser benötigt.
4. Stellen Sie sicher, dass der Benutzer Schreibzugriff auf das Verzeichnis seines Benutzerlayers hat. Informationen finden Sie unter “Configure Security on User Layer Folders”in der Onlinedokumentation.
5. Starten Sie über Studio die freigegebene Layerimage-VM. Melden Sie sich als der betreffende Benutzer an. Wenn sich der Benutzer zum ersten Mal anmeldet, erstellt die VM einen Benutzerlayer in der Netzwerkdateifreigabe. Deaktivieren Sie Firewalls, Antiviren- und Anti-Spyware-Anwendungen.
6. Führen Sie PCmover auf der PvD-VM aus.

    a) Wählen Sie “PC to PC Transfer”und dann “Next”.

b) Wählen Sie “Old”und “Next”.
c) Wählen Sie “Wifi or Wired Network”und “Weiter”.
d) PCmover scannt nun die PvD-VM. Dies dauert ein paar Minuten. Danach wählen Sie “Next” .
e) Vorausgesetzt, Sie möchten nach Abschluss der Übertragung keine E-Mail-Benachrichtigung erhalten, wählen Sie “Next”.
f) Geben Sie ggf. ein Kennwort ein. Ein Kennwort stellt sicher, dass die Benutzerinformationen von der PvD-VM an keine andere VM als die freigegebene Layerimage-VM gesendet werden. Wählen Sie dann “Next”.

7. Führen Sie PCmover auf der App Layering-VM aus.

a) Wählen Sie “PC to PC Transfer”und dann “Next”.
b) Wählen Sie “New”und “Next”.
c) Geben Sie die erforderlichen Validierungswerte für die Seriennummer ein.
d) Geben Sie unter “Network Name”den Namen der PvD-VM ein und wählen Sie “Next”.
e) Rufen Sie das Fenster “Application Selections”auf. Citrix empfiehlt, die Auswahl aller Anwendungen aufzuheben. Sie müssten App-Layer für alle erforderlichen Anwendungen erstellt haben.
f) Rufen Sie das Fenster “User Account Selections”auf. Citrix empfiehlt, für jegliche Benutzer mit Ausnahme des Besitzers der persönlichen vDisk “Do not transfer this user” auszuwählen.
g) Rufen Sie das Fenster “Custom Settings”auf. Citrix empfiehlt, “Files and Settings Only” auszuwählen.
h) Rufen Sie das Fenster “Drive Selections”auf. Citrix empfiehlt, für alle Laufwerke außer C: “Do not transfer this drive”auszuwählen.
i) Nachdem Sie alle Fenster aufgerufen haben, klicken Sie auf “Next”.
j) Vorausgesetzt, Sie möchten nach Abschluss der Übertragung keine E-Mail-Benachrichtigung erhalten, wählen Sie “Next”.

PCmover beginnt nun mit der Übertragung von Dateien und Einstellungen von der PvD-VM an den App Layering-Benutzerlayer.

Ermitteln der erforderlichen Anwendungen mit PCmover

Sie können mit PCmover eine PvD-VM analysieren, um die installierten Anwendungen zu ermitteln. Diese Methode ist eine Alternative zur Verwendung von Programme und Features in der **Systemsteuerung**.

1. Führen Sie PCmover auf der PvD-VM aus.
2. Wählen Sie “PC to PC Transfer”und dann “Next”.

3. Wählen Sie “Old”und “Next”.
4. Wählen Sie “File Storage Device”und dann “Next”.
5. Rufen Sie das Fenster “Application Selections”auf und notieren Sie sich die installierten Anwendungen.
6. Brechen Sie PCmover ab.

Entfernen von Komponenten

September 21, 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 beispielsweise einen Delivery Controller entfernen, werden die SQL-Serversoftware und die Datenbanken nicht entfernt.

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.

Informationen zum Entfernen von Features, die nicht unten aufgeführt sind, finden Sie in der Dokumentation des jeweiligen Features.

Vorbereitung

Bevor Sie einen Controller entfernen, müssen Sie ihn aus der Site entfernen. Einzelheiten finden Sie unter Entfernen eines Controllers.

Schließen Sie Studio und Director, bevor Sie sie entfernen.

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 klicken Sie mit der rechten Maustaste auf **Citrix Virtual Apps *Version*** bzw. **Citrix Virtual Desktops *Version*** und wählen Sie **Deinstallieren**. Das Installationsprogramm wird gestartet. Wählen Sie die Komponenten aus, die Sie entfernen möchten.

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 mit der rechten Maustaste auf **Citrix Virtual Delivery Agent *Version***, und wählen Sie **Deinstallieren**. Das Installationsprogramm wird gestartet und Sie können die zu entfernenden Komponenten markieren. Nach dem Entfernen wird die Maschine in der Standardeinstellung automatisch neu gestartet.
- Zum Entfernen des universellen Druckservers klicken Sie mit der rechten Maustaste auf **Citrix Universeller Druckserver** 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:

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /remove /components
studio
```

Entfernen von VDAs über die Befehlszeile

Führen Sie auf dem Installationsmedium im Setupverzeichnis \x64\XenDesktop den Befehl `XenDesktopVdaSetup.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.

Nach dem Entfernen wird die Maschine in der Standardeinstellung automatisch neu gestartet.

Mit dem folgenden Befehl werden beispielsweise der VDA und die Citrix Workspace-App entfernt:

```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /removeall
```

Informationen zum Entfernen von VDAs mit einem Skript in Active Directory finden Sie unter Installieren oder Entfernen von VDAs mit Skripts.

Upgrade und Migration

April 19, 2024

Informationen zum Upgrade

Bei Upgrades wird eine Bereitstellung auf Citrix Virtual Apps and Desktops 7 1912 Long Term Service (LTSR) aktualisiert, ohne dass neue Maschinen oder Sites erstellt werden müssen. Ein solches Upgrade wird als direktes Upgrade bezeichnet.

Durch das Upgrade erhalten Sie Zugriff auf die neuesten Features und Technologien, auf die Sie Anspruch haben. Außerdem können Upgrades Korrekturen und Verbesserungen früherer Versionen enthalten.

Mögliche Versionen für ein Upgrade

Sie können von folgenden Version ein Upgrade auf LTSR ausführen:

- XenApp und XenDesktop 7.6 LTSR mit oder ohne kumulative Updates (CU), bis einschließlich CU9 (nur für unter Systemanforderungen aufgeführte Plattformen)
- XenApp und XenDesktop 7.15 LTSR mit oder ohne kumulative Updates (CU), bis einschließlich CU7
- XenApp und XenDesktop 7.16
- XenApp und XenDesktop 7.17
- XenApp und XenDesktop 7.18
- Citrix Virtual Apps and Desktops 7 1808
- Citrix Virtual Apps and Desktops 7 1811
- Citrix Virtual Apps and Desktops 7 1903
- Citrix Virtual Apps and Desktops 7 1906
- Citrix Virtual Apps and Desktops 7 1909

Wichtiger Hinweis zum Upgrade von VDAs

Wurde die PvD-Komponente (persönliche vDisk) jemals auf einem VDA installiert, kann dieser nicht auf Version 1912 LTSR oder höher aktualisiert werden. Um den neuen VDA zu verwenden, müssen Sie den bestehenden VDA deinstallieren und dann den neuen VDA installieren.

Die ist auch dann erforderlich, wenn Sie PvD nie verwendet haben.

Herausfinden, ob Sie das betrifft

Wie PvD eventuell in früheren Versionen installiert wurde:

- Auf der grafischen Benutzeroberfläche des VDA-Installationsprogramms war PvD eine Option (Kontrollkästchen auf der Seite **Zusätzliche Komponenten**). In den 7.x-Versionen bis 7.15 LTSR war diese Option standardmäßig aktiviert. Wenn Sie die Standardeinstellungen akzeptiert haben (oder die Option in einem Release explizit aktiviert haben), wurde PvD installiert.
- In der Befehlszeile wurde PvD über die Option `/baseimage` installiert. Wenn Sie diese Option angegeben oder ein Skript verwendet haben, das diese Option enthielt, wurde PvD installiert.

Wenn Sie nicht wissen, ob auf Ihrem VDA PvD installiert ist, führen Sie das Installationsprogramm für den neuen VDA (1912 LTSR oder höher) auf der Maschine bzw. dem Image aus.

- Wenn PvD installiert ist, weist eine Meldung darauf hin, dass eine inkompatible Komponente vorhanden ist.
  - Klicken Sie auf der grafischen Benutzeroberfläche auf der Seite mit der Meldung auf **Abbrechen** und bestätigen Sie, dass Sie das Installationsprogramm schließen möchten.
  - Wenn Sie die Befehlszeile verwenden, schlägt der Befehl unter Anzeige der Meldung fehl.
- Wenn PvD nicht installiert ist, wird das Upgrade fortgesetzt.

Aktion

Wenn PvD auf dem VDA nicht installiert ist, folgen Sie dem normalen Upgradeverfahren.

Wenn PvD auf dem VDA installiert ist, gehen Sie folgendermaßen vor:

1. Deinstallieren Sie den VDA. Einzelheiten finden Sie unter Entfernen von Komponenten.
2. Installieren Sie den neuen VDA.

Wenn Sie PvD weiterhin verwenden möchten, können Sie dies nur auf den Versionen VDA 7.15 LTSR bis Win 7 und Win 10 (1607 oder früher) tun.

Ausführen des Upgrades

Beachten Sie die Dokumentation, bevor Sie mit dem Upgrade beginnen.

Upgrade der Kernkomponenten und VDAs:

1. Führen Sie das Installationsprogramm auf den Maschinen aus, auf denen die Komponenten 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.

Upgradevorbereitung und Empfehlungen: Der Artikel Upgrade einer Bereitstellung ist Ihre primäre Informationsquelle für die Kernkomponenten und VDAs. Dieser Artikel beschreibt die Upgradesequenz und Reihenfolge, Einschränkungen, Vorbereitungsschritte und andere Überlegungen. Er enthält auch das Upgradeverfahren Schritt für Schritt und Anweisungen für das Upgrade der Datenbanken und der Site nachdem Sie die Kernkomponenten aktualisiert haben.

Einzelheiten zur Installation: Nachdem Sie alle Vorbereitungen abgeschlossen haben und bereit sind, das Installationsprogramm zu starten, zeigt Ihnen der Installationsartikel, was Sie sehen (wenn Sie die grafische Benutzeroberfläche verwenden) oder was Sie eingeben (wenn Sie die Befehlszeilenschnittstelle verwenden), um ein Upgrade der Komponenten durchzuführen. Wenn das Installationsprogramm abgeschlossen ist, kehren Sie zur Anleitung unter Upgrade einer Bereitstellung für die Upgrades von Datenbank und Site zurück.

- Installieren/Aktualisieren von Kernkomponenten über die grafische Oberfläche
- Installieren/Aktualisieren von Kernkomponenten über die Befehlszeile
- Installieren/Aktualisieren von VDAs über die grafische Oberfläche
- Installieren/Aktualisieren von VDAs über die Befehlszeile

Weitere Informationen zur Installation von Hotfixes für Controller finden Sie unter CTX201988.

Upgradelizenzierung

Einen umfassenden Überblick über die Verwaltung der Citrix Lizenzierung finden Sie unter Activate, upgrade, and manage Citrix licenses.

Für eine On-Premises-Bereitstellung können Sie das vollständige Produktinstallationsprogramm verwenden, um den Lizenzserver zu aktualisieren. Sie können die Lizenzkomponenten auch separat herunterladen und aktualisieren. Siehe Upgrade.

Upgrade anderer Komponenten

Zusätzlich zu den Kernkomponenten und VDAs enthalten On-Premises-Bereitstellungen von Citrix Virtual Apps and Desktops die folgenden Komponenten, die Sie aktualisieren können, wenn neuere Versionen veröffentlicht werden.

- StoreFront
- AppDNA
- Citrix App Layering
- HDX RealTime Optimization Pack
- Profilverwaltung

- Citrix Provisioning
- Sitzungsaufzeichnung
- Workspace Environment Management

Häufig gestellte Fragen

Dieser Abschnitt enthält Antworten auf häufig gestellte Fragen zum Upgrade von Citrix Virtual Apps and Desktops.

- **In welcher Reihenfolge muss die Virtual Apps and Desktops-Umgebung aktualisiert werden?**

  Der VDA kann jederzeit und in beliebiger Reihenfolge aktualisiert werden. Aktualisieren Sie zunächst die Hälfte der Controller, bevor Sie Ihre Site aktualisieren. Aktualisieren Sie anschließend die Site und zum Schluss die restlichen Controller. Weitere Informationen finden Sie unter Aktualisierungsreihenfolge und Upgradeverfahren.

- **Meine Site hat mehrere Delivery Controller (in verschiedenen Zonen). Was geschieht, wenn nur einige aktualisiert werden? Muss ich jeden Controller der Site im gleichen Wartungsfenster aktualisieren?**

  Es hat sich bewährt, alle Delivery Controller in einem Wartungsfenster zu aktualisieren, da verschiedene Dienste auf den Controllern miteinander kommunizieren. Das Beibehalten unterschiedlicher Versionen kann zu Problemen führen. Es wird empfohlen, zunächst die Hälfte der Controller zu aktualisieren, dann die Site zu aktualisieren und zum Schluss die restlichen Controller zu aktualisieren. (Weitere Informationen finden Sie unter Upgradeverfahren.)

- **Muss ich inkrementelle Upgrades durchführen oder kann ich direkt zur neuesten Version wechseln?**

  Sie können Zwischenversionen fast immer überspringen und sofort die neueste Version installieren, sofern der Artikel **Neue Features** für die Upgrade-Version keine anderslautenden Informationen enthält. Siehe Upgradehandbuch.

- **Können Kunden ein Upgrade von einer LTSR-Umgebung (Long Term Service Release) auf ein aktuelles Release durchführen?**

  Ja. Kunden müssen nicht auf Dauer in einer LTSR-Umgebung bleiben. Sie können eine LTSR-Umgebung in ein aktuelles Release umwandeln, je nach Geschäftsanforderungen und verwendeten Features.

- **Sind gemischte Versionen von Komponenten zulässig?**

  Citrix empfiehlt, alle Komponenten in einer Site auf dieselbe Version zu aktualisieren. Sie können zwar von einigen Komponenten die früheren Versionen verwenden, jedoch sind u. U. nicht

alle Features einer aktuellen Version verfügbar. Weitere Informationen finden Sie unter Hinweise zu heterogenen Umgebungen.

- **Wie häufig muss ein aktuelles Release aktualisiert werden?**

  Ein aktuelles Release wird nach Veröffentlichung für insgesamt 6 Monate gewartet (EOM). Citrix empfiehlt Kunden, das jeweils neueste aktuelle Release zu übernehmen. 18 Monate nach Veröffentlichung wird das Ende des Lebenszyklus (EOL) für aktuelle Releases erreicht. Weitere Informationen finden Sie unter Current Release Lifecycle.

- **Welches Upgrade ist empfehlenswert: LTSR oder aktuelles Release?**

  Aktuelle Releases bieten die neuesten und innovativsten Virtualisierungsfeatures für Apps, Desktops und Server. Damit bleiben Sie auf dem neuesten Stand der Technik und sind der Konkurrenz stets voraus.

  Long Term Service Releases (LTSRs) sind ideal für Produktionsumgebungen großer Unternehmen, die dieselbe Basisversion für einen längeren Zeitraum beibehalten möchten.

  Weitere Informationen finden Sie unter Wartungsoptionen.

- **Muss ich meine Lizenzen aktualisieren?**

  Sie müssen sicherstellen, dass Ihre aktuelle Lizenz nicht abgelaufen ist und somit für das Release gültig ist, auf die Sie ein Upgrade durchführen. Siehe CTX111618. Informationen zur Verlängerung finden Sie unter Verlängerungslizenzen für Customer Success Services.

- **Wie lange dauert ein Upgrade?**

  Die erforderliche Zeit für das Upgrade einer Bereitstellung hängt von der Infrastruktur und dem Netzwerk ab. Wir können daher keine genaue Dauer angeben.

- **Was sind bewährte Methoden?**

  Lesen und befolgen Sie die Vorbereitungshinweise.

- **Welche Betriebssysteme werden unterstützt?**

  Siehe Systemanforderungen.

  Wenn Ihr vorhandenes Betriebssystem für die Version, auf die Sie aktualisieren, nicht verwendet werden kann, finden Sie weitere Informationen unter Ihre Möglichkeiten.

- **Welche Versionen von VMware vSphere (vCenter + ESXi) werden unterstützt?**

  Unter Hosts/Virtualisierungsressourcen werden die unterstützten Versionen für alle unterstützten Hosts auf, einschließlich VMware aufgelistet.

- **Wann erreicht meine Version das Ende des Lebenszyklus (EOL)?**

  Konsultieren Sie die Produktmatrix.

- **Was sind bekannte Probleme im aktuellen Release?**

- Citrix Virtual Apps and Desktops
- StoreFront
- Citrix Provisioning
- Citrix Lizenzserver
- Citrix Workspace-App

Migration

Durch eine Migration werden Daten von einer früheren Bereitstellung in eine neuere Version verschoben. Eine Migration umfasst die Installation neuerer 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.
- Informationen zur Migration von XenApp 6.x finden Sie unter Migrieren von XenApp 6.x.

Weitere Informationen

LTSR (Long Term Service Release)-Bereitstellungsupdates verwenden kumulative Updates (CUs). Ein CU aktualisiert Basiskomponenten des LTSR, und jedes CU enthält einen eigenen Metainstaller.

Jedes CU hat eigene Dokumentation. Für 7.15 LTSR zum Beispiel, verwenden Sie den Link auf der Seite Neues Features für das neueste CU. Jede CU-Seite enthält Informationen zur unterstützten Version, Anweisungen und einen Link zum CU-Downloadpaket.

Änderungen in 7.x

September 21, 2021

Ab XenApp und XenDesktop 7.x ändern sich die Citrix Virtual Apps and Desktops-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.

Sofern nicht anders angegeben, bezieht sich *7.x* und "neuere Versionen"auf XenApp-Version 7.5 oder höher und XenDesktop-Version 7 oder höher, einschließlich aller Citrix Virtual Apps and Desktops-Releases.

Dieser Abschnitt enthält eine Übersicht. Umfassende Informationen zum Upgrade von Versionen vor 7.x finden Sie unter Upgrade auf XenApp 7.

Änderungen an den Elementen nach XenApp 6

Obwohl die funktionellen Elemente nicht genau gleich sind, erleichtert die folgende Tabelle das Zuordnen der funktionellen Elemente von XenApp bis Version 6.5 zu neuere Versionen: Die Unterschiede an der Architektur werden weiter unten beschrieben.

XenApp 6.x und früher	Neuere Versionen
Independent Management Architecture (IMA)	FlexCast Management Architecture (FMA)
Farm	Site
Workergruppe	Maschinenkatalog und Bereitstellungsgruppe
Worker	Virtual Delivery Agent (VDA), Maschine für Multisitzungs-OS, VDA für Multisitzungs-OS, Maschine für Einzelsitzungs-OS, VDA für Einzelsitzungs-OS
Remotedesktopdienste (RDS) oder Terminaldienste-Maschine	Maschine für Einzelsitzungs-OS, VDA für Multisitzungs-OS
Zonen- und Datensammelpunkt	Delivery Controller
Delivery Services Console	Citrix Studio und Citrix Director
Veröffentlichen von Anwendungen	Bereitstellen von Anwendungen
Datenspeicher	Datenbank
Lastauswertungsprogramm	Lastverwaltungsrichtlinie
Administrator	Delegierter Administrator, Rolle, Bereich

Änderungen an der Architektur

Ab Version 7.x basiert Citrix Virtual Apps and Desktops (zuvor "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 späteren Versionen steht die Site an oberster Ebene. 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 späteren Versionen 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 späteren Versionen 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 späteren Versionen 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 späteren Versionen 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 späteren Versionen 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 bereitgestell-

ten Anwendungen haben. Sie können alternativ zu mehreren Bereitstellungsgruppen optional Anwendungsgruppen erstellen.

- **Datenbank:** In späteren Versionen wird der IMA-Datenspeicher nicht für Konfigurationsinformationen verwendet. 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 späteren Versionen 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 späteren Versionen 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	Spätere Versionen
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 späteren Versionen aktivieren Sie die Features für bestimmte Benutzer, indem Sie diese Einstellungen für vorhandene Bereitstellungsgruppen konfigurieren. Siehe Konfigurieren des Vorabstarts und des Fortbestehens von Sitzungen.
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. Siehe Benutzer.
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	Spätere Versionen
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 in Citrix Virtual Apps and Desktops 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 Citrix 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 (einschließlich Citrix Receiver für Windows vor Version 3.0, Citrix Receiver für Linux 11.100 und Citrix Online-Plug-In 12.1) 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 späteren Releases 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 späteren 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

Die folgenden Änderungen betreffen die Citrix Workspace-App (zuvor “Citrix Receiver”):

- **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-Releases 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

December 18, 2023

Einführung

Sie können bestimmte Bereitstellungen aktualisieren, ohne zunächst neue Maschinen oder Sites erstellen zu müssen. Dies wird als direktes Upgrade bezeichnet. Informationen zu den Versionen von Citrix Virtual Apps and Desktops, die Sie aktualisieren können, finden Sie unter Citrix Upgrade Guide.

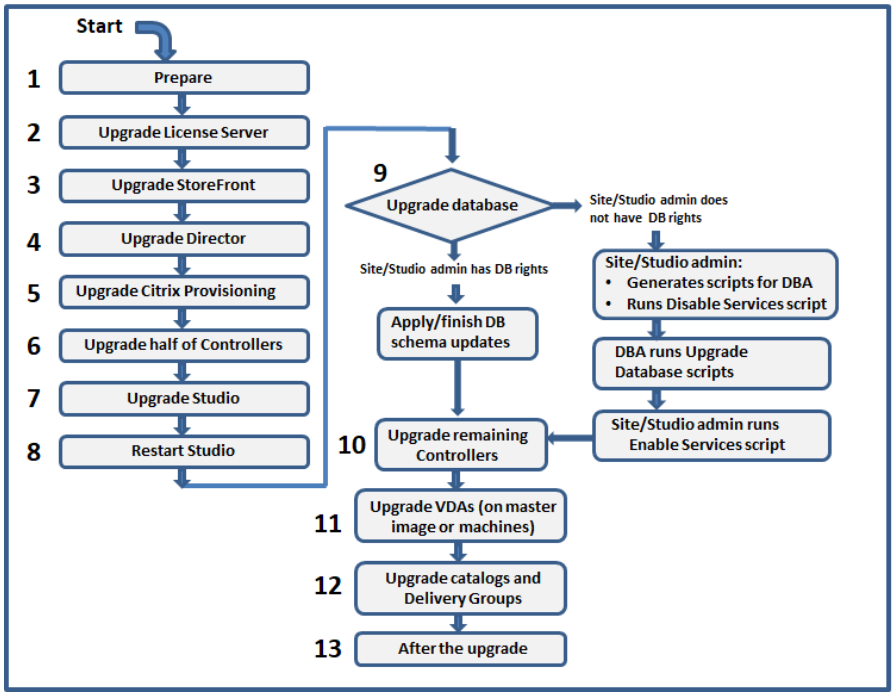
Zum Starten eines Upgrades führen Sie das Installationsprogramm von der neuen Version aus, um zuvor installierte Kernkomponenten, VDAs und bestimmte andere Komponenten zu aktualisieren. Anschließend führen Sie ein Upgrade der Sitedatenbanken und der Site durch.

Sie können Upgrades aller Komponenten durchführen, die mit dem Komplettinstallationsprogramm (und den dedizierten VDA-Installationspaketen) installiert werden können, sofern eine neuere Version verfügbar ist. Informationen zu anderen Komponenten, die nicht mit dem Komplettinstallationsprogramm installiert werden (z. B. Citrix Provisioning und Profilverwaltung) finden Sie in der zugehörigen Dokumentation. Informationen zu Hostupgrades finden Sie in der entsprechenden Dokumentation.

Lesen Sie vor einem Upgrade alle Informationen in diesem Artikel.

Aktualisierungsreihenfolge

Die folgende Abbildung zeigt die Upgradereihenfolge. Unter Upgradeverfahren finden Sie Details zu den einzelnen Schritten.



> **Hinweis:**
>
> Um Fehler zu vermeiden, müssen Sie alle Delivery Controller und die Datenbank aktualisieren, bevor Sie Aufgaben im Zusammenhang mit Bereitstellungen und Bereitstellungsgruppen ausführen (z. B. Maschinenkatalog erstellen oder löschen, Maschine in einer Bereitstellungsgruppe aktualisieren usw.).

Upgradeverfahren

Die meisten Hauptproduktkomponenten können unter Ausführen des Produktinstallationsprogramms auf der Maschine mit der jeweiligen Komponente aktualisiert werden.

Wenn eine Maschine mehrere Komponenten enthält (z. B. Studio und Lizenzserver), werden alle Komponenten aktualisiert, wenn das Produktmedium neuere Versionen enthält.

Verwenden der Installationsprogramme:

- Zum Ausführen der grafischen Oberfläche des Komplettinstallationsprogramms 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**.
- Geben Sie den entsprechenden Befehl ein, um die Befehlszeilenschnittstelle zu verwenden. Weitere Informationen finden Sie unter Installieren über die Befehlszeile.

Schritt 1: Vorbereiten

Treffen Sie vor dem Upgrade alle erforderlichen Vorbereitungen. Erledigen Sie jegliche erforderlichen Aufgaben:

- Upgrade von VDAs auf 1912 oder höher
- Einschränkungen
- Hinweise zu heterogenen Umgebungen
- Ältere Betriebssysteme
- Vorbereitung
- Sitetests zur Vorbereitung
- SQL Server-Versionsprüfung

Schritt 2: Upgrade des Lizenzservers durchführen

Liegt eine neue Version der Citrix Lizenzserver-Software vor, aktualisieren Sie diese Komponente vor allen anderen Komponenten.

Wenn Sie noch nicht geprüft haben, ob Ihr Lizenzserver mit der neuen Version kompatibel ist, sollten Sie das Installationsprogramm auf der Lizenzserver ausführen, bevor Sie andere Kernkomponenten aktualisieren.

Schritt 3: StoreFront aktualisieren

Wenn das Installationsmedium eine neue Version der StoreFront-Software enthält, führen Sie das Installationsprogramm auf der Maschine mit dem StoreFront-Server aus.

- Wählen Sie in der GUI im Bereich **Erweitern der Bereitstellung** die Option **Citrix StoreFront**.
- Führen Sie `CitrixStoreFront-x64.exe` in einer Befehlszeile aus. Die Datei ist im Ordner `x64` des Citrix Virtual Apps and Desktops-Installationsmediums.

Schritt 4: Director aktualisieren

Wenn das Installationsmedium eine neue Version der Director-Software enthält, führen Sie das Installationsprogramm auf der Maschine mit Director aus.

Schritt 5: Citrix Provisioning aktualisieren

Für Citrix Provisioning gibt es ein eigenes Installationsmedium, separat vom Citrix Virtual Apps and Desktops-Installationsmedium. Informationen zum Installieren und Aktualisieren der Server- und

Zielgerätesoftware für Citrix Provisioning finden Sie unter Produktdokumentation für Citrix Provisioning.

Schritt 6: Hälfte der Delivery Controller aktualisieren

Wenn Ihre Site beispielsweise über vier Controller verfügt, führen Sie das Installationsprogramm auf zweien 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.

Vorabtests an der Site werden auf dem ersten Controller ausgeführt, bevor das eigentliche Upgrade gestartet wird. Weitere Informationen finden Sie unter Sitetests zur Vorbereitung.

Schritt 7: Studio aktualisieren

Wenn Sie Studio noch nicht aktualisiert haben (weil es sich auf einer Maschine mit einer anderen Komponente befindet), führen Sie das Installationsprogramm auf der Maschine mit Studio aus.

Schritt 8: Studio neu starten

Starten Sie Studio nach dem Upgrade neu. Der Upgradeprozess wird automatisch fortgesetzt.

Schritt 9: Datenbank und Site aktualisieren

> **Hinweis:**
>
> Um Fehler zu vermeiden, müssen Sie alle Delivery Controller und die Datenbank aktualisieren, bevor Sie Aufgaben im Zusammenhang mit Bereitstellungen und Bereitstellungsgruppen ausführen (z. B. Maschinenkatalog erstellen oder löschen, Maschine in einer Bereitstellungsgruppe aktualisieren usw.).

Der Artikel Vorbereitung enthält Informationen zu den zum Aktualisieren des Schemas der SQL Server-Datenbanken erforderlichen Berechtigungen.

- Wenn Sie ausreichende Berechtigungen zum Aktualisieren des SQL Server-Datenbankschemas haben, können Sie ein automatisches Datenbankupgrade beginnen. Fahren Sie mit dem Verfahren unter Automatisches Upgrade von Datenbank und Site fort.
- Wenn Sie keine ausreichenden Datenbankberechtigungen haben, können Sie ein manuelles Upgrade mit Skripts beginnen und die Hilfe des Datenbankadministrators in Anspruch nehmen (einer Person mit den erforderlichen Berechtigungen). Für ein manuelles Upgrade generiert der Studio-Benutzer Skripts, die Dienste aktivieren und deaktivieren, und führt diese dann aus. Der Datenbankadministrator führt andere Skripts, die das Datenbankschema aktualisieren, mit dem SQLCMD-Hilfsprogramm oder mit SQL Server Management Studio im SQLCMD-Modus aus. Fahren Sie mit dem Verfahren unter Manuelles Aktualisieren von Datenbank und Site fort.
- Wenn Sie eine Bereitstellung mit mehreren Zonen haben und die Datenbank und Site automatisch aktualisieren möchten, empfiehlt Citrix das Durchführen des dbschema-Upgrades in der Zone, in der sich die SQL Server-Sitedatenbanken befinden. Andernfalls kann das automatische Upgrade der Datenbank und Site fehlschlagen.

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.

Automatisches Upgrade von Datenbank und Site

1. Starten Sie das neu aktualisierte Studio.
2. Geben Sie an, dass Sie das Siteupgrade automatisch starten möchten, und bestätigen Sie, dass Sie bereit sind.

Das Datenbank- und Siteupgrade wird fortgesetzt.

Manuelles Aktualisieren von Datenbank und Site

1. Starten Sie das neu aktualisierte Studio.
2. Geben Sie an, dass Sie die Site manuell aktualisieren möchten. Der Assistent prüft die Kompatibilität des Lizenzservers und fordert eine Bestätigung an.
3. Bestätigen Sie, dass Sie die Datenbank gesichert haben.

   Der Assistent erstellt Skripts und eine Checkliste der Upgradeschritte und zeigt diese an. Wenn sich das Datenbankschema mit dem Produktupgrade nicht ändert, wird das Skript nicht generiert. Ändert sich beispielsweise das Schema der Protokollierungsdatenbank nicht, wird das Skript `UpgradeLoggingDatabase.sql` nicht generiert.
4. Führen Sie die folgenden Skripts in der angegebenen Reihenfolge aus:

   - `DisableServices.ps1`: Der Studio-Benutzer führt dieses PowerShell-Skript auf einem Controller aus, um die Produktdienste zu deaktivieren.

- `UpgradeSiteDatabase.sql`: Der Datenbankadministrator führt dieses SQL-Skript auf dem Server mit der Sitedatenbank aus.
- `UpgradeMonitorDatabase.sql`: Der Datenbankadministrator führt dieses SQL-Skript auf dem Server mit der Überwachungsdatenbank aus.
- `UpgradeLoggingDatabase.sql`: Der Datenbankadministrator führt dieses SQL-Skript auf dem Server mit der Konfigurationsprotokollierungsdatenbank aus. Führen Sie dieses Skript nur aus, wenn diese Datenbank geändert wird (z. B. nach dem Anwenden eines Hotfixes).
- `EnableServices.ps1`: Der Studio-Benutzer führt dieses PowerShell-Skript auf einem Controller aus, um die Produktdienste zu aktivieren.

Nach dem Upgrade der Datenbank und der Aktivierung der Produktdienste testet Studio automatisch 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.

5. Nach Abschluss der Checklistenaufgaben klicken Sie auf **Upgrade fertig stellen**.

Schritt 10: Upgrade der übrigen Delivery Controller durchführen

Wählen Sie in der neu aktualisierten Studio-Version im Navigationsbereich **Citrix Studio** *Sitename* aus. Wählen Sie auf der Registerkarte **Häufige Aufgaben** die Option **Upgrade der übrigen Delivery Controller durchführen**.

Nachdem Sie das Upgrade abgeschlossen und bestätigt haben, schließen Sie Studio und öffnen es neu. Sie werden von Studio ggf. zu einem zusätzlichen Siteupgrade aufgefordert, um die Controllerdienste bei der Site zu registrieren oder eine Zonen-ID zu erstellen, falls noch keine vorhanden ist.

Schritt 11: VDAs aktualisieren

> **Wichtig:**
>
> Informationen zum Aktualisieren eines VDA auf Version 1912 oder höher finden Sie unter Upgrade von VDAs auf 1912 oder höher.

Führen Sie das Produktinstallationsprogramm auf Maschinen mit VDAs aus.

Wenn Sie Maschinen mit Maschinenerstellungsdiensten und einem Masterimage erstellt haben, wechseln Sie zum Host und aktualisieren Sie den VDA auf dem Masterimage. Sie können jedes der verfügbaren VDA-Installationsprogramme verwenden.

- Anleitungen für die graphische Benutzeroberfläche finden Sie unter Installieren von VDAs.
- Anleitungen für die Befehlszeile finden Sie unter Installieren über die Befehlszeile.

Wenn Sie Maschinen mit Citrix Provisioning erstellt haben, finden Sie Informationen zum Upgrade in der Produktdokumentation für Citrix Provisioning.

Mehr erfahren Sie in diesem Video:

Schritt 12: Maschinenkataloge und Bereitstellungsgruppen aktualisieren

- Führen Sie ein Update von Katalogen durch, die Maschinen mit aktualisierten VDAs verwenden.
- Führen Sie ein Upgrade von Katalogen durch, die Maschinen mit aktualisierten VDAs verwenden.
- Führen Sie ein Upgrade von Bereitstellungsgruppen durch, die Maschinen mit aktualisierten VDAs verwenden.

Schritt 13: Nachbereitung

Nach Abschluss eines Upgrades können Sie die aktualisierte Site testen. Wählen Sie in Studio im Navigationsbereich **Citrix Studio (Sitename)**. Wählen Sie auf der Registerkarte **Häufige Aufgaben** die Option **Site testen**. Diese Tests werden automatisch nach dem Upgrade der Datenbank ausgeführt, Sie können sie jedoch jederzeit wiederholen.

Die Tests können 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. Um dies zu vermeiden führen Sie folgende Schritte aus:

- Aktivieren Sie den SQL Server Browser-Dienst (falls erforderlich) und starten Sie ihn.
- Starten Sie den SQL Server-Dienst (SQLEXPRESS) neu.

Aktualisieren Sie andere Komponenten in Ihrer Bereitstellung. Anleitungen finden Sie in der folgenden Produktdokumentation:

- StoreFront
- AppDNA
- Citrix App Layering
- HDX RealTime Optimization Pack
- Profilverwaltung
- Citrix Provisioning
- Sitzungsaufzeichnung
- Workspace Environment Management

Informationen zum Ersetzen der Microsoft SQL Server Express LocalDB-Software durch eine höhere Version finden Sie unter Ersetzen von SQL Server Express LocalDB.

Upgrade von Datenbankschemas

Wenn Sie ein Upgrade auf ein neues CU durchführen, werden evtl. einige Datenbankschemas aktualisiert. In der folgenden Tabelle sind die Datenbankschemas aufgeführt, die aktualisiert werden:

From\To	1912 CU1	1912 CU2	1912 CU3	1912 CU4	1912 CU5	1912 CU6	1912 CU7	1912 CU8
7.15 RTM/CU	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; logging	Site; Monitor; Config; logging
1912 RTM	Config	Site; Config	Site; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config
1912 CU1		Site; Config	Site; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config
1912 CU2			Site; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config
1912 CU3				Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config
1912 CU4					Site; Config	Site; Config	Site; Config	Site; Monitor; Config
1912 CU5						Site; Config	Site; Config	Site; Monitor; Config
1912 CU6							Config	Monitor; Config
1912 CU7								Monitor; Config

Begriffsdefinitionen:

- Site: Sitedatenspeicher Das Datenbankschema des Sitedatenspeichers wird aktualisiert.
- Überwachung: Überwachungsdatenspeicher. Das Datenbankschema des Überwachungsdatenspeichers wird aktualisiert.
- Konfiguration: Konfigurationstabelle. Desktop Studio-Version, Lizenzinformationen oder beides wird in der Sitekonfiguration aktualisiert.
- Protokollierung: Protokollierungsdatenspeicher. Das Datenbankschema des Protokollierungsdatenspeichers wird aktualisiert.

Upgrade von VDAs auf 1912 oder höher

Wurde die PvD-Komponente (persönliche vDisk) jemals auf einem VDA installiert, kann dieser nicht auf Version 1912 LTSR oder höher aktualisiert werden. Um den neuen VDA zu verwenden, müssen Sie den bestehenden VDA deinstallieren und dann den neuen VDA installieren.

Die ist auch dann erforderlich, wenn Sie PvD nie verwendet haben.

Wie PvD eventuell in früheren Versionen installiert wurde:

- Auf der grafischen Benutzeroberfläche des VDA-Installationsprogramms war PvD eine Option (Kontrollkästchen auf der Seite **Zusätzliche Komponenten**). In den 7.x-Versionen bis 7.15 LTSR war diese Option standardmäßig aktiviert. Wenn Sie die Standardeinstellungen akzeptiert haben (oder die Option in einem Release explizit aktiviert haben), wurde PvD installiert.
- In der Befehlszeile wurde PvD über die Option `/baseimage` installiert. Wenn Sie diese Option angegeben oder ein Skript verwendet haben, das diese Option enthielt, wurde PvD installiert.

Wenn Sie nicht wissen, ob auf Ihrem VDA PvD installiert ist, führen Sie das Installationsprogramm für den neuen VDA (1912 LTSR oder höher) auf der Maschine bzw. dem Image aus.

- Wenn PvD installiert ist, weist eine Meldung darauf hin, dass eine inkompatible Komponente vorhanden ist.
  - Klicken Sie auf der grafischen Benutzeroberfläche auf der Seite mit der Meldung auf **Abbrechen** und bestätigen Sie, dass Sie das Installationsprogramm schließen möchten.
  - Wenn Sie die Befehlszeile verwenden, schlägt der Befehl unter Anzeige der Meldung fehl.
- Wenn PvD nicht installiert ist, wird das Upgrade fortgesetzt.

Aktion

Wenn PvD auf dem VDA nicht installiert ist, folgen Sie dem normalen Upgradeverfahren.

Wenn PvD auf dem VDA installiert ist, gehen Sie folgendermaßen vor:

1. Deinstallieren Sie den VDA. Einzelheiten finden Sie unter Entfernen von Komponenten.
2. Installieren Sie den neuen VDA.

Wenn Sie PvD auf Windows 7- oder Windows 10-Maschinen (bis 1607 ohne Updates) weiterverwenden möchten, ist VDA 7.15 LTSR die neueste unterstützte Version.

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.

- **Early Release- oder Technology Preview-Versionen:** Sie können kein Upgrade einer Early Release-, Technology Preview- oder Preview-Version durchführen.

- **Komponenten unter älteren Betriebssystemen:** Sie können keine aktuellen VDAs unter Betriebssystemen installieren, die nicht mehr von Microsoft oder Citrix unterstützt werden. Weitere Informationen finden Sie unter Ältere Betriebssysteme.

- **Heterogene Umgebungen:** Wenn Sie Sites einer früheren Version neben Sites der aktuellen Version beibehalten müssen, lesen Sie die Hinweise zu heterogenen Umgebungen.

- **Produktauswahl:** Beim Upgrade einer älteren Version legen Sie nicht das Produkt (Citrix Virtual Apps oder Citrix Virtual Apps and Desktops) fest, das bei der Installation festgelegt wurde.

Hinweise zu heterogenen Umgebungen

Für ein Upgrade empfiehlt Citrix, dass Sie alle Komponenten und VDAs aktualisieren, damit Sie alle neuen und verbesserten Features der Edition und Version verwenden können.

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.

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. (Dies wird als Funktionsebene bezeichnet.) Standardmäßig gibt diese Einstellung die empfohlene VDA-Mindestversion an. Der Standardwert ist für die meisten Bereitstellungen ausreichend. Erwägen Sie nur dann, für die Einstellung eine frühere Version zu wählen, wenn der Katalog VDAs enthält, die älter als der Standardwert sind. Die Verwendung mehrerer VDA-Versionen in einem Maschinenkatalog wird nicht empfohlen.

Wenn ein Maschinenkatalog mit der standardmäßig VDA-Mindestversionseinstellung erstellt wird und auf Maschinen 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.

Mehrere Sites mit verschiedenen Versionen

Wenn Ihre Umgebung Sites mit mehreren Produktversionen enthält (z. B eine XenDesktop-Site der Version 7.18 und eine Citrix Virtual Apps and Desktops 1909-Site) empfiehlt Citrix die Verwendung von StoreFront zum Aggregieren von Anwendungen und Desktops aus den unterschiedlichen Produktversionen. 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.

Ältere Betriebssysteme

Angenommen, Sie haben eine frühere Version einer Komponente auf einer Maschine installiert, auf der eine unterstützte Betriebssystemversion ausgeführt wurde. Jetzt möchten Sie eine neuere Version der Komponente verwenden, doch das Betriebssystem wird für diese aktuelle Version nicht mehr unterstützt.

Beispielsweise haben Sie einen VDA für Serverbetriebssysteme unter Windows Server 2008 R2 installiert. Sie möchten diesen VDA auf die aktuelle Version aktualisieren, diese unterstützt jedoch Windows Server 2008 R2 nicht.

Wenn Sie versuchen, eine Komponente unter einem Betriebssystem zu installieren oder zu aktualisieren, das nicht länger zulässig ist, wird eine Fehlermeldung angezeigt (kann nicht unter diesem Betriebssystem installiert werden).

Dies gilt für das Upgrade auf aktuelle Releases und Long Term Service Releases. (Es gilt nicht für die Anwendung von CUs auf LTSR.)

Folgen Sie den Links, um zu erfahren, welche Betriebssysteme unterstützt werden.

- (Wählen Sie Ihre LTSR-Version auf der Hauptseite der Citrix Virtual Apps and Desktops-Produktdokumentation.)
  - Systemanforderungen.
  - Komponentenlisten in den Artikeln unter Neue Features.
- Aktuelle Releases (CR):
  - Delivery Controller, Studio, Director, VDAs, universeller Druckserver
  - Verbundauthentifizierungsdienst
  - Informationen zu StoreFront, Self-Service-Kennwortzurücksetzung und Sitzungsaufzeichnung finden Sie in dem Artikel zu den Systemanforderungen für die aktuelle Version.

Ungültige Betriebssysteme

Die Tabelle unten enthält die früheren Betriebssysteme, die für Installation/Upgrades von Komponenten der aktuellen Version nicht gültig sind. Es wird die jeweils letzte gültige Komponentenversion aufgeführt, die für jedes Betriebssystem unterstützt wird, und die Komponentenversion, ab der das Betriebssystem für Installation und Upgrades ungültig ist.

Die Betriebssysteme in der Tabelle enthalten Service Packs und Updates.

Betriebssystem	Komponente/Feature	Letzte gültige Version	Installation/Upgrade nicht möglich ab Version
Windows 7 und Windows 8	VDA	7.15 LTSR	7.16
Windows 7 und Windows 8	Andere Komponenten	7.17	7.18
Windows 10-Versionen vor 1607	VDA	7.15 LTSR	7.16
Windows 10 x86	VDA	1906.2.0	1909
Windows Server 2008 R2	VDA	7.15 LTSR	7.16
Windows Server 2008 R2	Andere Komponenten	7.17	7.18
Windows Server 2012	VDA	7.15 LTSR	7.16
Windows Server 2012	Andere Komponenten	7.17	7.18
Windows Server 2012 R2	Andere Komponenten*	1912 LTSR	2003
Windows Server 2012 R2	Server-VDI	7.15 LTSR	7.16

Windows XP und Windows Vista sind für Komponenten und Technologien der Version 7.x nicht gültig.

*Gilt für Delivery Controller, Studio, Director und VDAs.

Möglichkeiten

Sie haben verschiedene Möglichkeiten. Sie haben folgende Möglichkeiten:

- Aktuelles Betriebssystem weiterverwenden

- Reimaging oder Upgrade der Maschine
- Neue Maschinen hinzufügen und dann alte Maschinen entfernen

Aktuelles Betriebssystem weiterverwenden Dies ist bei VDAs möglich. Wenn Sie Maschinen mit dem früheren Betriebssystem weiter verwenden möchten, stehen Ihnen folgende Optionen zur Auswahl:

- Verwenden Sie weiterhin die installierte Komponentenversion.
- Laden Sie die neueste gültige Komponentenversion herunter und aktualisieren Sie Ihre Komponente dann auf diese Version. (Dies setzt voraus, dass die letzte gültige Komponentenversion nicht bereits installiert ist.)

Angenommen, Sie führen einen VDA der Version 7.14 unter Windows 7 SP1 aus. Die letzte gültige VDA-Version unter Windows 7 ist XenApp und XenDesktop 7.15 LTSR. Sie können entweder Version 7.14 weiter verwenden oder einen VDA der Version 7.15 LTSR herunterladen und Ihren VDA auf diese Version aktualisieren. Diese früheren VDA-Versionen funktionieren in Bereitstellungen, die Delivery Controller in neueren Versionen enthalten. Ein VDA der Version 7.15 LTSR kann beispielsweise eine Verbindung mit einem Controller von Citrix Virtual Apps and Desktops 7 1808 herstellen.

Reimaging oder Upgrade der Maschine Dies ist bei VDAs und andere Maschinen möglich, auf denen keine Kernkomponenten (z. B. Delivery Controller) installiert sind. Wählen Sie eine der folgenden Optionen:

- Nachdem Sie die Maschine außer Betrieb genommen haben (Wartungsmodus aktivieren und warten, bis alle Sitzungen beendet sind), können Sie ein Reimaging auf eine unterstützte Windows-Betriebssystemversion durchführen und anschließend die neueste Version der Komponente installieren.
- Um das Betriebssystem ohne Reimaging zu aktualisieren, deinstallieren Sie zunächst die Citrix Software. Andernfalls nimmt die Citrix Software einen nicht unterstützten Zustand an. Installieren Sie dann die neue Komponente.

Neue Maschinen hinzufügen und dann alte Maschinen entfernen Diese Methode eignet sich, wenn Sie das Betriebssystem auf Maschinen mit einem Delivery Controller oder einer anderen Kernkomponente aktualisieren müssen.

Citrix empfiehlt, dass alle 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. Beispiel: Installieren Sie einen Controller auf zwei Windows Server 2016-Maschinen.
3. Fügen Sie der Site die neuen Controller hinzu.
4. Entfernen Sie die Controller, die unter nicht mehr gültigen Betriebssystemen ausgeführt werden. Beispiel: Installieren Sie einen Controller von zwei Windows Server 2008 R2-Maschinen. Folgen Sie den Empfehlungen zum Entfernen von Controllern unter Delivery Controller.

Vorbereitung

Lesen Sie vor Upgrades die folgenden Informationen und führen Sie die erforderlichen Aufgaben aus.

Wählen von Installationsprogramm und Schnittstelle

Verwenden Sie das Komplettinstallationsprogramm auf dem Produkt-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.

Einzelheiten zur Installation: Nachdem Sie alle Vorbereitungen abgeschlossen haben und bereit sind, das Installationsprogramm zu starten, zeigt Ihnen der Installationsartikel, was Sie sehen (wenn Sie die grafische Benutzeroberfläche verwenden) oder was Sie eingeben (wenn Sie die Befehlszeilenschnittstelle verwenden).

- Installieren/Aktualisieren von Kernkomponenten über die grafische Oberfläche
- Installieren/Aktualisieren von Kernkomponenten über die Befehlszeile
- Installieren/Aktualisieren von VDAs über die grafische Oberfläche
- Installieren/Aktualisieren von VDAs über die Befehlszeile

Wenn Sie einen Einzelsitzungs-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.

Beim Upgrade eines VDAs auf dieses Release wird ein Neustart der Maschine durchgeführt. Dieses Erfordernis besteht seit Version 7.17. und ist unvermeidlich. Das Upgrade wird nach dem Neustart automatisch fortgesetzt (es sei denn, Sie haben an der Befehlszeile `/noresume` angegeben).

Datenbankaktionen

Sichern Sie die Site-, Überwachungs- und der Konfigurationsprotokollierungsdatenbank. Folgen Sie den Anweisungen unter CTX135207. Wenn nach dem Upgrade Probleme entdeckt werden, können Sie das Backup wiederherstellen.

Weitere Informationen zum Aktualisieren nicht mehr unterstützter SQL Server-Versionen finden Sie unter SQL Server-Versionsprüfung. (Bezieht sich auf den SQL Server, der für die Site-, Überwachungs- und Konfigurationsprotokollierungsdatenbank verwendet wird.)

SQL Server Express LocalDB wird automatisch zur Verwendung mit dem lokalen Hostcache installiert. Wenn Sie eine frühere Version ersetzen müssen, muss die neue Version mindestens SQL Server Express 2017 LocalDB CU16 sein. Weitere Informationen zum Ersetzen von SQL Server Express LocalDB durch eine neue Version nach dem Upgrade der Komponenten und der Site finden Sie unter Ersetzen von SQL Server Express LocalDB.

Überprüfen des Stands der Citrix Lizenzierung

Einen umfassenden Überblick über die Verwaltung der Citrix Lizenzierung finden Sie unter Activate, upgrade, and manage Citrix licenses.

Sie können das vollständige Produktinstallationsprogramm verwenden, um den Lizenzserver zu aktualisieren. Sie können die Lizenzkomponenten auch separat herunterladen und aktualisieren. Siehe Upgrade.

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 2019.1115 sein.

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 `XenDesktopServerSetup.exe` vom ISO-Layout auf der Maschine mit einem Delivery Controller aus. Eventuelle Kompatibilitätsprobleme werden vom Installationsprogramm zusammen mit den empfohlenen Schritten zur Behebung gemeldet.
- Führen Sie im `XenDesktop Setup`-Verzeichnis auf dem Installationsmedium den Befehl `.\LicServVerify.exe -h <license-server-fqdn> -p 27000 -v` aus. Es wird dann angezeigt, ob der Lizenzserver kompatibel ist. Wenn der Lizenzserver nicht kompatibel ist, aktualisieren Sie ihn.

Backup aller Änderungen an StoreFront

Wenn Sie Änderungen an Dateien in `C:\inetpub\wwwroot\Citrix\<StoreName>\App_Data` wie *default.ica* und *usernamepassword.tfrm* gemacht haben, legen Sie für jeden Store vor einem Upgrade ein Backup an. Nach dem Upgrade können Sie sie wiederherstellen, um Ihre Änderungen wieder anzuwenden.

Schließen von Anwendungen und Konsolen

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 der Skripts über Studio aus. Der Datenbankadministrator führt weitere Skripts mit einem Tool wie SQL Server Management Studio aus.

Andere Vorbereitungsaufgaben

- Falls erforderlich, sichern Sie Vorlagen und aktualisieren Sie Hypervisors.
- Erledigen Sie sämtliche anderen, zur Gewährleistung der Betriebskontinuität erforderlichen Vorbereitungsaufgaben.

Sitetests zur Vorbereitung

Wenn Sie Delivery Controller und eine Site aktualisieren, werden vor dem eigentlichen Upgrade Vorbereitungstests an der Site ausgeführt. Dadurch wird Folgendes geprüft:

- Die Sitedatenbank ist erreichbar und wurde gesichert.
- Verbindungen mit wichtigen Citrix-Diensten funktionieren ordnungsgemäß.
- Die Citrix Lizenzserver-Adresse ist verfügbar.
- Die Konfigurationsprotokollierungsdatenbank ist erreichbar.

Nachdem die Tests ausgeführt wurden, können Sie einen Bericht mit den Ergebnissen anzeigen. Anschließend können Sie eventuelle Probleme beheben und die Tests wiederholen. Wenn Sie die Vorbereitungstests und die Problembehebung nicht ausführen, kann sich dies auf die Funktionsweise Ihrer Site auswirken.

Der Bericht mit dem Testergebnis wird als HTML-Datei (`PreliminarySiteTestResult.html`) im Verzeichnis der Installationsprotokolle gespeichert. Die Datei wird erstellt, wenn sie nicht vorhanden ist. Wenn die Datei existiert, wird ihr Inhalt überschrieben.

Ausführen der Tests

- Wenn Sie die grafische Benutzeroberfläche des Installationsprogramms zum Aktualisieren verwenden, können Sie über eine Seite des Assistenten die Tests starten und den Bericht anzeigen. Nachdem die Tests ausgeführt wurden und Sie den Bericht angezeigt und alle ggf. gefundenen Probleme gelöst haben, können Sie die Tests erneut ausführen. Wenn die Tests bestanden werden, klicken Sie auf "Weiter", um mit dem Assistenten fortzufahren.
- Bei Upgrades über die Befehlszeilenschnittstelle werden die Tests automatisch ausgeführt. Wird ein Test nicht bestanden, wird das Upgrade in der Standardeinstellung nicht durchgeführt. Nachdem Sie den Bericht angezeigt und Probleme behoben haben, führen Sie den Befehl erneut aus.

Citrix empfiehlt, vor Upgrades von Controller und Site immer die Vorbereitungstests auszuführen und alle Probleme zu beheben. Der potentielle Nutzen überwiegt den geringen Zeitaufwand für die Tests. Sie können diese empfohlene Aktion jedoch außer Kraft setzen.

- Bei Upgrades über die grafische Benutzeroberfläche können Sie die Tests überspringen.
- Bei Upgrades über die Befehlszeile können Sie die Tests nicht überspringen. Standardmäßig führt ein nicht bestandener Sitetest dazu, dass das Installationsprogramm fehlschlägt und kein Upgrade durchgeführt wird. In den meisten Fällen werden bei Verwendung der Option `/ignore_site_test_failure` Sitetestfehler ignoriert und das Upgrade wird fortgesetzt. (Informationen zu Ausnahmen finden Sie unter SQL Server-Versionsprüfung.)

Upgrade mehrerer Controller

Wenn Sie das Upgrade eines Controllers starten und anschließend das Upgrade eines weiteren Controllers in derselben Site (vor Abschluss des ersten Upgrades), gilt Folgendes:

- Wenn die Vorbereitungstests am ersten Controller abgeschlossen wurden, wird die Seite für Vorbereitungstests nicht im Assistenten für den zweiten Controller angezeigt.
- Wenn die Tests auf dem ersten Controller noch laufen, wenn Sie das zweite Upgrade starten, wird die Seite für Vorbereitungstests im Assistenten für diesen angezeigt. Nach Abschluss der Tests des ersten Controllers werden allerdings nur die diesen betreffenden Testergebnisse gespeichert.

Nicht mit der Siteintegrität zusammenhängende Testfehler

- Wenn die Vorbereitungstests aufgrund Arbeitsspeichermangel fehlschlagen, stellen Sie mehr Arbeitsspeicher zur Verfügung und führen Sie die Tests dann erneut aus.
- Wenn Sie eine Berechtigung für Upgrades aber nicht für Sitetests haben, schlagen die Vorbereitungstests fehl. Führen Sie in diesem Fall das Installationsprogramm mit einem Benutzerkonto aus, das über die Berechtigung zum Ausführen der Tests verfügt.

SQL Server-Versionsprüfung

Die Bereitstellung von Citrix Virtual Apps and Desktops erfordert eine unterstützte Version von Microsoft SQL Server für die Site-, Überwachungs- und Konfigurationsprotokollierungsdatenbank. Ein Upgrade einer Citrix Bereitstellung mit einer nicht mehr unterstützten SQL Server-Version, kann zu Funktionsstörungen führen, außerdem erlischt der Support für die Site.

Informationen zu den für den jeweiligen Citrix Release unterstützten SQL Server-Versionen finden Sie im Artikel Systemanforderungen der Releasedokumentation.

Beim Upgrade eines Controllers überprüft das Citrix Installationsprogramm die aktuell für die Site-, Überwachungs- und Konfigurationsprotokollierungsdatenbank verwendete SQL Server-Version.

- Falls bei der Überprüfung festgestellt wird, dass die aktuell installierte SQL Server-Version von dem Citrix-Release auf das sie aktualisieren nicht unterstützt wird:
  - Grafische Oberfläche: Das Upgrade wird mit einer Meldung angehalten. Klicken Sie auf **Ich verstehe** und dann auf **Abbrechen**, um das Citrix-Installationsprogramm zu schließen. (Sie können das Upgrade nicht fortsetzen.)
  - Befehlszeilenschnittstelle: Der Befehl schlägt fehl (selbst mit der Option /`ignore_db_check_fail`).

  Aktualisieren Sie die SQL Server-Version und starten Sie das Citrix Upgrade erneut.
- Kann die Überprüfung die installierte SQL Server-Version nicht ermitteln, sehen Sie nach, ob sie von dem Release, auf das Sie aktualisieren, unterstützt wird (unter Systemanforderungen).
  - Grafische Oberfläche: Das Upgrade wird mit einer Meldung angehalten.

    * Wird die installierte SQL Server-Version unterstützt, klicken Sie auf **Ich verstehe**, um die Meldung zu schließen, und dann auf **Weiter**, um mit dem Citrix-Upgrade fortzufahren.
    * Wenn die installierte SQL Server-Version nicht unterstützt wird, klicken Sie auf **Ich verstehe**, um die Meldung zu schließen, und dann auf **Abbrechen**, um das Citrix-Upgrade abzubrechen. Aktualisieren Sie die SQL Server-Version auf eine unterstützte Version und starten Sie das Citrix-Upgrade neu.

- Befehlszeilenschnittstelle: Der Befehl schlägt mit einer Meldung fehl. Nach dem Schließen der Meldung:

    * Wenn die installierte SQL Server-Version unterstützt wird, führen Sie den Befehl erneut mit der Option `/ignore_db_check_failure` aus.
    * Wenn die installierte SQL Server-Version nicht unterstützt wird, aktualisieren Sie sie auf eine unterstützte Version. Führen Sie den Befehl erneut aus, um das Citrix Upgrade zu starten.

Upgrade von SQL Server

Wenn Sie neue SQL Server-Server einrichten und die Sitedatenbank migrieren, müssen die Verbindungszeichenfolgen aktualisiert werden.

Verwendet die Site aktuell SQL Server Express (von Citrix bei der Siteerstellung automatisch installiert) gehen Sie folgendermaßen vor:

1. Installieren Sie die aktuelle SQL Server Express-Version.
2. Trennen Sie die Datenbank.
3. Fügen Sie die Datenbank an das neue SQL Server Express an.
4. Migrieren Sie die Verbindungszeichenfolgen.

Weitere Informationen finden Sie unter Konfigurieren von Verbindungszeichenfolgen und in der Microsoft-Dokumentation zu SQL Server.

Ersetzen von SQL Server Express LocalDB

Microsoft SQL Server Express LocalDB wird vom lokalen Hostcache auf Standalone-Basis verwendet wird. Der lokale Hostcache erfordert keine anderen Komponenten von SQL Server Express als SQL Server Express LocalDB.

Wenn Sie einen Delivery Controller einer Version vor 1912 installiert haben und die Bereitstellung auf Version 1912 oder höher aktualisieren, aktualisiert Citrix die SQL Server Express LocalDB-Version nicht automatisch. Warum? Weil es möglicherweise Nicht-Citrix-Komponenten gibt, die SQL Server Express

LocalDB benötigen. Wenn Sie Nicht-Citrix-Komponenten haben, die SQL Server Express LocalDB verwenden, stellen Sie sicher, dass ein Upgrade von SQL Server Express LocalDB die Ausführung dieser Komponenten nicht beeinträchtigt. Um SQL Server Express LocalDB zu aktualisieren (bzw. zu ersetzen), folgen Sie den Anweisungen in diesem Abschnitt.

- **Beim Upgrade von Delivery Controllern auf Citrix Virtual Apps and Desktops Version 1912, 1912 LTSR oder 2003** ist das Upgrade von SQL Server Express LocalDB optional. Der lokale Hostcache funktioniert ordnungsgemäß, unabhängig davon, ob Sie SQL Server Express LocalDB aktualisieren. Citrix hat die Option des Umstiegs auf eine neuere SQL Server Express LocalDB-Version bereitgestellt für den Fall, dass eine Einstellung des Supports für SQL Server Express LocalDB 2014 durch Microsoft Bedenken auslöst.
- **Beim Upgrade von Delivery Controllern auf Citrix Virtual Apps and Desktops-Versionen über 2003** ist die unterstützte Mindestversion SQL Server Express 2017 LocalDB CU 16. Wenn Sie ursprünglich einen Delivery Controller einer Version vor 1912 installiert hatten und SQL Server Express LocalDB seitdem nicht durch eine neuere Version ersetzt haben, müssen Sie diese Datenbanksoftware jetzt ersetzen. Andernfalls funktioniert der lokale Hostcache nicht.

Sie benötigen Folgendes:

- Das Installationsmedium für die Version von Citrix Virtual Apps and Desktops, auf die Sie ein Update ausgeführt haben. Das Medium enthält ein Exemplar von Microsoft SQL Server Express LocalDB 2017 CU 16.
- Das Windows-Tool Sysinternals, das Sie von Microsoft herunterladen können.

Verfahren:

1. Führen Sie ein Upgrade der Komponenten, Datenbanken und Site von Citrix Virtual Apps and Desktops aus. (Die Upgrades haben Auswirkungen auf die Site-, Überwachungs- und der Konfigurationsprotokollierungsdatenbank. Sie haben keine Auswirkungen auf die Datenbank des lokalen Hostcaches, welcher SQL Server Express LocalDB verwendet.)
2. Laden Sie `PsExec` von Microsoft auf den Delivery Controller herunter. Siehe PsExec v2.2 in der Microsoft-Dokumentation.
3. Beenden Sie den Citrix Dienst für hohe Verfügbarkeit.
4. Führen Sie an einer Eingabeaufforderung `PsExec` aus und wechseln Sie zum Netzwerkdienstkonto.

   ```
   psexec -i -u "NT AUTHORITY\NETWORK SERVICE"cmd
   ```

   Optional können Sie mit `whoami` überprüfen, ob die Eingabeaufforderung unter dem Netzwerkdienstkonto ausgeführt wird.

   ```
   whoami
   nt authority\network service
   ```


5. Wechseln Sie in den Ordner mit SqlLocalDB.

   ```
   cd "C:\Program Files\Microsoft SQL Server\120\Tools\Binn"
   ```

6. Beenden und löschen Sie `CitrixHA` (LocalDB).

   ```
   SqlLocalDB stop CitrixHA

   SqlLocalDB delete CitrixHA
   ```

7. Entfernen Sie die zugehörigen Dateien aus `C:\Windows\ServiceProfiles\NetworkService`.

   ```
   1 HADatabaseName.*
   2 HADatabaseName_log.*
   3 HAImportDatabaseName.*
   4 HAImportDatabaseName_log.*
   5 <!--NeedCopy-->
   ```

   Tipp: In Ihrer Bereitstellung gibt es `HAImportDatabaseName.*` und `HAImportDatabaseName_log.*` möglicherweise nicht.

8. Deinstallieren Sie SQL Server Express LocalDB 2014 vom Server mit dem Windows-Feature zum Entfernen von Programmen.

9. Installieren Sie SQL Server Express LocalDB 2017. Doppelklicken Sie im Ordner `Support > SQLLocalDB` auf dem Installationsmedium für Citrix Virtual Apps and Desktops auf `sqllocaldb.msi`. Möglicherweise wird ein Neustart angefordert, um die Installation abzuschließen. (Die neue SQLLocalDB ist in `C:\Program Files\Microsoft SQL Server\140\Tools\Binn`.)

10. Starten Sie den Citrix Dienst für hohe Verfügbarkeit.

11. Stellen Sie sicher, dass die lokale Hostcachedatenbank auf jedem Delivery Controller erstellt wurde. Dadurch wird bestätigt, dass der Dienst für hohe Verfügbarkeit (sekundärer Broker) bei Bedarf übernehmen kann.

    - Gehen Sie auf dem Controller-Server zu `C:\Windows\ServiceProfiles\NetworkService`.
    - Überprüfen Sie, ob `HaDatabaseName.mdf` und `HaDatabaseName_log.ldf` erstellt wurden.

Upgrade eines XenApp 6.5-Workers auf einen neuen VDA

September 19, 2023

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, das Betriebssystem aktualisieren und dann einen neuen VDA für Serverbetriebssysteme installieren.

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. 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. Aktualisieren Sie das Betriebssystem des Servers auf eine unterstützte Version. Eine Liste der unterstützten Plattformen finden Sie im Abschnitt "VDA für Serverbetriebssystem"unter Systemanforderungen.
4. 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

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) .NET Framework 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 Serverbetriebssysteme.

Migrieren von XenApp 6.x

March 15, 2022

> **Wichtig:**
>
> Durch Migration werden Daten von einer früheren Bereitstellung auf eine neuere Version verschoben. Dies umfasst die Installation neuerer 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.
>
> Open-Source-Migrationsskripts sind auf https://github.com/citrix/xa65migrationtool verfügbar. Citrix unterstützt diese Skripts jedoch nicht.
>
> Der Rest dieses Artikels enthält Informationen, die als Referenz für die Open-Source-Migrationsskripts verwendet werden können.

Einführung

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. Weitere Informationen finden Sie unter Upgrade einer Bereitstellung.

Informationen zu Änderungen an Architektur, Komponenten und Features in den 7.x-Versionen finden Sie unter Änderungen in Version 7.x.

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. Details werden später erläutert.

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/oder Farmdaten in XML-Dateien.

2. 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.
3. Auf dem XenApp 7.6-Controller:

a) Importieren Sie die PowerShell-Importmodule.
b) Importieren Sie mit den Import-Cmdlets die Richtlinien- und/oder Farmdaten (Anwendungen), wobei Sie die XML-Dateien als Eingabe verwenden.

4. 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.

Migrationstoolpaket

Das Migrationstool enthält zwei separate, unabhängige Pakete:

- **ReadIMA** 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

Modul bzw. Datei	Beschreibung
XmlUtilities.psd1	PowerShell-Manifestdatei für das Skriptmodul XmlUtilities.psm1.
XmlUtilities.psm1	Freigegebenes PowerShell-Skriptmodul mit XML-Funktionen

- **ImportFMA** 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). Weitere Informationen hierzu finden Sie unter 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. Citrix Richtlinieneinstellungen, die mit Windows Gruppenrichtlinienobjekten erstellt wurden, 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. Benutzernamen, Servernamen und andere XenApp-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 und oft als Warnung gemeldet, während die Skriptausführung fortgesetzt wird. 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 sollten die grundlegenden PowerShell-Konzepte der Ausführungsrichtlinie, Module, Cmdlets und Skripts verstehen. Obwohl umfangreiche Erfahrung in der Erstellung 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 Dokumentation in den eDocs.
- 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.

    Die Symboldatendateien in diesem Ordner sind TXT-Dateien, die nach den Browsernamen der veröffentlichten Anwendungen benannt sind (die Dateien sind zwar TXT-Dateien, die gespeicherten Daten sind jedoch verschlüsselte binäre Symboldaten, die vom Importskript zum erneuten Erstellen des Anwendungssymbols gelesen werden können). 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. Beispiel: Export-XAFarm ist ein Cmdlet. ExportXAFarm.psd1 und ExportXAFarm.psm1 sind Dateien, die nicht ausgeführt werden können.
- In den nachfolgenden schrittweisen Anleitungen sind die meisten Parameterwerte für <string> mit Anführungszeichen versehen. Diese sind optional für Zeichenfolgen, die nur aus einem Wort

bestehen.

Export des XenApp 6.x-Servers

- 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 Windows-Berechtigungen zum Ausführen von PowerShell-Skripts verfügen. Schrittweise Anleitungen finden Sie unten.
- 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 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 auf einer funktionierenden Farm ausführen, die aktive Benutzerverbindungen hat. Die Exportskripts lesen nur die statische Farmkonfiguration und die Richtliniendaten.

Importieren auf den XenApp 7.6-Server

- 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 Windows-Berechtigungen zum Ausführen von PowerShell-Skripts verfügen. Schrittweise Anleitungen finden Sie unten.
- 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. In

den Protokollen wird genau angegeben, was während eines tatsächlichen Importvorgangs passieren würde. Wenn Fehler auftreten, können Sie diese beheben, bevor Sie einen tatsächlichen Import durchführen.

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. Sie sollten nun zwei ZIP-Dateien haben: 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. Beispiel: `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. Beispiel: `Set-ExecutionPolicy RemoteSigned`.
7. Importieren der Moduldefinitionsdateien “ExportPolicy.psd1”und “ExportXAFarm.psd1”: `Import-Module .\\ExportPolicy.psd1` und `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 Richtlinien- und Farmdaten die folgenden Cmdlets aus.

Richtliniendaten: `Export-Policy`

Parameter	Beschreibung
-XmlOutputFile “*string*.xml”	Name der XML-Ausgabedatei. 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. Standardwert: Keiner. Dieser Parameter ist erforderlich.
-LogFile *string*	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”ebenfalls angegeben ist, wird ein Fehler generiert, sonst 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. Standardwert: False; Protokollausgabe wird erstellt
-NoClobber	Vorhandene Protokolldatei, die im Parameter “LogFile”angegeben wurde, nicht überschreiben. Wenn die Protokolldatei nicht vorhanden ist, hat dieser Parameter keine Auswirkung. Standardwert: False; eine vorhandene Protokolldatei wird überschrieben
-NoDetails	Keine ausführlichen Berichte zur Skriptausführung an die Konsole senden. Standardwert: False; ausführliche Berichte werden an der Konsole gesendet
-SuppressLogo	Meldung “XenApp 6.x to XenApp/XenDesktop 7.6 Migration Tool Version #yyyyMMdd-hhmm#” nicht auf Konsole drucken. Diese Meldung, in der die Skriptversion angegeben wird, kann bei der Problembehandlung hilfreich sein, daher empfiehlt Citrix, diesen Parameter wegzulassen. Standardwert: False; die Meldung wird auf der Konsole gedruckt

Beispiel: Das folgende Cmdlet exportiert Richtlinieninformationen in die XML-Datei “MyPolicies.xml”. Der Vorgang wird in der Datei “MyPolicies.log”protokolliert.

```
Export-Policy -XmlOutputFile ".\MyPolicies.XML"-LogFile ".\MyPolicies
.Log"
```

Farmdaten: `Export-XAFarm`

Parameter	Beschreibung
XmlOutputFile “*string*.xml”	Name der XML-Ausgabedatei. 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. Standardwert: Keiner. Dieser Parameter ist erforderlich.
-LogFile “*string*”	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”ebenfalls angegeben ist, wird ein Fehler generiert, sonst 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. Standardwert: False; Protokollausgabe wird erstellt
-NoClobber	Vorhandene Protokolldatei, die im Parameter “LogFile”angegeben wurde, nicht überschreiben. Wenn die Protokolldatei nicht vorhanden ist, hat dieser Parameter keine Auswirkung. Standardwert: False; eine vorhandene Protokolldatei wird überschrieben
-NoDetails	Keine ausführlichen Berichte zur Skriptausführung an die Konsole senden. Standardwert: False; ausführliche Berichte werden an der Konsole gesendet

Parameter	Beschreibung
-SuppressLogo	Meldung “XenApp 6.x to XenApp/XenDesktop 7.6 Migration Tool Version #yyyyMMdd-hhmm#” nicht auf Konsole drucken. Diese Meldung, in der die Skriptversion angegeben wird, kann bei der Problembehandlung hilfreich sein, daher empfiehlt Citrix, diesen Parameter wegzulassen. Standardwert: False; die Meldung wird auf der Konsole gedruckt
-IgnoreAdmins	Administratorinformationen nicht exportieren. Siehe Erweiterte Verwendung. Standardwert: False; Administratorinformationen werden exportiert
-IgnoreApps	Anwendungsinformationen nicht exportieren. Siehe Erweiterte Verwendung. Standardwert: False; Anwendungsinformationen werden exportiert
-IgnoreServers	Serverinformationen nicht exportieren. Standardwert: 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. Standardwert: False; andere Informationen werden exportiert Diese Option ermöglicht das Durchführen eines Exports, wenn ein Fehler vorliegt, der keine Auswirkungen auf die exportierten oder importierten Daten hat.
-AppLimit *integer*	Anzahl der Anwendungen, die exportiert werden. Siehe Anforderungen, Vorbereitungen und Best Practices. Standardwert: Alle Anwendungen werden exportiert

Parameter	Beschreibung
-EmbedIconData	Anwendungssymboldaten in die gleiche XML-Datei einbetten wie die anderen Objekte. Standard: Symbole werden separat gespeichert. Siehe Anforderungen, Vorbereitungen und Best Practices.
-SkipApps *integer*	Anzahl der Anwendungen, die übersprungen werden. Siehe Erweiterte Verwendung. Standardwert: Keine Anwendungen werden übersprungen

Beispiel: Das folgende Cmdlet exportiert Farminformationen in die XML-Datei "MyFarm.xml". Der Vorgang wird in der Datei "MyFarm.log"protokolliert. Ein Ordner mit dem Namen "MyFarm-icons"wird zum Speichern der Datendateien für die Anwendungssymbole erstellt. Dieser Ordner ist am gleichen Speicherort wie "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

Sie können eine Importvorschau ausführen (indem Sie das Cmdlet `Import-Policy` oder `Import-XAFarm` mit dem Preview-Parameter ausführen) und die Protokolldateien überprüfen, bevor Sie einen tatsächlichen Import ausführen.

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 sich die extrahierten Dateien aus ImportFMA.zip befinden.

4. Öffnen Sie eine PowerShell-Konsole und legen Sie das aktuelle Verzeichnis als Skriptspeicherort fest: `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. Beispiel: `Set-ExecutionPolicy RemoteSigned`.
7. Importieren Sie die PowerShell-Moduldefinitionsdateien "ImportPolicy.psd1"und "ImportXAFarm.psd1": `Import-Module .\\ImportPolicy.psd1` und `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. Führen Sie zum Importieren von Richtlinien- und Anwendungsdaten die folgenden Cmdlets aus.

Richtliniendaten: `Import-Policy`, unter Angabe der XML-Datei mit den exportierten Richtliniendaten.

Parameter	Beschreibung
-XmlInputFile "*string*.xml"	Name der XML-Eingabedatei. Diese Datei enthält Daten, die mit dem Cmdlet "Export-Policy" gesammelt wurden. Sie muss die Erweiterung .xml haben. Standardwert: Keiner. Dieser Parameter ist erforderlich.

Parameter	Beschreibung
-XsdFile “*string*”	Name der XSD-Datei. Mit dieser Datei überprüfen die Importskripts die Syntax der XML-Eingabedatei. Siehe Erweiterte Verwendung. Standardwert: PolicyData.XSD
-LogFile “*string*”	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. Standardwert: False; Protokollausgabe wird erstellt
-NoClobber	Vorhandene Protokolldatei, die im Parameter “LogFile”angegeben wurde, nicht überschreiben. Wenn die Protokolldatei nicht vorhanden ist, hat dieser Parameter keine Auswirkung. Standardwert: False; eine vorhandene Protokolldatei wird überschrieben
-NoDetails	Keine ausführlichen Berichte zur Skriptausführung an die Konsole senden. Standardwert: False; ausführliche Berichte werden an der Konsole gesendet
-SuppressLogo	Meldung “XenApp 6.x to XenApp/XenDesktop 7.6 Migration Tool Version #yyyyMMdd-hhmm#” nicht auf Konsole drucken. Diese Meldung, in der die Skriptversion angegeben wird, kann bei der Problembehandlung hilfreich sein, daher empfiehlt Citrix, diesen Parameter wegzulassen. Standardwert: False; die Meldung wird auf 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. Standardwert: False; ein echter Import wird ausgeführt

Beispiel: Mit dem folgenden Cmdlet werden Richtliniendaten aus der XML-Datei "MyPolicies.xml"importiert. Der Vorgang wird in der Datei "MyPolicies.log"protokolliert.

```
Import-Policy -XmlInputFile ".\MyPolicies.XML"-LogFile ".\MyPolicies.Log"
```

Anwendungen: `Import-XAFarm` unter Angabe der XML-Datei mit den exportierten Farmdaten.

Parameter	Beschreibung
-XmlInputFile "*string*.xml"	Name der XML-Eingabedatei. Diese Datei enthält Daten, die mit dem Cmdlet "Export-XAFarm" gesammelt wurden. Sie muss die Erweiterung .xml haben. Standardwert: Keiner. Dieser Parameter ist erforderlich.
-XsdFile "*string*"	Name der XSD-Datei. Mit dieser Datei überprüfen die Importskripts die Syntax der XML-Eingabedatei. Siehe Erweiterte Verwendung. Standardwert: XAFarmData.XSD
-LogFile "*string*"	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. Standardwert: False; Protokollausgabe wird erstellt
-NoClobber	Vorhandene Protokolldatei, die im Parameter “LogFile”angegeben wurde, nicht überschreiben. Wenn die Protokolldatei nicht vorhanden ist, hat dieser Parameter keine Auswirkung. Standardwert: False; eine vorhandene Protokolldatei wird überschrieben
-NoDetails	Keine ausführlichen Berichte zur Skriptausführung an die Konsole senden. Standardwert: False; ausführliche Berichte werden an der Konsole gesendet
-SuppressLogo	Meldung “XenApp 6.x to XenApp/XenDesktop 7.6 Migration Tool Version #yyyyMMdd-hhmm#” nicht auf Konsole drucken. Diese Meldung, in der die Skriptversion angegeben wird, kann bei der Problembehandlung hilfreich sein, daher empfiehlt Citrix, diesen Parameter wegzulassen. Standardwert: False; die Meldung wird auf 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. Standardwert: False; ein echter Import wird ausgeführt
-DeliveryGroupName “*string*”	Bereitstellungsgruppenname für alle importierten Anwendungen. Siehe Erweiterte Verwendung. Standardwert: “** - Delivery Group”

Parameter	Beschreibung
-MatchFolder "*string*"	Import von Anwendungen in Ordnern, deren Namen mit der Zeichenfolge (String) übereinstimmen. Siehe Erweiterte Verwendung. Standardwert: Keine Übereinstimmung
-NotMatchFolder "*string*"	Import von Anwendungen in Ordnern, deren Namen mit der Zeichenfolge (String) nicht übereinstimmen. Siehe Erweiterte Verwendung. Standardwert: Keine Übereinstimmung
-MatchServer "*string*"	Import von Anwendungen auf Servern, deren Namen mit der Zeichenfolge (String) übereinstimmen. Siehe Erweiterte Verwendung.
-NotMatchServer "*string*"	Import von Anwendungen auf Servern, deren Namen nicht mit der Zeichenfolge (String) übereinstimmen. Siehe Erweiterte Verwendung. Standardwert: Keine Übereinstimmung
-MatchWorkerGroup "*string*"	Import von Anwendungen, die für Workergruppen veröffentlicht wurden und deren Namen mit der Zeichenfolge (String) übereinstimmen. Siehe Erweiterte Verwendung. Standardwert: Keine Übereinstimmung
-NotMatchWorkerGroup "*string*"	Import von Anwendungen, die für Workergruppen veröffentlicht wurden und deren Namen nicht mit der Zeichenfolge (String) übereinstimmen. Siehe Erweiterte Verwendung. Standardwert: Keine Übereinstimmung
-MatchAccount "*string*"	Import von Anwendungen, die für Benutzerkonten veröffentlicht wurden und deren Namen mit der Zeichenfolge (String) übereinstimmen. Siehe Erweiterte Verwendung. Standardwert: Keine Übereinstimmung
-NotMatchAccount "*string*"	Import von Anwendungen, die für Benutzerkonten veröffentlicht wurden und deren Namen nicht mit der Zeichenfolge (String) übereinstimmen. Siehe Erweiterte Verwendung. Standardwert: Keine Übereinstimmung

Parameter	Beschreibung
-IncludeStreamedApps	Import von 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"
```

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. Die Werte der Einstellungen sollten gleich bleiben (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.

- Bei einer großen Anzahl von Richtlinien ist ein visueller Vergleich u. U. 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 vollständig 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. Lesen Sie sich noch einmal durch, wie Filter in einer XenApp 7.6-Site im Gegensatz zu XenApp 6.x angewendet werden. Durch die wesentlichen Unterschiede zwischen der XenApp 6.x-Farm und der XenApp 7.6-Site kann sich die Wirkung von Filtern ändern.

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 u. U. Änderungen erforderlich.

Filter	Überlegungen
Zugriffssteuerung	Die Zugriffssteuerung sollte die gleichen Werte wie die ursprünglichen XenApp 6.x-Filter enthalten und ohne Änderungen funktionieren.
Citrix CloudBridge	Ein einfacher Boolescher Wert, der ohne Änderungen funktionieren sollte. (Dieses Produkt heißt jetzt NetScaler SD-WAN.)
Client-IP-Adresse	Listet Client-IP-Adressbereiche auf. Jeder Bereich ist entweder zugelassen oder verweigert. Das Importskript behält die Werte bei, aber Änderungen können erforderlich sein, wenn sich andere Clients mit den XenApp 7.6-VDA-Maschinen verbinden.

Filter	Überlegungen
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.
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.

Filter	Überlegungen
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 einige Konten möglicherweise aufgelöst und andere nicht. Obwohl nicht sehr wahrscheinlich ist, dass verschiedene Domänen und Benutzer den gleichen Namen haben, sollten Sie unbedingt die Filter sorgfältig überprüfen, um sicherzustellen, dass sie korrekte Werte enthalten.

Anwendungen

Die Skripts zum Import von Anwendungen importieren nicht nur Anwendungen, sondern sie erstellen auch Objekte, z. B. 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 sehr 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 selbst zu er-

stellen, 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 ist ebenfalls 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 eine große Anzahl von 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.

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"
```

Beim nächsten Mal, wenn Sie `Export-XAFarm` ausführen, sollen die nächsten 100 Anwendungen exportiert werden. Sie verwenden den Parameter "SkipApps", um die bereits exportierten Anwendungen (die ersten 200) zu überspringen, und exportieren mit dem Parameter "AppLimit"die nächsten 100 Anwendungen.

```
Export-XAFarm -XmlOutputFile "Apps201-300.xml"-AppLimit "100"-SkipApps
 "200"
```

Ausschließen von Objekten aus dem Export

Einige Objekte brauchen nicht exportiert zu werden und können ignoriert werden. Dazu zählen besonders Objekte, die nicht importiert werden. Weitere Informationen hierzu finden Sie unter 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. Hiermit können Sie andere Daten in eine XML-Ausgabedatei exportieren und dann den Export erneut ausführen, um die Anwendungen in eine zweite 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 Export der Zone möglicherweise fehl. Wenn Sie den Parameter "IgnoreZones"verwenden, wird der Exportvorgang 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/oder 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?redirectedfrom=MSDN.

  - **MatchWorkerGroup** und **NotMatchWorkerGroup** –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.

    ```
    Import-XAFarm –XmlInputFile XAFarm.xml –LogFile XAFarmImport.
    log –MatchWorkerGroup 'Productivity Apps' –DeliveryGroupName '
    Productivity Apps'
    ```

  - **MatchFolder** und **NotMatchFolder** –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.

    ```
    Import-XAFarm –XmlInputFile XAFarm.xml –LogFile XAFarmImport
    .log –MatchFolder 'Productivity Apps' –DeliveryGroupName '
    Productivity Apps'
    ```

    Beispielsweise importiert das folgende Cmdlet Anwendungen in Ordnern, deren Name "MS Office Apps"enthält, in die Standardbereitstellungsgruppe.

    ```
    Import-XAFarm -XmlInputFile .\TheFarmApps.XML -MatchFolder "
    .*/MS Office Apps/.*"
    ```

  - **MatchAccount** und **NotMatchAccount** –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".

    ```
    Import-XAFarm –XmlInputFile XAFarm.xml –LogFile XAFarmImport.
    log –MatchAccount 'DOMAIN\\Finance Group' –DeliveryGroupName '
    Finance'
    ```

  - **MatchServer** und **NotMatchServer** –Beispiel: Bei Anwendungen, die auf Servern organisiert sind, importiert das folgende Cmdlet Anwendungen von Servern, deren Name nicht "Current"ist, in eine XenApp-Bereitstellungsgruppe mit dem Namen "Legacy".


```
Import-XAFarm -XmlInputFile XAFarm.xml -LogFile XAFarmImport.
log -NotMatchServer 'Current'-DeliveryGroupName 'Legacy'
```

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: Objekt verweist nicht auf eine Instanz eines Objekts. 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:
  - "Ein Laufwerk mit dem Namen 'LocalGpo'ist bereits vorhanden."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.
  - "Es wurde kein Parameter gefunden, der dem Parameternamen 'Controller'entspricht." 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 und entfernen Sie es auch nicht separat.
- 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 Komponenten, die diese Einstellungen unterstützen, wurden entweder durch neue Technologien/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
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, in FMA auf 64 Zeichen. Anwendungen, deren Ordnerpfad einen Ordnernamen mit mehr als 64 Zeichen enthält, werden beim Import übersprungen. Das Limit gilt nur für die Ordnernamen im Ordnerpfad. Der gesamte Ordnerpfad kann länger sein als die aufgeführten Limits. 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

FMA-Eigenschaft	Wert
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.
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.

IMA-Eigenschaft	Anmerkungen
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.
CachingOption	FMA verwendet eine andere Technologie für den Sitzungsvorabstart.
ServerNames	FMA verwendet eine andere Technologie.
WorkerGroupNames	FMA unterstützt keine Workergruppen.

Sicherheit

February 6, 2020

Citrix Virtual Apps and Desktops bietet 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 trennt Citrix Virtual Apps and Desktops vertrauliche Daten und geistiges Eigentum sicher von Endpunktgeräten, da alle Daten in einem Datencenter gespeichert werden. Wenn Richtlinien für das Zulassen von Datenübertragungen aktiviert sind, werden alle Daten verschlüsselt.

Die Citrix Virtual Apps and Desktops-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.

Citrix Virtual Apps and Desktops vereinfacht 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 Citrix Virtual Apps and Desktops 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 Citrix Virtual Apps and Desktops 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 kann Sicherheitsbedenken im Zusammenhang Zeitpersonal von Drittanbietern verringern. 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 Citrix Virtual Apps oder Citrix Virtual Desktops 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.

Citrix Virtual Apps and Desktops unterstützt auch die mehrstufige Authentifizierung für Windows oder eine bestimmte Anwendung. Mit der mehrstufigen Authentifizierung können auch alle Ressourcen, die von Citrix Virtual Apps and Desktops bereitgestellt werden, verwaltet werden. Diese Methoden sind u. a.:

- Token
- Smartcards
- RADIUS
- Kerberos
- Biometrie

Citrix Virtual Desktops kann mit vielen Sicherheitslösungen von Drittanbietern verwendet werden, von der Identitätsverwaltung bis zu Antivirensoftware. Eine Liste der unterstützten Produkte finden Sie unter http://www.citrix.com/ready.

Bestimmte Releases von Citrix Virtual Apps and Desktops sind für Common Criteria zertifiziert. Eine Liste dieser Normen finden Sie unter https://www.commoncriteriaportal.org/cc/.

Bewährte Methoden und Überlegungen zur Sicherheit

February 17, 2023

> **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 http://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.

Verwenden Sie plattformspezifische Antimalware-Software.

Wenn Sie Software installieren, verwenden Sie die angegebenen Standardpfade.

- Wenn Sie Software an einem anderen Speicherort als dem angegebenen Standardpfad installieren, sollten Sie weitere Sicherheitsmaßnahmen für den Dateispeicherort hinzufügen, z. B. eingeschränkte Berechtigungen.

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 Dokumentation 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 Konfig-

> urieren 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.

Firewalls

Schützen Sie alle Maschinen in der Umgebung mit Perimeterfirewalls, u. a. bei Bedarf auch an Grenzen von Enklaven.

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.

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.

> **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 Datencenters 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 (http://www.iana.org/) registriert.

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 im Artikel "Verwalten von Bereitstellungsgruppen".
- 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.

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 Multisitzungs-OS 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 Citrix Virtual Apps and Desktops-Komponenten, wie den VDA für Einzelsitzungs-OS, 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 Citrix Virtual Apps oder Citrix Virtual Desktops-Bereitstellung verwendet werden, und die Möglichkeit zum Enumerieren von Ressourcen in einem Hypervisorpool in der Konsole.
- Citrix Maschinenerstellungsdienste (NT SERVICE\CitrixMachineCreationService): Orchestriert das Erstellen von Desktop-VMs.
- Citrix Überwachungsdienst (NT SERVICE\CitrixMonitor): Sammelt Metrik für Citrix Virtual Apps oder Citrix Virtual Desktops, 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. Folgen Sie den 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.
- Benutzer sehen den Desktop in einem Fenster: Benutzer melden sich zunächst am 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.

XML-Vertrauenseinstellung

Die XML-Vertrauensstellung gilt für Bereitstellungen, die Folgendes verwenden:

- Eine On-Premises-Installation von StoreFront
- Eine (Benutzer-)Authentifizierungstechnologie für Abonnenten ohne erforderliche Kennwörter. Beispiele hierfür sind Lösungen mit Domänen-Passthrough, Smartcards, SAML und Veridium.

Wenn Sie die XML-Vertrauensstellung aktivieren, können Benutzer Anwendungen erfolgreich authentifizieren und starten. Der Delivery Controller stuft die von StoreFront gesendeten Anmeldeinformationen als vertrauenswürdig ein. Aktivieren Sie diese Einstellung nur, wenn die Kommunikation zwischen Delivery Controllern und StoreFront gesichert ist (durch Firewalls, IPsec oder andere empfohlene Sicherheitsfunktionen).

Diese Einstellung ist standardmäßig deaktiviert.

Überprüfen, aktivieren oder deaktivieren Sie die XML-Vertrauensstellung mit dem PowerShell-SDK von Citrix Virtual Apps and Desktops.

- Zum Überprüfen des aktuellen Werts der XML-Vertrauensstellung führen Sie `Get-BrokerSite` aus und überprüfen den Wert für `TrustRequestsSentToTheXMLServicePort`.
- Zum Aktivieren der XML-Vertrauensstellung führen Sie `Set-BrokerSite -TrustRequestsSentToTh $true` aus.
- Zum Deaktivieren der XML-Vertrauensstellung führen Sie `Set-BrokerSite -TrustRequestsSentTo $false` aus.

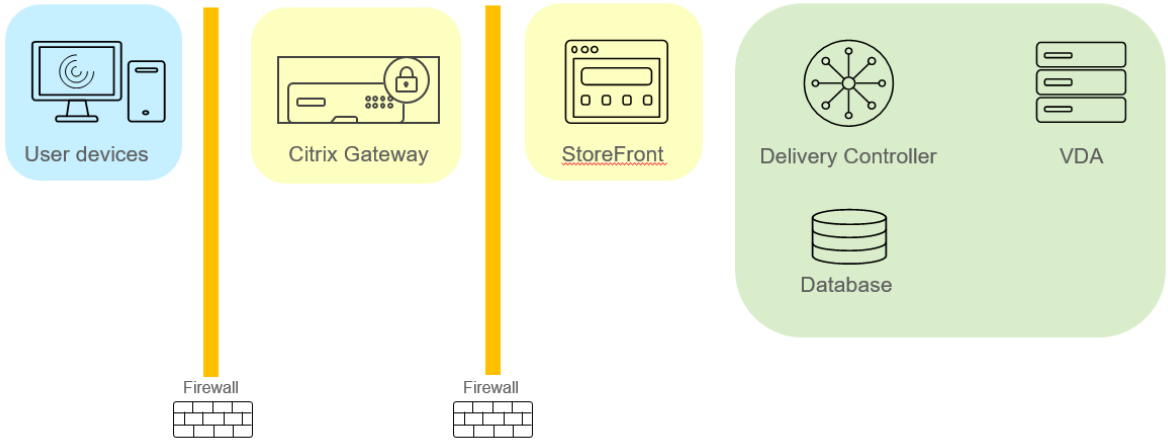
Integrieren von Citrix Virtual Apps and Desktops und Citrix Gateway

February 7, 2020

StoreFront-Server werden für die Zugriffsverwaltung auf veröffentlichte Ressourcen und Daten bereitgestellt und konfiguriert. Für den Remotezugriff wird das Hinzufügen von Citrix Gateway vor StoreFront empfohlen.

> **Hinweis:**
>
> Detaillierte Konfigurationsschritte zur Integration von Citrix Virtual Apps and Desktops und Citrix Gateway finden Sie in der StoreFront-Dokumentation.

Die folgende Abbildung zeigt ein Beispiel für eine vereinfachte Citrix Bereitstellung mit Citrix Gateway. Citrix Gateway kommuniziert mit StoreFront zum Schutz von Apps und Daten, die mit Citrix Virtual Apps and Desktops bereitgestellt werden. Die Benutzergeräte führen zum Herstellen einer sicheren Verbindung für den Zugriff auf Apps, Desktops und Dateien die Citrix Workspace-App aus.



Die Anmeldung und Authentifizierung von Benutzern erfolgt über Citrix Gateway. Citrix 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

February 6, 2020

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 anzeigen, zusätzlich zu den globalen Informationen, 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. Kann auch Sitzungsverwaltungs- und Energieverwaltungsvorgänge für die Maschinen in diesen Bereitstellungsgruppen durchführen.

Rolle	Berechtigungen
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.
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
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 erwog, Peter zu einem Volladministrator für den Win7-Bereich zu machen. Sie 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. Es gibt keine Delegation. 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 funk-

tionale Zuständigkeiten (Rollen). Beispiel: Es gibt zwei Volladministratoren, andere sind Helpdeskadministratoren. Außerdem 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 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 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. Dabei werden weder die Rolle noch der Bereich gelöscht. Es wirkt sich auch nicht auf andere Administratoren aus, die mit diesem Rollen-/Bereichspaar konfiguriert sind.

Klicken Sie zum Verwalten von Administratoren im Studio-Navigationsbereich auf **Konfiguration > Administratoren** und dann im mittleren Bereich obenauf die Registerkarte **Administratoren**.

- **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.

- **Kopieren eines Administrators:** Wählen Sie den Administrator 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.
- **Bearbeiten eines Administrators:** Wählen Sie den Administrator im mittleren Bereich aus und klicken Sie im Aktionsbereich auf **Administrator bearbeiten**. Sie können die Rollen-/Geltungsbereichspaare bearbeiten oder löschen und neue hinzufügen.
- **Löschen eines Administrators:** Wählen Sie den Administrator 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.

Im oberen Bereich werden die Administratoren angezeigt, die Sie erstellt haben. Wählen Sie einen Administrator aus, um die Details im unteren Bereich anzuzeigen. Die Spalte **Warnungen** gibt an, ob die dem Administrator zugeordneten Rollen-/Bereichspaare unbrauchbare Rollen oder Bereiche enthalten. Die folgende Warnmeldung wird angezeigt, wenn ein zugeordnetes Rollen-/Bereichspaar unbrauchbare Rollen oder Bereiche enthält:

- Zugehörige Rolle oder Bereich nicht verwendbar
  - Entfernen Sie das Rollen-/Bereichspaar vom Administrator.

> **Wichtig:**
>
> Eine Warnmeldung wird nur angezeigt, wenn ein zugeordnetes Rollen-/Bereichspaar eine unbrauchbare Rollen, einen unbrauchbaren Bereich oder beides enthält.

Führen Sie einen der folgenden Schritte aus, um das Rollen-/Bereichspaar vom Administrator zu entfernen:

- Löschen Sie das Rollen-/Bereichspaar.
  1. Klicken Sie im Bereich **Aktionen** auf **Administrator bearbeiten**.
  2. Wählen Sie im Fenster **Administrator bearbeiten** das Rollen-/Bereichspaar aus und klicken Sie auf **Löschen**.
  3. Klicken Sie zum Beenden auf **OK**.
- Löschen Sie den Administrator.
  1. Klicken Sie im Bereich **Aktionen** auf **Administrator löschen**.
  2. Klicken Sie im Fenster **Studio** auf **Löschen**.

Erstellen und Verwalten von Rollen

Wenn Administratoren eine Rolle erstellen oder bearbeiten, können sie nur die Berechtigungen aktivieren, die sie selbst haben. Dadurch wird verhindert, dass Administratoren eine Rolle mit mehr Berechtigungen erstellen, als sie derzeit haben, und sie dann sich selbst zuweisen (oder eine ihnen bereits zugewiesene Rolle bearbeiten).

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- oder Kleiner-Als-Zeichen, senkrechter Strich, eckige Klammern, runde Klammern, 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. Nur Editionen, die benutzerdefinierten Rollen unterstützen, haben diese 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**.

- **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.
- **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.
- **Kopieren einer Rolle:** Wählen Sie die Rolle 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.
- **Bearbeiten einer Rolle:** Wählen Sie die Rolle 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.
- **Löschen einer Rolle:** Wählen Sie die Rolle 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 wie folgt 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 Bereich hinzufügen, bleiben sie Teil des Bereichs "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 haben immer den Geltungsbereich "Alle".) Maschinen, Energieaktionen, Desktops und Sitzungen bekommen nicht direkt einen Bereich zugeordnet. Administratoren können Berechtigungen für diese Objekte über die zugeordneten Maschinenkataloge oder Bereitstellungsgruppen zugewiesen werden.

Geltungsbereichsnamen können bis zu 64 Unicode-Zeichen enthalten. Bereichsnamen dürfen keines der folgenden Zeichen enthalten: umgekehrter Schrägstrich, Schrägstrich, Semikolon, Doppelpunkt, Nummernzeichen, Komma, Sternchen, Fragezeichen, Gleichheitszeichen, Größer-Als- oder Kleiner-Als-Zeichen, senkrechter Strich, eckige Klammern, runde Klammern, 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 verbunden, müssen Sie sicherstellen, dass kein Rollen-/Geltungsbereichspaar durch Änderungen am Bereich unbrauchbar wird.

Klicken Sie zum Verwalten von Geltungsbereichen im Studio-Navigationsbereich auf **Konfiguration > Administratoren** und dann im mittleren Bereich oben auf die Registerkarte **Geltungsbereiche**.

- **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.
- **Geltungsbereich kopieren:** Wählen Sie den Geltungsbereich im mittleren Bereich aus und klicken Sie im Bereich "Aktionen"auf **Geltungsbereich kopieren**. Geben Sie einen Namen und eine Beschreibung ein. Ändern Sie bei Bedarf die Objekttypen und Berechtigungen.
- **Geltungsbereich bearbeiten:** Wählen Sie den Geltungsbereich im mittleren Bereich aus und klicken Sie im Bereich "Aktionen"auf **Geltungsbereich bearbeiten**. Ändern Sie den Namen und die Beschreibung sowie die Objekttypen und Objekte nach Bedarf.

- **Geltungsbereich löschen:** Wählen Sie den Geltungsbereich im mittleren Bereich aus und klicken Sie im Bereich "Aktionen"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 Studio-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 ist in Programme\Citrix\DelegatedAdmin\SnapIn\Citrix.DelegatedAdmin.Admin.V1\Scripts\.

  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 string`	Zielspeicherort für die Ausgabe. Standard = stdout
`-AdminAddress string`	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.
CommonParameters	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

September 21, 2021

Smartcards und ähnliche Technologien werden im Rahmen der in diesem Abschnitt beschriebenen

Richtlinien unterstützt. Zur Verwendung von Smartcards mit Citrix Virtual Apps oder Citrix Virtual Desktops ist Folgendes zu berücksichtigen:

- 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 Citrix Virtual Apps- bzw. Citrix Virtual Desktops-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.

> **Hinweis:**
>
> Die Smartcard-Registrierung mit dem Feature Schnelle Smartcard wird nicht unterstützt. Die Smartcardregistrierung funktioniert möglicherweise, wenn "Schnelle Smartcard"deaktiviert ist, das hängt jedoch vom Typ der Smartcard und der Middleware ab. Wenden Sie sich an den Smartcard- und Middleware-Anbieter, um in Erfahrung zu bringen, inwiefern deren Produkte Citrix Virtual Apps and Desktops und die Smartcardregistrierung über virtuelle Sitzungen unterstützen.

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. Citrix Virtual Apps and Desktops unterstützt diese Art der 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 in Citrix Virtual Apps oder Citrix Virtual Desktops 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 bei Verwendung der Citrix Workspace-App (Citrix Receiver Mindestversion 4.3) unterstützt.
  - Versionen von Citrix Virtual Apps and Desktops (zuvor "XenApp und XenDesktop") vor 7.6 FP3 unterstützen keine virtuellen Smartcards.
  - Weitere Informationen zu virtuellen Smartcards 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 Citrix Virtual Apps and Desktops 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 unter Das Citrix Ready-Programm.

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 http://www.citrix.com/ready.

Middleware	Geeignete Karten
Gemalto Mini Driver für .NET-Karte	Gemalto .NET v2+

Informationen zur Verwendung von Smartcards mit anderen Gerätetypen finden Sie in der Citrix Workspace-App-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.

Die folgenden Smartcards wurden mit Remote-PC-Zugriff getestet:

Middleware	Geeignete Karten
Gemalto .NET-Minitreiber	Gemalto .NET v2+

Schnelle Smartcard

Schnelle Smartcard ist eine Verbesserung gegenüber der alten HDX PC/SC-basierten Smartcardumleitung. Das Feature verbessert die Leistung, wenn Smartcards in WANs mit hoher Latenz verwendet werden.

Schnelle Smartcard ist standardmäßig auf Hostmaschinen mit derzeit unterstützten Windows-VDAs aktiviert. Um Schnelle Smartcard auf dem Host zu deaktivieren (z. B. für Diagnosezwecke), wählen Sie für die Registrierungseinstellung "Disable Cryptographic Redirection"einen beliebigen Wert ungleich null:

```
HKLM\SOFTWARE\Citrix\SmartCard
CryptographicRedirectionDisable (DWORD)
<!--NeedCopy-->
```

Um Schnelle Smartcard auf dem Client zu aktivieren, fügen Sie den ICA-Parameter "SmartCardCryptographicRedirection"in die Datei *default.ica* der zugehörigen StoreFront-Site ein:

```
[WFClient]
SmartCardCryptographicRedirection=On
```

Einschränkungen:

- Nur Citrix Receiver für Windows unterstützt schnelle Smartcards. Wenn Sie das Feature in der Standard-ICA-Datei konfigurieren, verwenden Citrix Receiver für andere Betriebssysteme als Windows weiterhin die alte PC/SC-Umleitung.
- Schnelle Smartcard unterstützt als einziges Double-Hop-Szenario ICA> ICA, wenn es auf beiden Hops aktiviert ist. Da schnelle Smartcard keine ICA > RDP-Double-Hops unterstützt, funktioniert ein solches Szenario nicht.

- Schnelle Smartcard unterstützt Cryptography Next Generation nicht. Daher unterstützt schnelle Smartcard keine Smartcards mit Elliptic Curve Cryptography (ECC).
- Schnelle Smartcard unterstützt nur Schlüsselcontaineroperationen mit Schreibschutz.
- Schnelle Smartcard unterstützt das Ändern der Smartcard-PIN nicht.

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 Workspace-App-Version. Die unterstützten Versionen werden in der Dokumentation zur Citrix Workspace-App normalerweise in einem Smartcard-Artikel oder im Artikel zu den Systemanforderungen aufgeführt.

Benutzererfahrung

Smartcardunterstützung ist in Citrix Virtual Apps and Desktops 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.

Sie können PINs mit einem Kartenverwaltungsprogramm oder einem Herstellerdienstprogramm zurücksetzen.

> **Wichtig:**
>
> In einer Citrix Virtual Apps- oder Citrix Virtual Desktops-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 Citrix Virtual Apps and Desktops 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 http://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 Workspace-App 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 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.

Schritt 5. Aktivieren Sie Citrix 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 der Citrix Workspace-App 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 die Citrix Workspace-App 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 die Citrix Workspace-App).

Smartcardbereitstellungen

February 7, 2020

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	Verbunden über Citrix Gateway
Nicht in Domänen eingebundene Computer	Direkte Verbindung
Remotezugriff von nicht in Domänen eingebundenen Computern	Verbunden über Citrix 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 Citrix Gateway bereitstellen, melden sich die Benutzer an den Geräten an und werden von Receiver für Windows zur Authentifizierung bei Citrix Gateway aufgefordert. Dies gilt sowohl für in Domänen eingebundene Geräte als auch für Geräte, die nicht in Domänen eingebunden sind. Die Benutzer können sich bei Citrix Gateway mit Smartcard und PIN oder mit expliziten Anmeldeinformationen anmelden. Sie können somit die bimodale Authentifizierung für Anmeldungen bei Citrix Gateway bereitstellen. Konfigurieren Sie die Passthrough-Authentifizierung von Citrix Gateway an StoreFront und delegieren Sie die Validierung der Anmeldeinformationen für Smartcardbenutzer an Citrix 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.

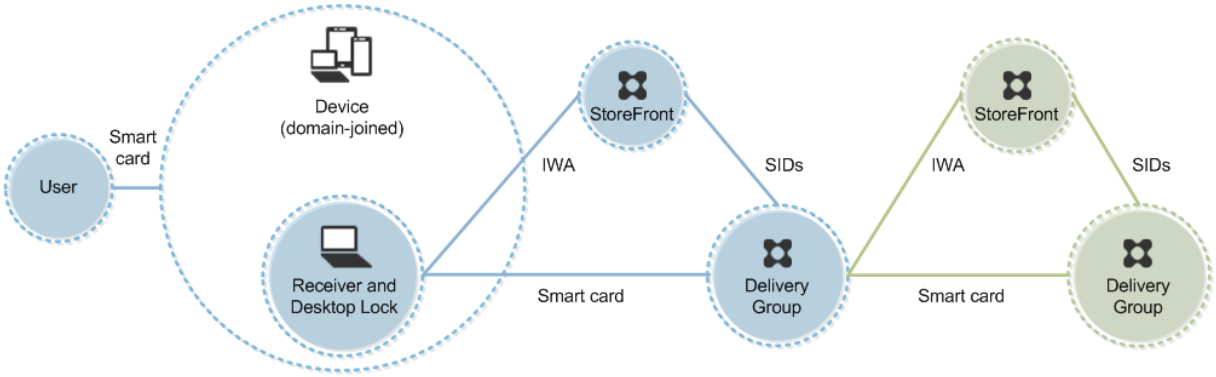
Richtlinieneinstellung	Desktop-Verhalten
Keine Aktion	Keine Aktion.
Arbeitsstation sperren	Die Desktopsitzung wird getrennt und der virtuelle Desktop gesperrt.
Abmeldung erzwingen	Der Benutzer wird zur Abmeldung gezwungen. Wenn die Netzwerkverbindung unterbrochen ist und diese Einstellung aktiviert wird, 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.

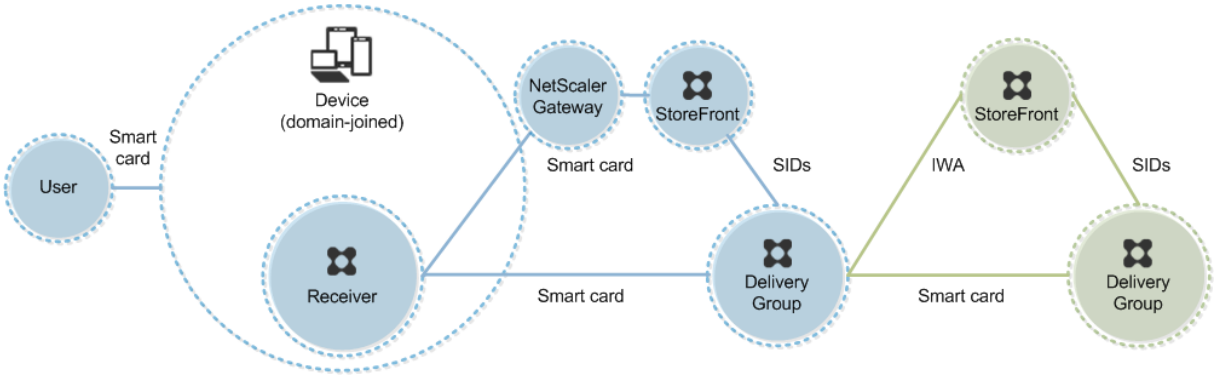


Zum Anmelden beim Gerät benötigt der Benutzer eine Smartcard und eine PIN. Der Benutzer wird dann durch Receiver beim Storefront-Server mittels integrierter Windows-Authentifizierung (IWA) authentifiziert. StoreFront übergibt die Sicherheits-IDs (SIDs) an Citrix Virtual Apps oder Citrix Virtual Desktops. 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 Citrix Gateway/Access Gateway.



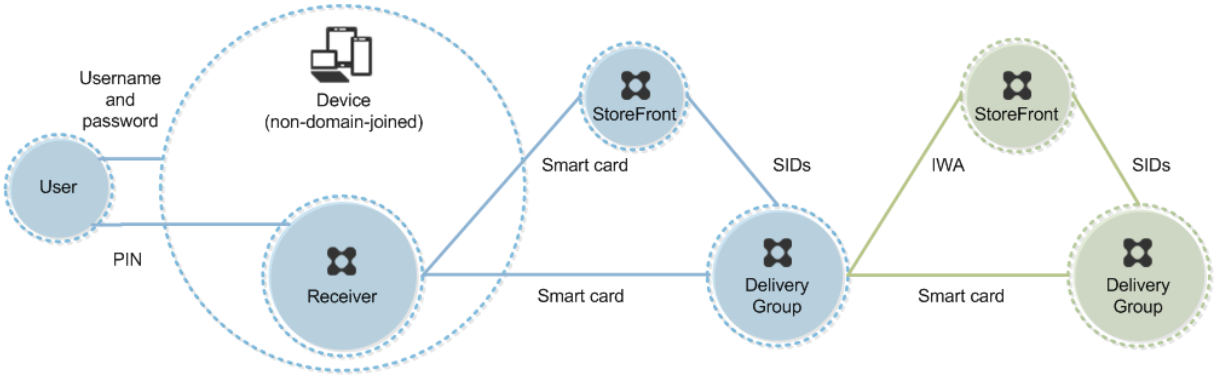
Der Benutzer meldet sich mit Smartcard und PIN beim Gerät und anschließend erneut bei Citrix Gateway oder Access Gateway an. Die zweite Anmeldung kann entweder mit Smartcard und PIN oder einem Benutzernamen und einem Kennwort erfolgen, da Receiver in dieser Bereitstellung eine bimodale Authentifizierung zulässt.

Der Benutzer wird automatisch bei StoreFront angemeldet; StoreFront übergibt die Sicherheits-IDs (SIDs) an Citrix Virtual Apps oder Citrix Virtual Desktops. 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.



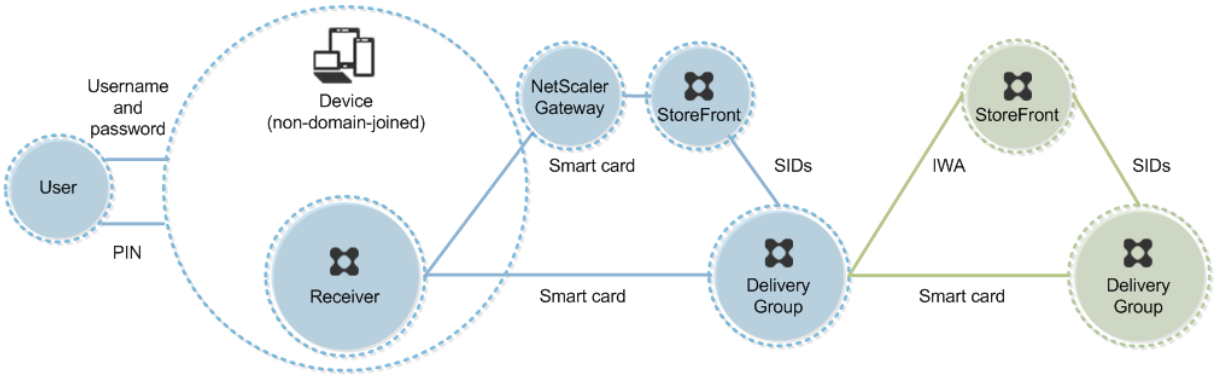
Ein Benutzer meldet sich beim Gerät an. Normalerweise muss er seinen Benutzernamen und das Kennwort eingeben, aber da das Gerät nicht Mitglied einer Domäne ist, sind die Anmeldeinformationen für diese Anmeldung optional. Da bimodale Authentifizierung in dieser Bereitstellung möglich ist, fordert Receiver 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 Citrix Virtual Apps oder Citrix Virtual Desktops. 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 Citrix Virtual Apps oder Citrix Virtual Desktops. 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.

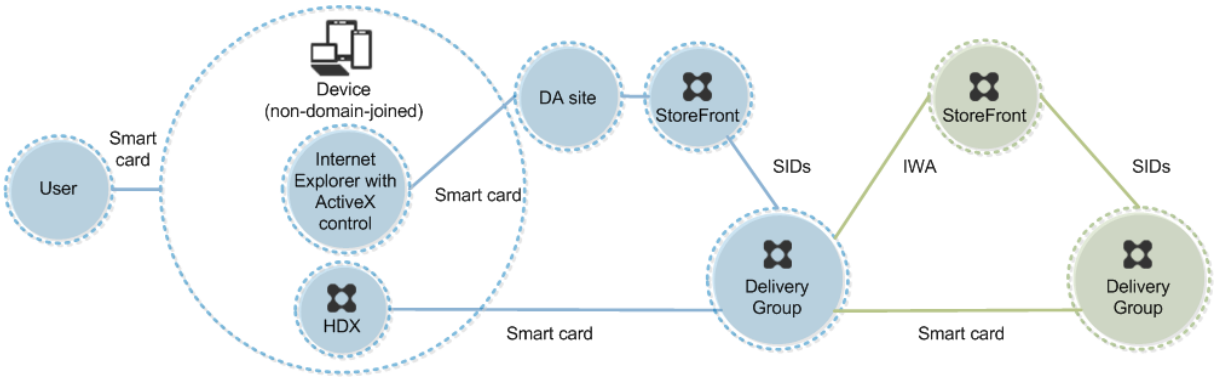
Diese Bereitstellung kann um einen zweiten StoreFront-Server und einen Server mit gehosteten Anwendungen auf ein Double-Hop-System erweitert werden. Ein Receiver auf dem virtuellen Desktop übernimmt die Authentifizierung beim zweiten StoreFront-Server. Für diese zweite Verbindung kann eine beliebige 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 Citrix Virtual Apps, Citrix Virtual Desktops 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 Citrix Virtual Apps oder Citrix Virtual Desktops. Der erste verfügbare Desktop in der alphabetischen Liste einer zugewiesenen Desktopgruppe wird gestartet.

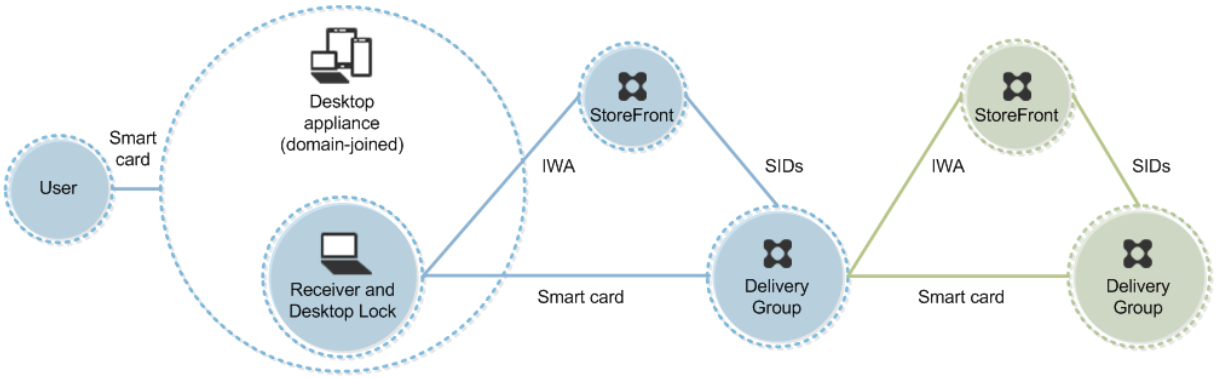
Diese Bereitstellung kann um einen zweiten StoreFront-Server und einen Server mit gehosteten Anwendungen auf ein Double-Hop-System erweitert werden. Ein Receiver auf dem virtuellen Desktop übernimmt die Authentifizierung beim zweiten StoreFront-Server. Für diese zweite Verbindung kann eine beliebige 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 Citrix Virtual Apps, Citrix Virtual Desktops 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 Citrix Virtual Apps oder Citrix Virtual Desktops. 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

February 6, 2020

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 Citrix 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 **Benutzer wechseln** auswählen, um eine andere Kachel auszuwählen, da die Single Sign-On-Kachel nicht funktioniert.

Transport Layer Security (TLS)

June 8, 2022

Citrix Virtual Apps and Desktops unterstützt das TLS-Protokoll (Transport Layer Security) für TCP-basierte Verbindungen zwischen Komponenten. Citrix Virtual Apps and Desktops unterstützt außerdem das Protokoll DTLS (Datagram Transport Layer Security) für UDP-basierte ICA-/HDX-Verbindungen unter Einsatz von adaptivem Transport.

TLS und DTLS ähneln einander und unterstützen die gleichen digitalen Zertifikate. Wird eine Citrix Virtual Apps- oder Citrix Virtual Desktops-Site für TLS konfiguriert, wird sie automatisch auch für DTLS konfiguriert. Verwenden Sie die nachstehenden Verfahren. Die meisten Schritte gelten für TLS und DTLS gleichermaßen, auf Ausnahmen wird ausdrücklich hingewiesen.

- 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 der Citrix Workspace-App und Virtual Delivery Agents (VDAs) unter Ausführung der folgenden Schritte:

  - Konfigurieren Sie TLS auf den Maschinen, auf denen die VDAs installiert sind. Der Einfachheit halber werden Maschinen, auf denen VDAs installiert sind, im Folgenden einfach als “VDAs”bezeichnet. Allgemeine Informationen finden Sie unter TLS-Einstellungen auf VDAs. Es wird dringend empfohlen, das von Citrix gelieferte PowerShell-Skript zum Konfigurieren von TLS/DTLS zu verwenden. Einzelheiten finden Sie unter Konfigurieren von TLS auf einem VDA mit dem PowerShell-Skript. Wenn Sie TLS/DTLS manuell konfigurieren möchten, lesen Sie den Abschnitt 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.
- Bei gepoolten, mit Maschinenerstellungsdiensten oder Provisioning Services bereitgestellten VDAs wird das VDA-Maschinenimage beim Neustart zurückgesetzt und vorherige TLS-Einstellungen gehen verloren. Führen Sie das PowerShell-Skript bei jedem VDA-Neustart aus, um die TLS-Einstellungen neu zu konfigurieren.

> **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.

Installieren von TLS-Serverzertifikaten auf Controllern

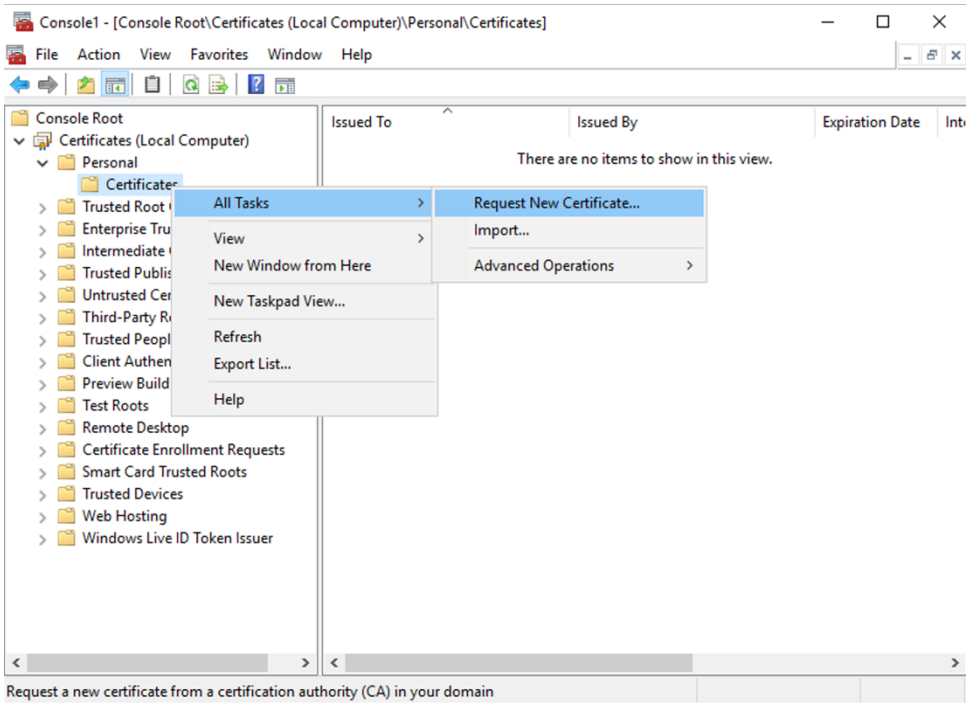
Für HTTPS wird TLS vom XML-Dienst über Serverzertifikate, nicht aber über Clientzertifikate unterstützt. In diesem Abschnitt wird das Beschaffen und Installieren von TLS-Zertifikaten für Delivery Controller beschrieben. Die gleichen Schritte können auf Cloud Connectors zum Verschlüsseln des STA- und 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.

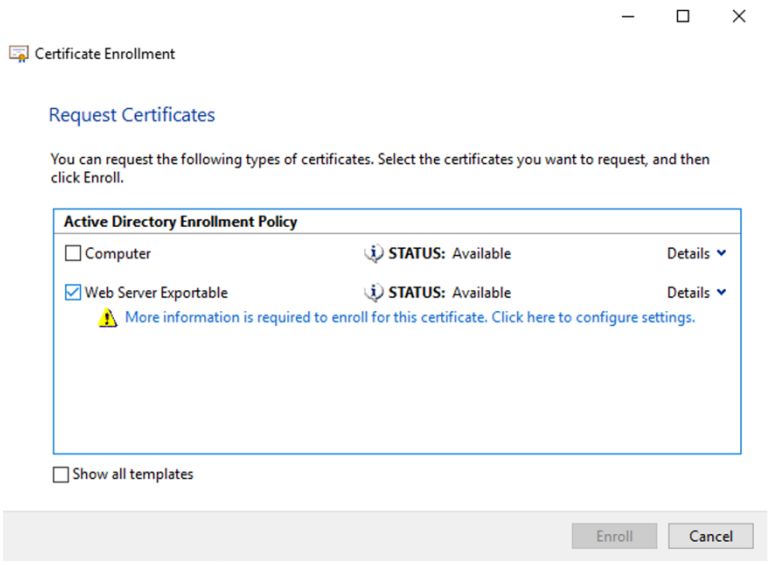
Wenn die Microsoft-Zertifizierungsstelle in eine Active Directory-Domäne oder die vertrauenswürdige Gesamtstruktur integriert ist, zu der die Delivery Controller gehören, können Sie ein Zertifikat über den Assistenten für die Zertifikatregistrierung des MMC-Snap-Ins Zertifikate beschaffen.

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**.



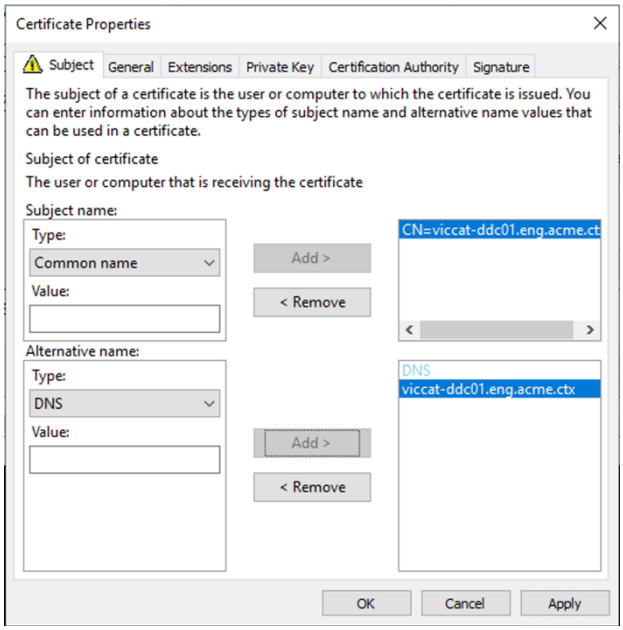
3. Klicken Sie auf **Weiter** und erneut auf **Weiter**, um zu bestätigen, dass Sie das Zertifikat von der Active Directory-Registrierung erwerben.
4. Wählen Sie die Vorlage für das Zertifikat "Serverauthentifizierung"aus. Wenn die Vorlage automatisch einen Antragsteller enthält, können Sie auf **Registrieren** 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"

$SSLxml = "http add sslcert ipport=$IPPort certhash=$Thumbprint
    appid={
 $Formatted_Guid }
 "

```



```
$SSLxml | netsh

. netsh http show sslcert
<!--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.

> **Hinweis:**
>
> Ist der Controller unter Windows Server 2016 oder Windows Server 2019 und StoreFront unter Windows Server 2012 R2 installiert, muss die Reihenfolge der TLS-Verschlüsselungssammlungen auf dem Controller oder StoreFront geändert werden. Diese Konfigurationsänderung ist bei Installation von Controller und StoreFront unter anderen Windows Server-Kombinationen nicht erforderlich.

Die Liste der Verschlüsselungssammlungen muss `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384` oder `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256` (oder beide) oder ähnliche TLS_ECDHE-Verschlüsselungssammlungen enthalten. Diese TLS_ECDHE-Verschlüsselungssammlungen müssen vor jeglichen TLS_DHE_-Verschlüsselungssammlungen stehen.

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`, oder eine ähnliche TLS_ECDHE-Verschlüsselungssammlung vor allen 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.

> **Hinweis:**
>
> 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
<!--NeedCopy-->
```

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. Bevor Sie TLS für eine Bereitstellungsgruppe konfigurieren, müssen Sie TLS für alle darin enthaltenen VDAs konfigurieren.

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. Legen Sie die zulässige Mindestversion fest. 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.

  DTLS 1.0 entspricht TLS 1.1 und DTLS 1.2 entspricht TLS 1.2.

- **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 Workspace-App 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 http://support.microsoft.com/kb/811833. Die folgende Tabelle enthält die Verschlüsselungssammlungen in jeder Gruppe:

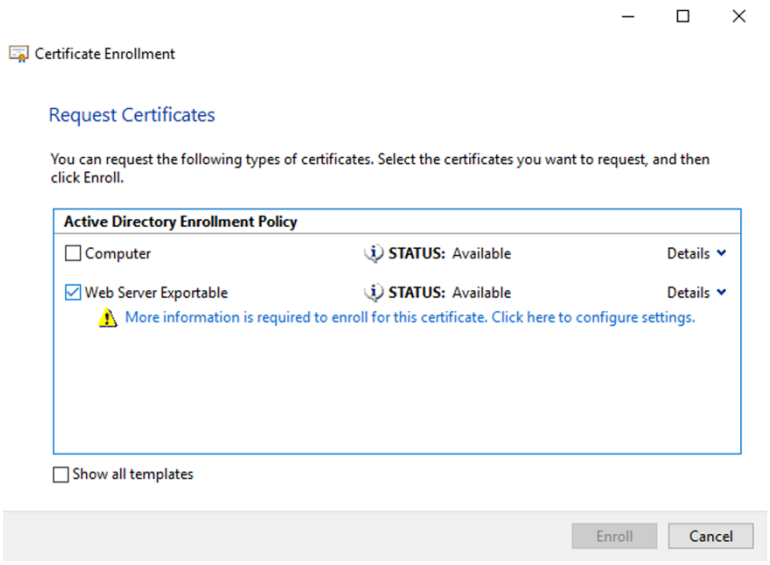
TLS-/DTLS-Verschlüsselungssammlung	ALLE	COM	GOV	ALLE	COM	GOV
FIPS-Modus	Aus	Aus	Aus	Ein	Ein	Ein
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 *	X	X	X	X		X
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	X	X	X	X		X
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	X	X		X	X	

*Unter Windows Server 2012 R2 nicht unterstützt.

> **Hinweis:**
>
> Der VDA unterstützt keine DHE-Verschlüsselungssammlungen (zum Beispiel `TLS_DHE_RSA_WITH_AES_256_GCM_SHA384`, `TLS_DHE_RSA_WITH_AES_256_CBC_SHA`, `TLS_DHE_RSA_WITH_AES_128_GCM_SHA256` und `TLS_DHE_RSA_WITH_AES_128_CBC_SHA`.) Wenn sie von Windows ausgewählt werden, werden sie möglicherweise nicht von Receiver verwendet.
>
> Wenn Sie ein Citrix Gateway verwenden, finden Sie in der Citrix ADC-Dokumentation Informationen zur Unterstützung der Verschlüsselungssammlung für die Back-End-Kommunikation. Informationen zur Unterstützung der TLS-Verschlüsselungssammlung finden Sie unter Ciphers available on the Citrix ADC appliances. Informationen zu für DTLS unterstützten Verschlüsselungssammlungen finden Sie unter DTLS-Unterstützung für Verschlüsselungssammlungen.

Anfordern und Installieren eines Zertifikats

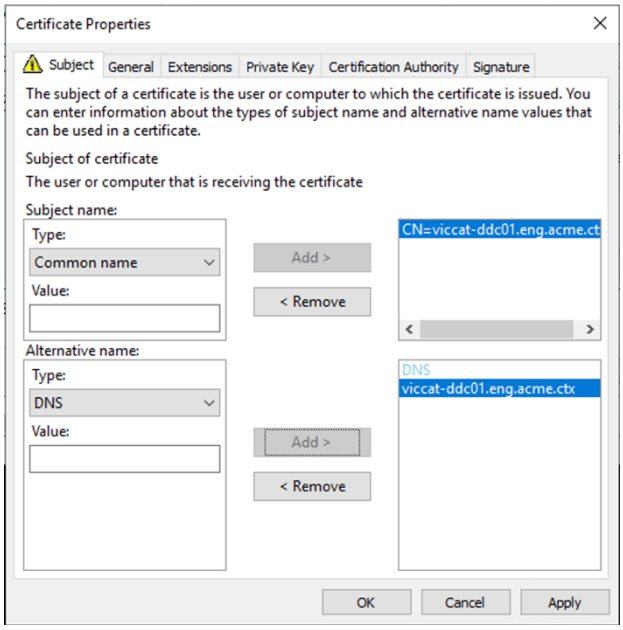
1. Öffnen Sie auf dem VDA die MMC-Konsole und fügen Sie das Zertifikat-Snap-In hinzu. Wählen Sie bei Aufforderung "Computerkonto"aus.
2. Erweitern Sie **Persönlich > Zertifikate** und verwenden Sie dann den Kontextmenübefehl **Alle Aufgaben > Neues Zertifikat anfordern**.
3. Klicken Sie auf **Weiter** 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. Es ist sowohl der standardmäßige Windows-**Computer** als auch **Web Server Exportable** zulässig. 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 **Details** und konfigurieren Sie Folgendes:

   Antragstellername: Wählen Sie **Allgemeiner Name** und geben Sie den FQDN des VDAs an.

   Alternativer Name: Wählen Sie **DNS** und geben Sie den FQDN des VDAs an.

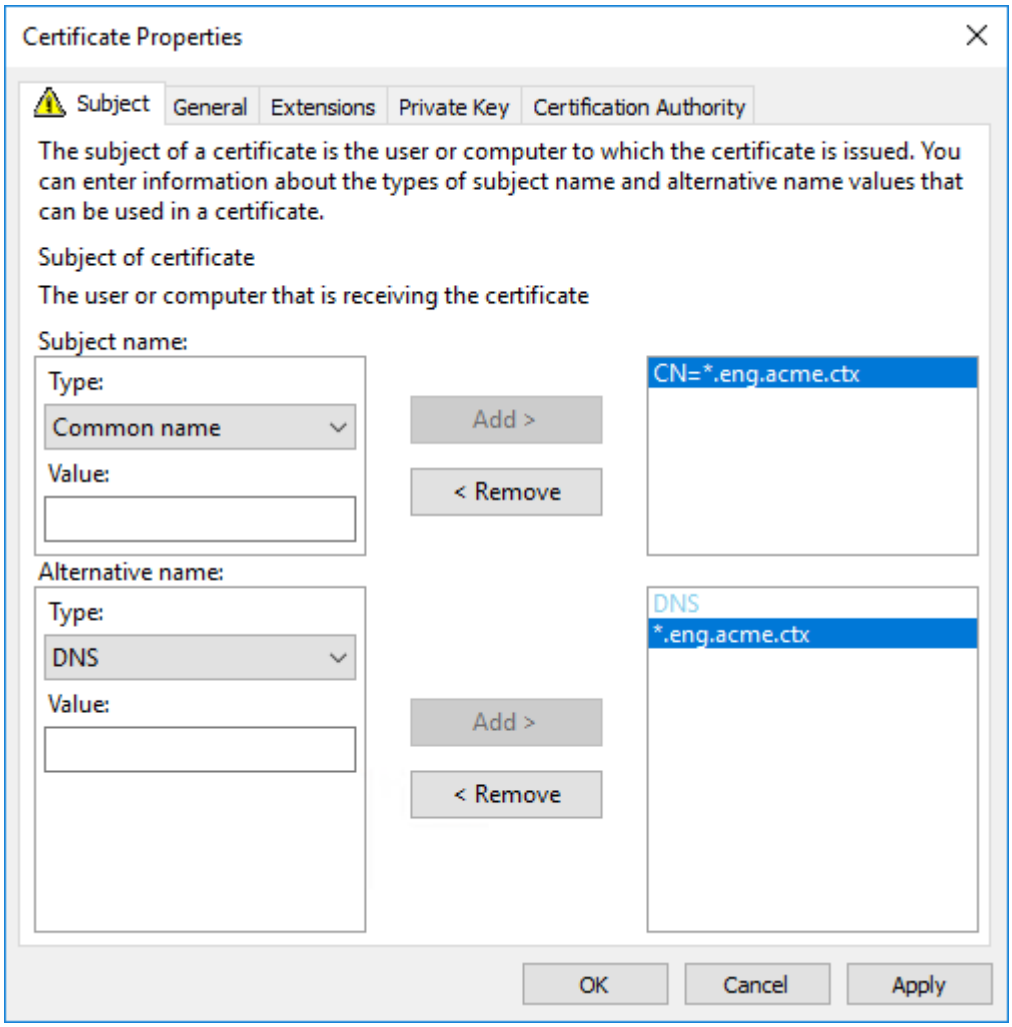


> **Hinweis:**
>
> Verwenden Sie die automatische Registrierung von Active Directory-Zertifikatdienste-Zertifikaten zur Automatisierung des Ausstellens und Bereitstellens von Zertifikaten für die VDAs. Das Verfahren wird unter https://support.citrix.com/article/CTX205473 erläutert.

Sie können Platzhalterzertifikate verwenden, um mehrere VDAs mit einem einzelnen Zertifikat zu schützen:

Antragstellername: wählen Sie **Allgemeiner Name** und geben Sie die *.primary.domain der VDAs ein.

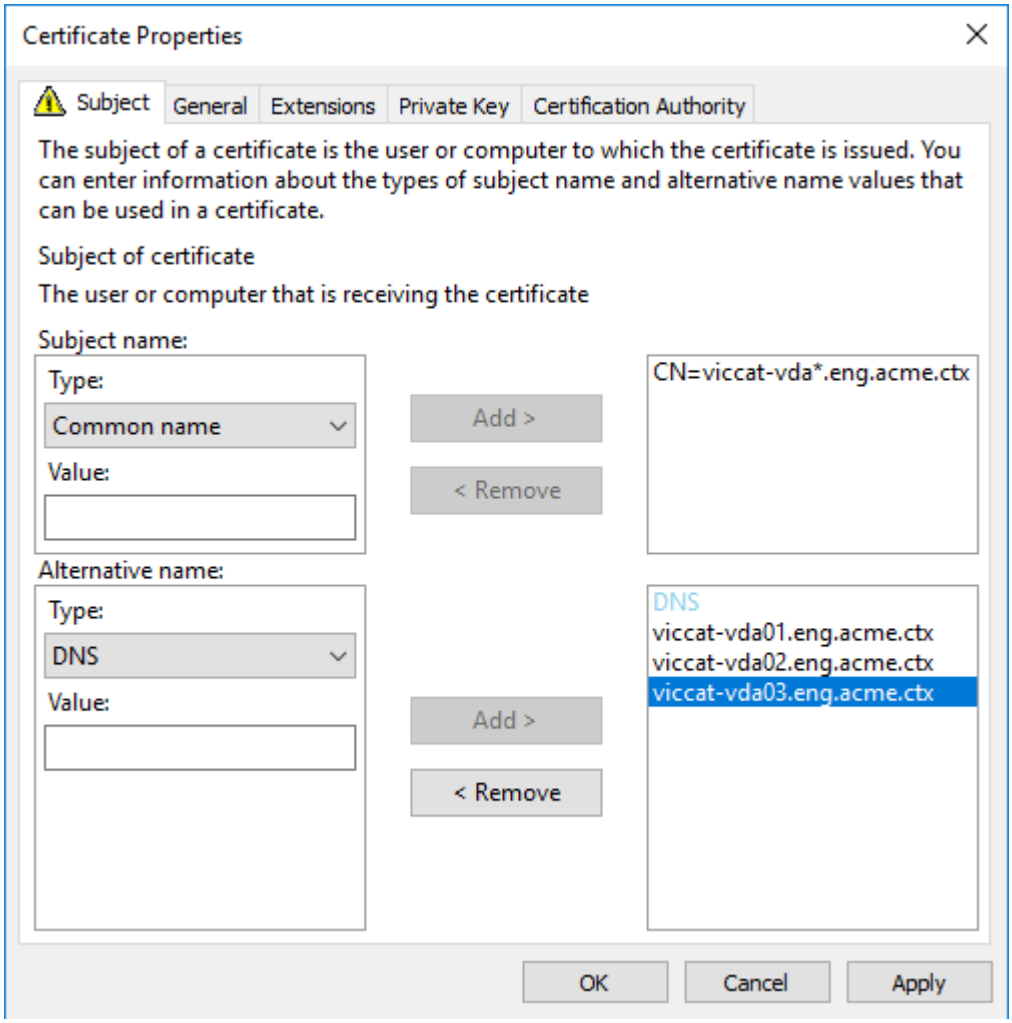
Alternativer Name: Wählen Sie **DNS** und geben Sie die *.primary.domain der VDAs an.



Sie können SAN-Zertifikate verwenden, um mehrere spezifische VDAs mit einem einzelnen Zertifikat zu schützen:

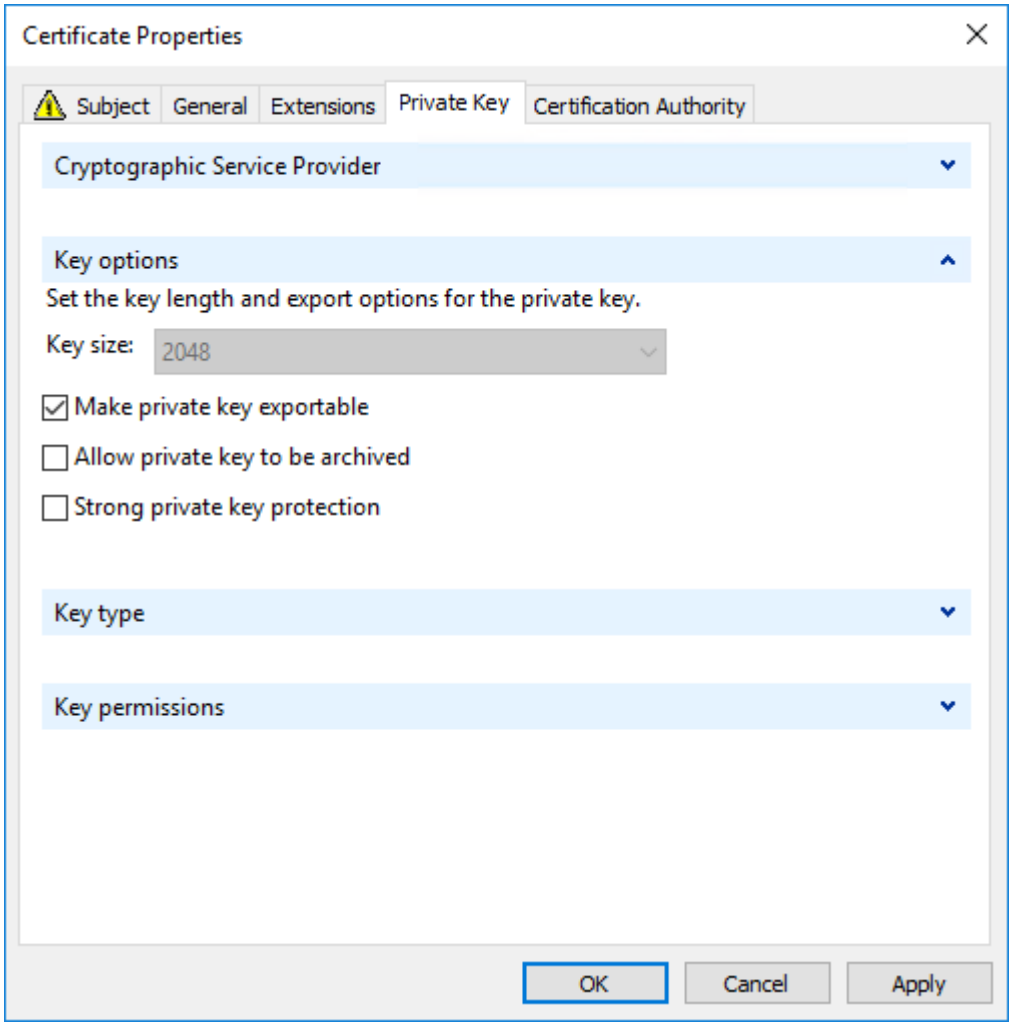
Antragstellername: wählen Sie **Allgemeiner Name** und geben Sie eine Zeichenfolge zur Identifizierung der Zertifikatnutzung ein.

Alternativer Name: Wählen Sie **DNS** und geben Sie einen Eintrag für den FQDN jedes VDAs an. Verwenden Sie ein Minimum alternativer Namen, um eine optimale TLS-Aushandlung zu gewährleisten.



Hinweis:

Sowohl für Platzhalter- als auch für SAN-Zertifikate muss **Privaten Schlüssel exportierbar machen** auf der Registerkarte “Privater Schlüssel”ausgewählt werden:



Konfigurieren von TLS auf einem VDA mit dem PowerShell-Skript

Installieren Sie das TLS-Zertifikat im Bereich Lokaler Computer > Eigene Zertifikate > Zertifikate des Zertifikatspeichers. Sind mehrere Zertifikate an diesem Speicherort, geben Sie den Fingerabdruck des Zertifikats im PowerShell-Skript an.

> **Hinweis:**
>
> Ab XenApp und XenDesktop 7.16 LTSR findet das PowerShell-Skript das richtige Zertifikat basierend auf dem FQDN des VDA. Sie brauchen den Fingerabdruck nicht angeben, wenn nur ein Zertifikat für den VDA-FQDN vorhanden ist.

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.

Wenn Sie TLS aktivieren, werden DHE-Verschlüsselungssammlung deaktiviert. ECDHE-Verschlüsselungssammlung sind nicht betroffen.

Wenn Sie TLS aktivieren, deaktiviert das Skript alle vorhandenen Windows-Firewallregeln für den angegebenen TCP-Port. Anschließend wird eine neue Regel hinzugefügt, durch die der ICA-Service eingehende Verbindungen nur am TLS-, TCP- und UDP-Port annehmen kann. Außerdem werden die Windows-Firewallregeln für Folgendes deaktiviert:

- Citrix ICA (Standard: 1494)
- Citrix CGP (Standard: 2598)
- Citrix WebSocket (Standard: 8008)

Die Benutzer können nur über TLS oder DTLS eine Verbindung herstellen. Sie können ICA/HDX, ICA/HDX mit Sitzungszuverlässigkeit oder HDX über WebSocket nicht ohne TLS oder DTLS verwenden.

> **Hinweis:**
>
> DTLS wird nicht mit ICA/HDX-Audio über UDP Real-time Transport oder mit ICA/HDX Framehawk unterstützt.

Siehe Netzwerkports.

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

Transport Layer Security (TLS)

Citrix Virtual Apps and Desktops unterstützt das TLS-Protokoll (Transport Layer Security) für TCP-basierte Verbindungen zwischen Komponenten. Citrix Virtual Apps and Desktops unterstützt außerdem das Protokoll DTLS (Datagram Transport Layer Security) für UDP-basierte ICA-/HDX-Verbindungen unter Einsatz von adaptivem Transport.

TLS und DTLS ähneln einander und unterstützen die gleichen digitalen Zertifikate. Wird eine Citrix Virtual Apps- oder Citrix Virtual Desktops-Site für TLS konfiguriert, wird sie automatisch auch für DTLS konfiguriert. Verwenden Sie die nachstehenden Verfahren. Die meisten Schritte gelten für TLS und DTLS gleichermaßen, auf Ausnahmen wird ausdrücklich hingewiesen.

- 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 der Citrix Workspace-App und Virtual Delivery Agents (VDAs) unter Ausführung der folgenden Schritte:

  - Konfigurieren Sie TLS auf den Maschinen, auf denen die VDAs installiert sind. Der Einfachheit halber werden Maschinen, auf denen VDAs installiert sind, im Folgenden einfach als "VDAs"bezeichnet. Allgemeine Informationen finden Sie unter TLS-Einstellungen auf VDAs. Es wird dringend empfohlen, das von Citrix gelieferte PowerShell-Skript zum Konfigurieren von TLS/DTLS zu verwenden. Einzelheiten finden Sie unter Konfigurieren von TLS auf einem VDA mit dem PowerShell-Skript. Wenn Sie TLS/DTLS manuell konfigurieren möchten, lesen Sie den Abschnitt 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.
    * Bei gepoolten, mit Maschinenerstellungsdiensten oder Provisioning Services bereitgestellten VDAs wird das VDA-Maschinenimage beim Neustart zurückgesetzt und vorherige TLS-Einstellungen gehen verloren. Führen Sie das PowerShell-Skript bei jedem VDA-Neustart aus, um die TLS-Einstellungen neu zu konfigurieren.

> **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.

Installieren von TLS-Serverzertifikaten auf Controllern

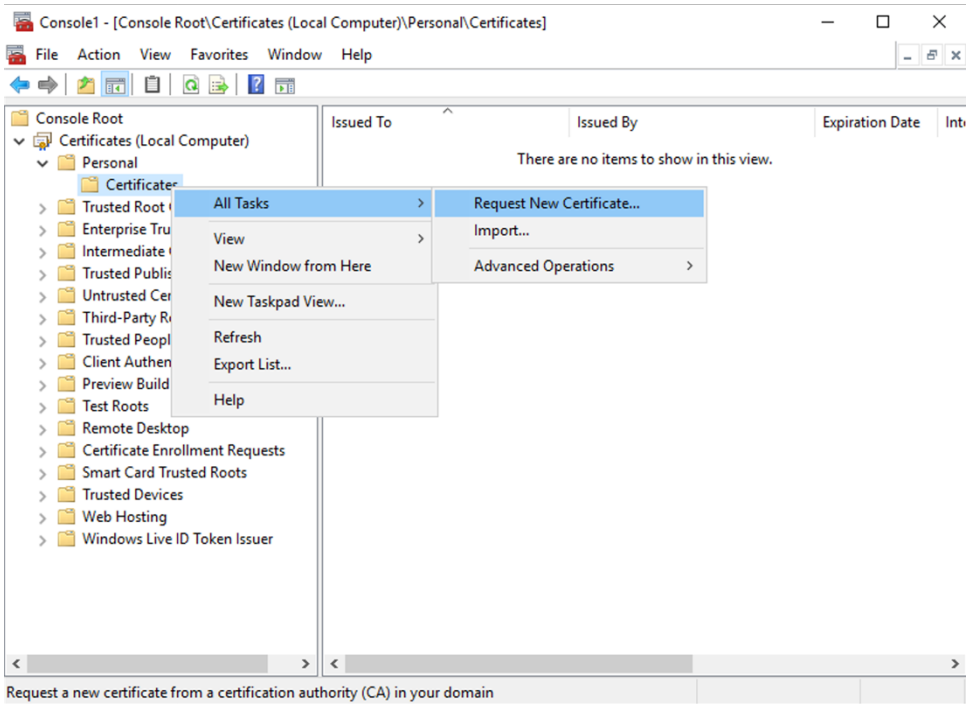
Für HTTPS wird TLS vom XML-Dienst über Serverzertifikate, nicht aber über Clientzertifikate unterstützt. In diesem Abschnitt wird das Beschaffen und Installieren von TLS-Zertifikaten für Delivery Controller beschrieben. Die gleichen Schritte können auf Cloud Connectors zum Verschlüsseln des STA- und 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.

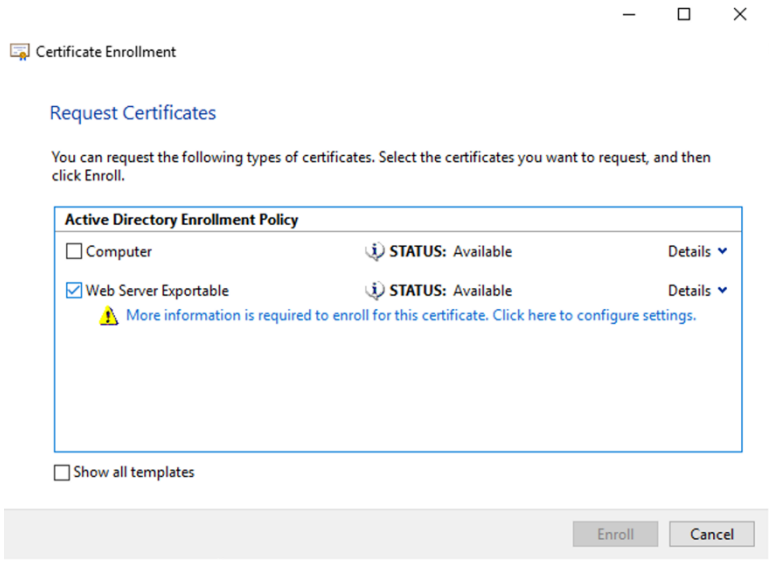
Wenn die Microsoft-Zertifizierungsstelle in eine Active Directory-Domäne oder die vertrauenswürdige Gesamtstruktur integriert ist, zu der die Delivery Controller gehören, können Sie ein Zertifikat über den Assistenten für die Zertifikatregistrierung des MMC-Snap-Ins Zertifikate beschaffen.

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.

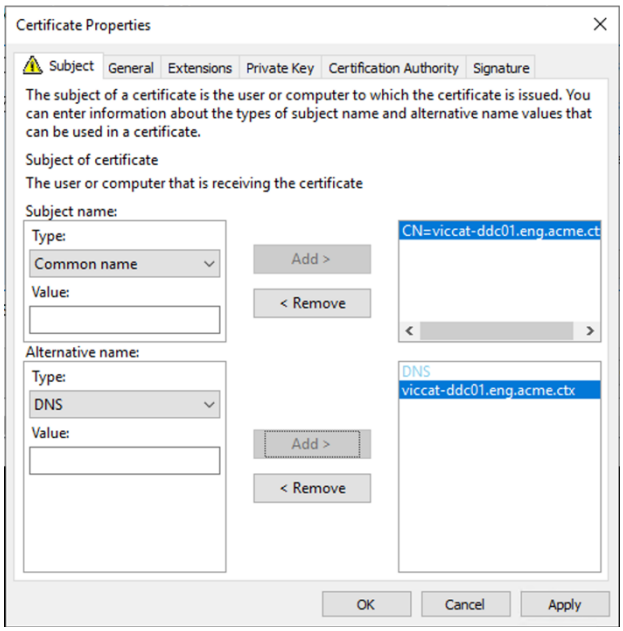


5. Um weitere Details für die Zertifikatvorlage anzugeben, klicken Sie auf die Schaltfläche **Details** und konfigurieren Sie Folgendes:

   Antragstellername: Wählen Sie "Allgemeiner Name"und geben Sie den FQDN des Delivery Con-

trollers 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:

   <!JEKYLL@5300@0>

3. Führen Sie die folgenden Befehle im selben PowerShell-Fenster aus, um den Fingerabdruck des zuvor installierten Zertifikats abzurufen:

   <!JEKYLL@5300@1>

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:

   <!JEKYLL@5300@2>

Bei korrekter Konfiguration zeigt die Ausgabe des letzten Befehls <!JEKYLL@5300@3>, dass der Listener den richtigen <!JEKYLL@5300@4> verwendet und dass <!JEKYLL@5300@5> 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.

> **Hinweis:**
>
> Ist der Controller unter Windows Server 2016 oder Windows Server 2019 und StoreFront unter Windows Server 2012 R2 installiert, muss die Reihenfolge der TLS-Verschlüsselungssammlungen auf dem Controller oder StoreFront geändert werden. Diese Konfigurationsänderung ist bei Installation von Controller und StoreFront unter anderen Windows Server-Kombinationen nicht erforderlich.

Die Liste der Verschlüsselungssammlungen muss <!JEKYLL@5300@6> oder <!JEKYLL@5300@7> (oder beide) oder ähnliche TLS_ECDHE-Verschlüsselungssammlungen enthalten. Diese TLS_ECDHE-Verschlüsselungssammlungen müssen vor jeglichen TLS_DHE_-Verschlüsselungssammlungen stehen.

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 <!JEKYLL@5300@8> oder <!JEKYLL@5300@9>, oder eine ähnliche TLS_ECDHE-Verschlüsselungssammlung, vor allen 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.

> **Hinweis:**
>
> 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:

<!JEKYLL@5300@10>

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. Bevor Sie TLS für eine Bereitstellungsgruppe konfigurieren, müssen Sie TLS für alle darin enthaltenen VDAs konfigurieren.

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 unter-

> stützt 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. Legen Sie die zulässige Mindestversion fest. 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.

DTLS 1.0 entspricht TLS 1.1 und DTLS 1.2 entspricht TLS 1.2.

- **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 Workspace-App 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 http://support.microsoft.com/kb/811833. Die folgende Tabelle enthält die Verschlüsselungssammlungen in jeder Gruppe:

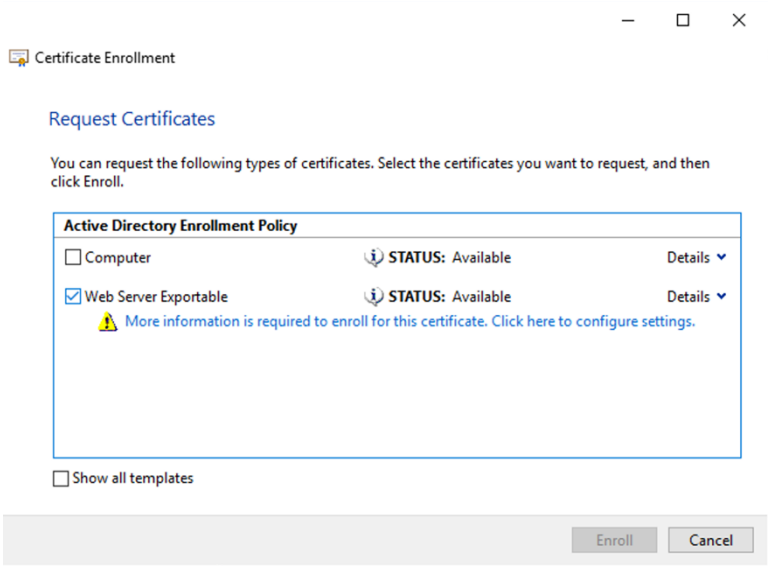
TLS-/DTLS-Verschlüsselungssammlung	**ALLE**	**COM**	**GOV**	**ALLE**	**COM**	**GOV**
FIPS-Modus	Aus	Aus	Aus	Ein	Ein	Ein
<!JEKYLL@530@11>*	X		X	X		X
<!JEKYLL@530@12>	X		X	X		X
<!JEKYLL@530@13>	X	X		X	X	

*Unter Windows Server 2012 R2 nicht unterstützt.

> **Hinweis:**
>
> Der VDA unterstützt keine DHE-Verschlüsselungssammlungen (zum Beispiel <!JEKYLL@5300@14>, <!JEKYLL@5300@15>, <!JEKYLL@5300@16> und <!JEKYLL@5300@17>.) Wenn sie von Windows ausgewählt werden, werden sie möglicherweise nicht von Receiver verwendet.
>
> Wenn Sie ein Citrix Gateway verwenden, finden Sie in der Citrix ADC-Dokumentation Informationen zur Unterstützung der Verschlüsselungssammlung für die Back-End-Kommunikation. Informationen zur Unterstützung der TLS-Verschlüsselungssammlung finden Sie unter Ciphers available on the Citrix ADC appliances. Informationen zu für DTLS unterstützten Verschlüsselungssammlungen finden Sie unter DTLS-Unterstützung für Verschlüsselungssammlungen.

Anfordern und Installieren eines Zertifikats

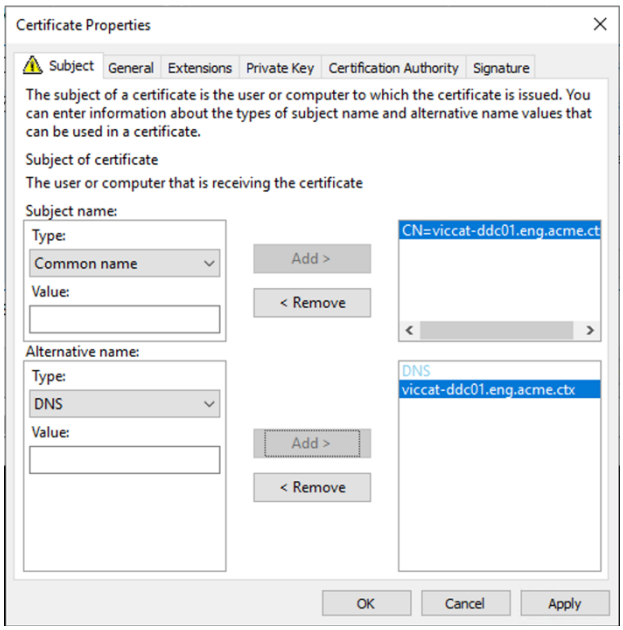
1. Öffnen Sie auf dem VDA die MMC-Konsole und fügen Sie das Zertifikat-Snap-In hinzu. Wählen Sie bei Aufforderung "Computerkonto"aus.
2. Erweitern Sie **Persönlich > Zertifikate** und verwenden Sie dann den Kontextmenübefehl **Alle Aufgaben > Neues Zertifikat anfordern**.
3. Klicken Sie auf **Weiter** 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. Es ist sowohl der standardmäßige Windows-**Computer** als auch **Web Server Exportable** zulässig. 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 **Details** und konfigurieren Sie Folgendes:

   Antragstellername: Wählen Sie **Allgemeiner Name** und geben Sie den FQDN des VDAs an.

   Alternativer Name: Wählen Sie **DNS** und geben Sie den FQDN des VDAs an.

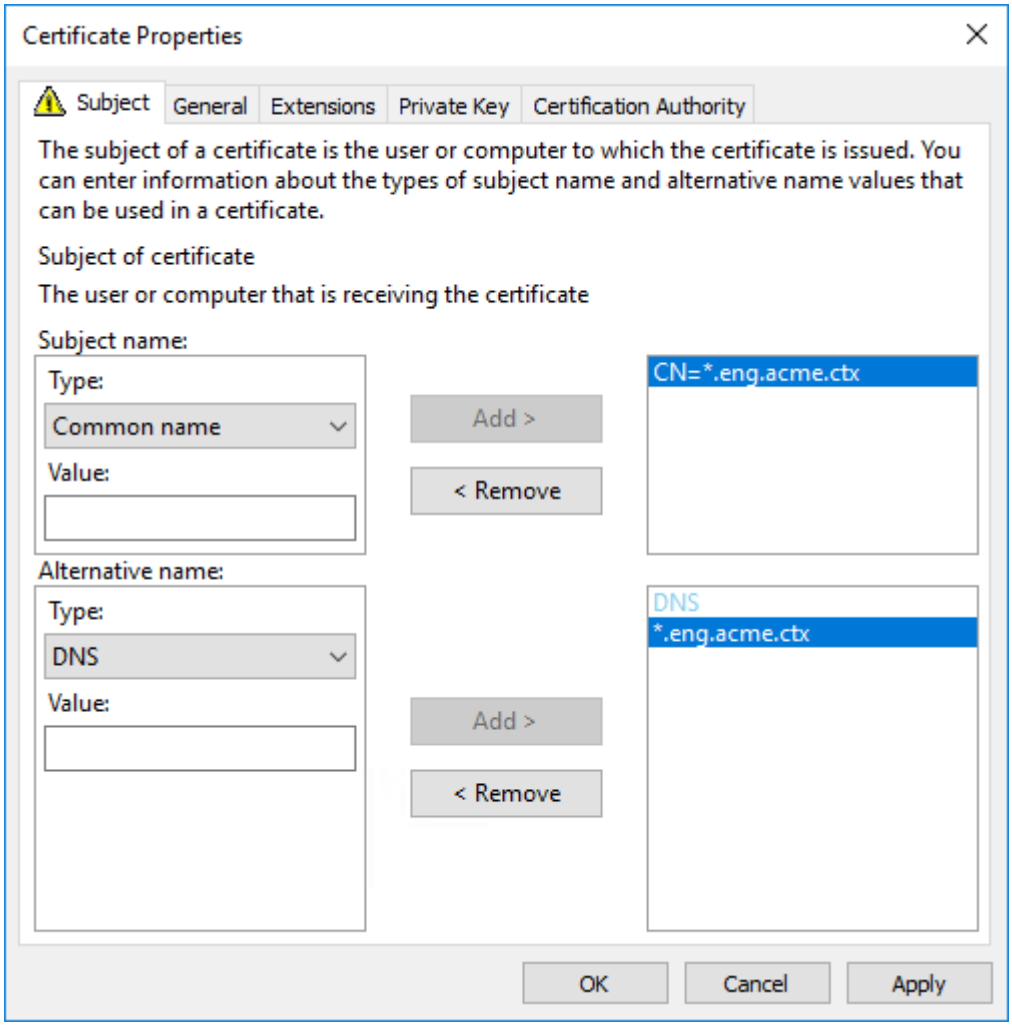


> **Hinweis:**
>
> Verwenden Sie die automatische Registrierung von Active Directory-Zertifikatdienste-Zertifikaten zur Automatisierung des Ausstellens und Bereitstellens von Zertifikaten für die VDAs. Das Verfahren wird unter https://support.citrix.com/article/CTX205473 erläutert.

Sie können Platzhalterzertifikate verwenden, um mehrere VDAs mit einem einzelnen Zertifikat zu schützen:

Antragstellername: wählen Sie **Allgemeiner Name** und geben Sie die *.primary.domain der VDAs ein.

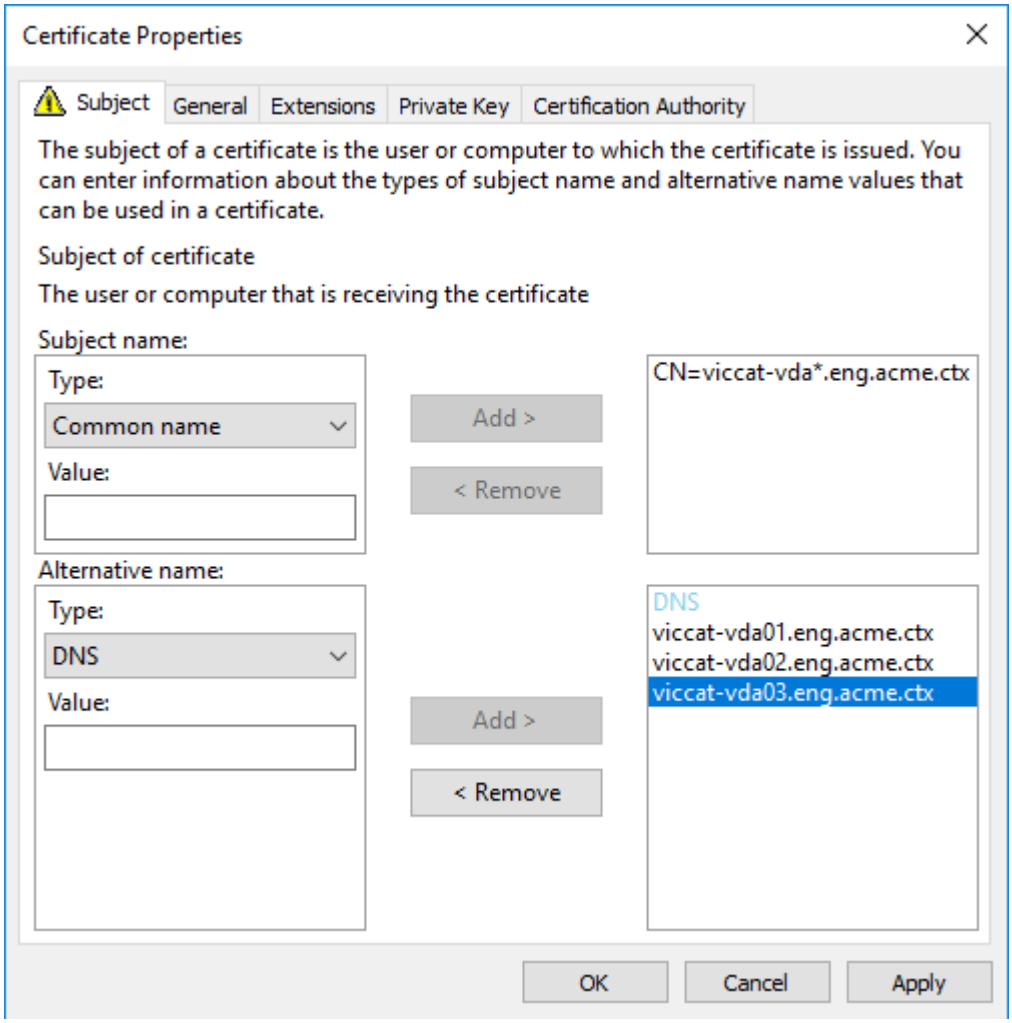
Alternativer Name: Wählen Sie **DNS** und geben Sie die *.primary.domain der VDAs an.



Sie können SAN-Zertifikate verwenden, um mehrere spezifische VDAs mit einem einzelnen Zertifikat zu schützen:

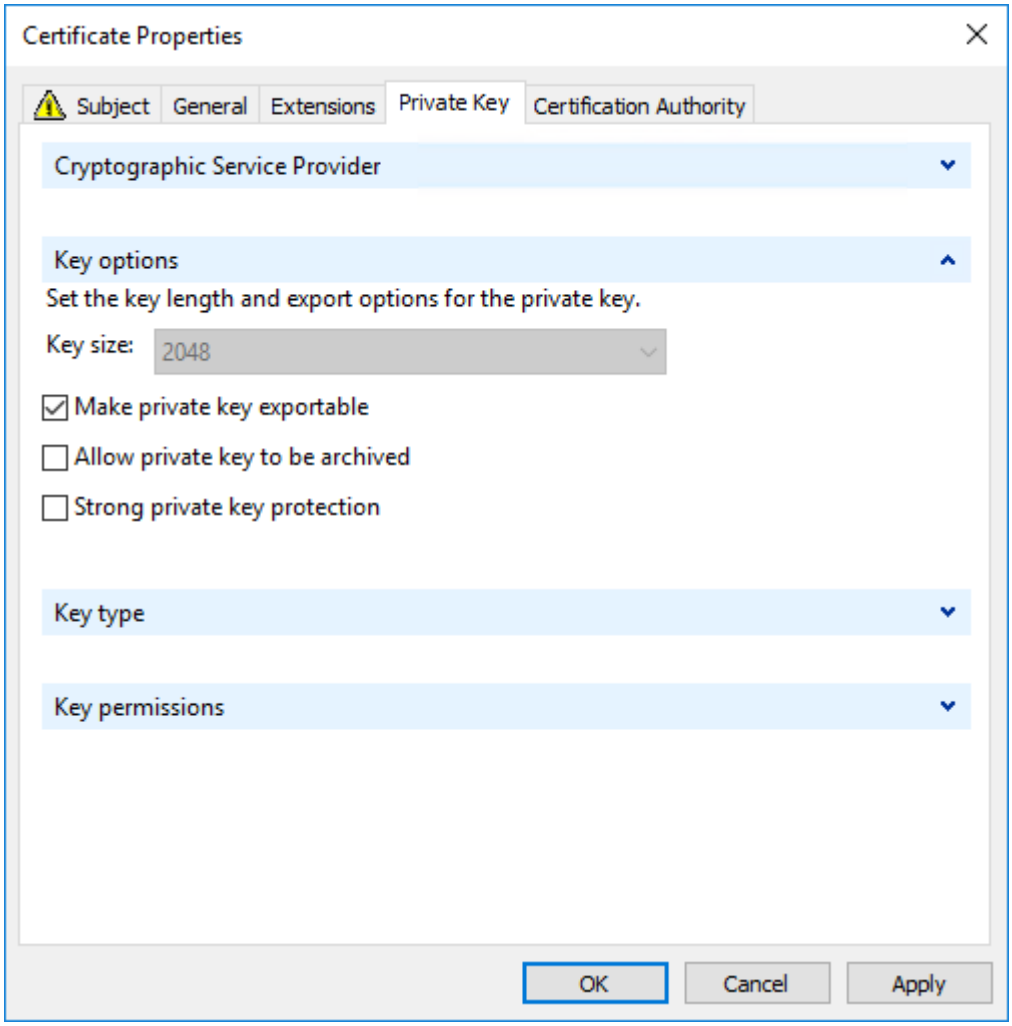
Antragstellername: wählen Sie **Allgemeiner Name** und geben Sie eine Zeichenfolge zur Identifizierung der Zertifikatnutzung ein.

Alternativer Name: Wählen Sie **DNS** und geben Sie einen Eintrag für den FQDN jedes VDAs an. Verwenden Sie ein Minimum alternativer Namen, um eine optimale TLS-Aushandlung zu gewährleisten.



Hinweis:

Sowohl für Platzhalter- als auch für SAN-Zertifikate muss **Privaten Schlüssel exportierbar machen** auf der Registerkarte “Privater Schlüssel”ausgewählt werden:



Konfigurieren von TLS auf einem VDA mit dem PowerShell-Skript

Installieren Sie das TLS-Zertifikat im Bereich Lokaler Computer > Eigene Zertifikate > Zertifikate des Zertifikatspeichers. Sind mehrere Zertifikate an diesem Speicherort, geben Sie den Fingerabdruck des Zertifikats im PowerShell-Skript an.

> **Hinweis:**
>
> Ab XenApp und XenDesktop 7.16 LTSR findet das PowerShell-Skript das richtige Zertifikat basierend auf dem FQDN des VDA. Sie brauchen den Fingerabdruck nicht angeben, wenn nur ein Zertifikat für den VDA-FQDN vorhanden ist.

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.

Wenn Sie TLS aktivieren, werden DHE-Verschlüsselungssammlung deaktiviert. ECDHE-Verschlüsselungssammlung sind nicht betroffen.

Wenn Sie TLS aktivieren, deaktiviert das Skript alle vorhandenen Windows-Firewallregeln für den angegebenen TCP-Port. Anschließend wird eine neue Regel hinzugefügt, durch die der ICA-Service eingehende Verbindungen nur am TLS-, TCP- und UDP-Port annehmen kann. Außerdem werden die Windows-Firewallregeln für Folgendes deaktiviert:

- Citrix ICA (Standard: 1494)
- Citrix CGP (Standard: 2598)
- Citrix WebSocket (Standard: 8008)

Die Benutzer können nur über TLS oder DTLS eine Verbindung herstellen. Sie können ICA/HDX, ICA/HDX mit Sitzungszuverlässigkeit oder HDX über WebSocket nicht ohne TLS oder DTLS verwenden.

> **Hinweis:**
>
> DTLS wird nicht mit ICA/HDX-Audio über UDP Real-time Transport oder mit ICA/HDX Framehawk unterstützt.

Siehe Netzwerkports.

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>”]‘

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.

Parameter	Beschreibung
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.
SSLMinVersion “”	Mindestversion des TLS-Protokolls zwischen Anführungszeichen. Gültige Werte: “TLS_1.0” (Standard), “TLS_1.1”und “TLS_1.2”.
SSLCipherSuite “”	TLS-Verschlüsselungssammlung zwischen Anführungszeichen. Gültige Werte: “GOV”, “COM”und “ALL”(Standardwert).

Beispiele Das folgende Skript installiert und aktiviert den TLS-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-Einzelsitzungs-OS oder NT SERVICE\TermService

für einen VDA für Windows-Multisitzungs-OS. Führen Sie auf der Maschine, auf der der VDA installiert ist, folgende Schritte aus:

Schritt 1. Starten Sie Microsoft Management Console (MMC): Start > Ausführen > mmc.exe.

Schritt 2. Fügen Sie dem MMC das Zertifikat-Snap-In hinzu:

1. Wählen Sie Datei > Snap-In hinzufügen/entfernen.
2. Wählen Sie Zertifikate aus, und klicken Sie dann auf Hinzufügen.
3. Wählen Sie unter "Dieses Snap-In verwaltet die Zertifikate für:"die Option "Computerkonto"und klicken Sie dann auf "Weiter".
4. 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".

Schritt 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.

Schritt 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-Einzelsitzungs-OS: "PORTICASERVICE"
- Für einen VDA für Windows-Multisitzungs-OS: "TERMSERVICE"

Schritt 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.

Schritt 6. Führen Sie regedit aus und navigieren Sie zu HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd.

1. 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).
2. 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&".)
3. 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).

Schritt 7. Stellen Sie sicher, dass der TLS-TCP- und der UDP-Port in der Windows-Firewall geöffnet sind, wenn nicht der Standardport 443 verwendet wird. (Wenn Sie die eingehende Regel für die

Windows-Firewall erstellen, wählen Sie in den Eigenschaften die Optionen "Verbindung zulassen" und "Aktiviert"aus.)

Schritt 8: Stellen Sie sicher, dass keine anderen Anwendungen oder Dienste (z. B. IIS) den TLS-TCP-Port verwenden.

Schritt 9. Damit die Änderungen auf VDAs für Windows-Multisitzungs-OS wirksam werden, starten Sie die Maschine neu. (Sie brauchen Maschinen mit VDAs für Windows-Einzelsitzungs-OS nicht neu starten.)

> **Wichtig:**
>
> Ein zusätzlicher Schritt ist erforderlich, wenn der VDA unter Windows Server 2012 R2, Windows Server 2016 oder Windows 10 Anniversary Edition oder einer unterstützten Nachfolgeversion ausgeführt wird. Dies betrifft Verbindungen von Citrix Workspace-App für HTML5 und Citrix Workspace-App für Chrome. Außerdem sind Verbindungen mit Citrix Gateway betroffen.
>
> Dieser Schritt ist auch für alle Verbindungen mit Citrix Gateway für alle VDA-Versionen erforderlich, wenn TLS zwischen dem Citrix Gateway und dem VDA konfiguriert ist.

Rufen Sie auf dem VDA (Windows Server 2012 R2, Windows Server 2016 oder Windows 10 Anniversary Edition oder höher) im Gruppenrichtlinien-Editor "Computerkonfiguration > Richtlinien > 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_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256
```

> **Hinweis:**
>
> Die ersten sechs 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 Workspace-App 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 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 das Systemereignisprotokoll auf dem VDA.

Tritt bei Verwendung der Citrix Workspace-App für Windows ein TLS-Verbindungsfehler auf, 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.

Die meisten Konfigurationen, bei denen der adaptive HDX-Transport eingesetzt wird, funktionieren mit DTLS. Das gilt auch für diejenigen mit den aktuellen Versionen der Citrix Workspace-App, von Citrix Gateway und des VDAs. Bei einigen Konfigurationen, bei denen zwischen Citrix Workspace-App und Citrix Gateway und zwischen Citrix Gateway und dem VDA DTLS verwendet wird, sind zusätzliche Maßnahmen erforderlich.

Zusätzliche Maßnahmen sind erforderlich, wenn zusätzlich eine der folgenden Bedingungen zutrifft:

- Die Citrix Gateway-Version unterstützt DTLS für den Datenverkehr an den VDA, doch die VDA-Version unterstützt DTLS nicht (Versionen bis einschließlich 7.15).
- Die VDA-Version unterstützt DTLS (ab Version 7.16), doch die Citrix Gateway-Version unterstützt DTLS für den Datenverkehr an den VDA nicht.

Führen Sie einen der folgenden Schritte aus, um zu verhindern, dass Verbindungen fehlschlagen:

- Aktualisieren Sie Citrix Gateway auf eine Version, die DTLS für den Datenverkehr an den VDA unterstützt.
- Aktualisieren Sie den VDA auf Version 7.16 oder höher.
- Deaktivieren Sie DTLS auf dem VDA.
- Deaktivieren Sie den adaptiven HDX-Transport.

> **Hinweis:**
>
> Um DTLS am VDA zu deaktivieren, deaktivieren Sie den UDP-Port 443 in der VDA-Firewallkonfiguration. Siehe Netzwerkports.

Kommunikation zwischen Controller und VDA

Die Kommunikation zwischen Controller und VDA wird auf Nachrichtenebene durch Windows Communication Framework (WCF) geschützt. 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 und Browserinhaltsumleitung

Sie können mit der HTML5-Videoumleitung und der Browserinhaltsumleitung HTTPS-Websites umleiten. 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.

Die Browserinhaltsumleitung ist standardmäßig aktiviert.

Weitere Informationen zur HTML5-Videoumleitung finden Sie unter Richtlinieneinstellungen für Multimedia.

Transport Layer Security (TLS) auf dem universellen Druckserver

June 27, 2024

TLS (Transport Layer Security) wird für TCP-Verbindungen zwischen dem Virtual Delivery Agent (VDA) und dem universellen Druckserver unterstützt.

> **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.

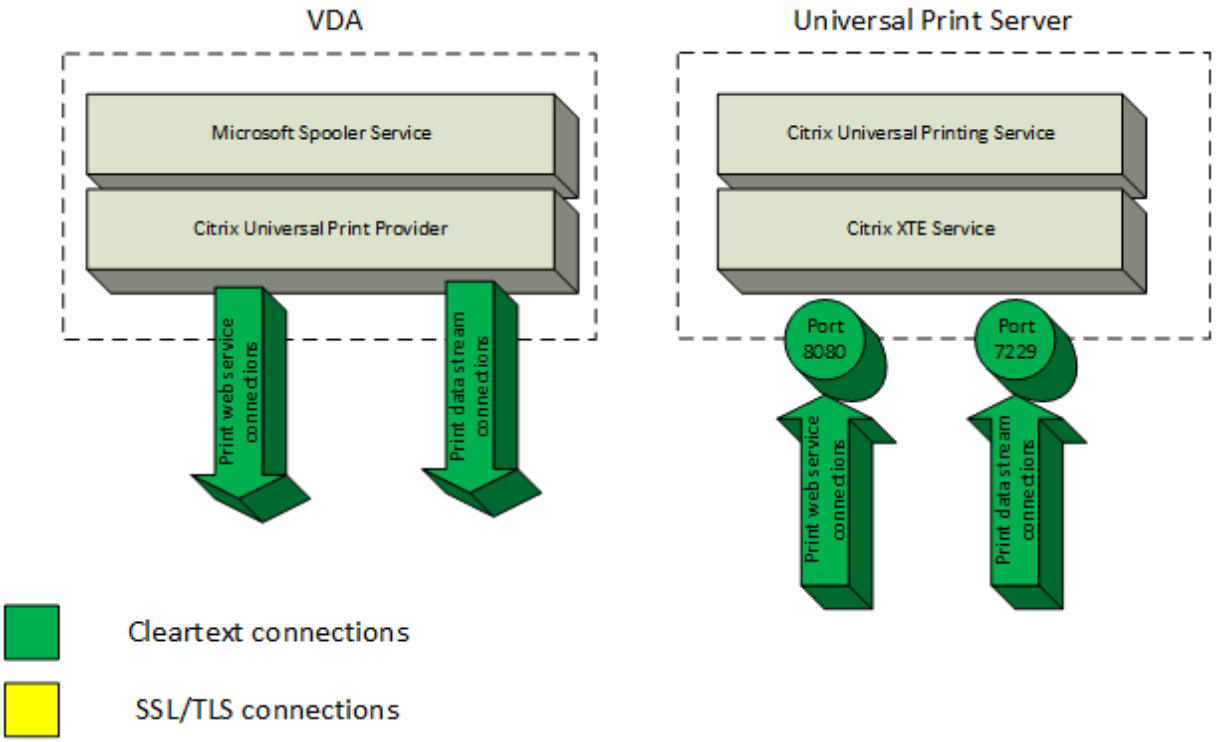
Arten von Druckverbindungen zwischen VDA und universellem Druckserver

Klartextverbindungen

Folgende mit dem Drucken zusammenhängende Verbindungen werden vom VDA mit Ports auf dem universellen Druckserver hergestellt. Die Verbindungen werden nur hergestellt, wenn die Richtlinieneinstellung **SSL aktiviert** auf die Standardeinstellung **Deaktiviert** festgelegt ist.

- Klartext-Druckwebdienstverbindungen (TCP-Port 8080)
- Klartext-Druckdatenstromverbindungen (CGP, TCP-Port 7229)

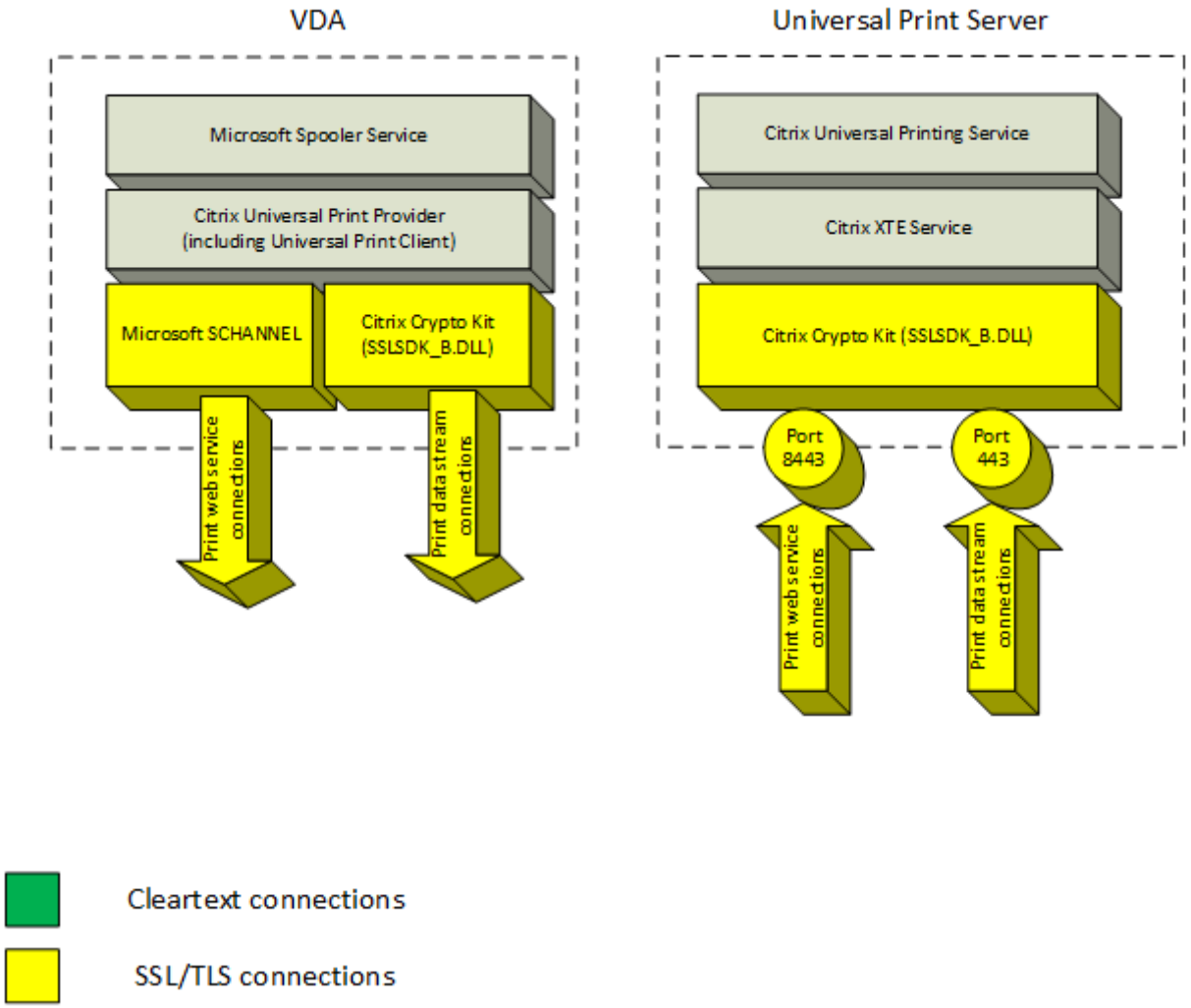
Im Artikel Dienstübersicht und Netzwerkportanforderungen für Windows des Microsoft-Supports werden die vom Microsoft Windows-Druckspoolerdienst verwendeten Ports beschrieben. Die SSL/TLS -Einstellungen in diesem Dokument gelten nicht für die NETBIOS- und RPC-Verbindungen, die vom Windows-Druckspoolerdienst hergestellt werden. Der VDA verwendet den Windows-Druckanbieter (win32spl.dll) als Fallback, wenn die Richtlinieneinstellung **Universellen Druckserver aktivieren** auf **Aktiviert mit Fallback auf systemeigenen Windows-Remotedruck** festgelegt ist.



Verschlüsselte Verbindungen

Folgende mit dem Drucken zusammenhängende SSL/TLS-Verbindungen werden vom VDA mit Ports auf dem universellen Druckserver hergestellt. Die Verbindungen werden nur hergestellt, wenn die Richtlinieneinstellung **SSL aktiviert** auf **Aktiviert** festgelegt ist.

- Verschlüsselte Druckwebdienstverbindungen (TCP-Port 8443)
- Verschlüsselte Druckdatenstromverbindungen (CGP, TCP-Port 443)



SSL/TLS-Clientkonfiguration

Der VDA fungiert als SSL/TLS-Client.

Verwenden Sie die Microsoft-Gruppenrichtlinie und die Registrierung, um Microsoft SCHANNEL SSP für verschlüsselte Druckwebdienstverbindungen (TCP-Port 8443) zu konfigurieren. Die Registrierungseinstellungen für Microsoft SCHANNEL SSP werden in dem Artikel Registrierungseinstellungen für Transport Layer Security (TLS) des Microsoft-Supports beschrieben.

Rufen Sie auf dem VDA (Windows Server 2016/Windows 10) 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_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256

> **Hinweis:**
>
> Wenn diese Gruppenrichtlinieneinstellung konfiguriert ist, wählt der VDA nur dann eine Verschlüsselungssammlung für verschlüsselte Druckwebdienstverbindungen (Standardport: 8443), wenn die Verbindungen in beiden SSL-Verschlüsselungssammlungslisten aufgeführt werden:
>
> - Gruppenrichtlinie –Reihenfolge der SSL-Verschlüsselungssammlungen
> - Liste gemäß Einstellung der Richtlinie "SSL-Verschlüsselungssammlung"(COM, GOV oder ALL)
>
> 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 für die Reihenfolge der Verschlüsselungssammlungen hinzufügen.
>
> **Wichtig:**
>
> Gruppenrichtlinienänderungen für die TLS-Konfiguration werden erst nach einem Neustart des Betriebssystems wirksam.
>
> Verwenden Sie eine Citrix Richtlinie zum Konfigurieren der SSL/TLS-Einstellungen für verschlüsselte Druckdatenstromverbindungen (CGP, TCP-Port 443).

SSL/TLS-Serverkonfiguration

Der universelle Druckserver fungiert als SSL/TLS-Server.

Verwenden Sie das PowerShell-Skript `Enable-UpsSsl.ps1`, um SSL/TLS-Einstellungen zu konfigurieren.

Installieren des TLS-Serverzertifikats auf dem universellen Druckserver

Für HTTPS unterstützt der universelle Druckserver TLS-Features über Serverzertifikate. Clientzertifikate werden nicht verwendet. Verwenden Sie Microsoft Active Directory-Zertifikatdienste oder eine andere Zertifizierungsstelle, um ein Zertifikat für den universellen Druckserver anzufordern.

Beachten Sie beim Registrieren/Anfordern eines Zertifikats über Active Directory-Zertifikatdienste Folgendes:

1. Speichern Sie das TLS-Zertifikat auf dem lokalen Computer im Zertifikatspeicher **Eigene Zertifikate**.

2. Legen Sie für das Attribut **CN** des Distinguished Name (DN) des Antragstellers den vollqualifizierten des universellen Druckservers fest. Geben Sie dies in der Zertifikatvorlage an.
3. Legen Sie den Kryptografiedienstanbieter zum Generieren der Zertifikatanforderung und des privaten Schlüssels auf **Microsoft Enhanced RSA and AES Cryptographic Provider** fest. Geben Sie dies in der Zertifikatvorlage an.
4. Legen Sie die Schlüsselgröße auf mindestens 2048 Bit fest. Geben Sie dies in der Zertifikatvorlage an.

Konfigurieren von SSL auf dem universellen Druckserver

Der XTE-Dienst auf dem universellen Druckserver überwacht auf eingehende Verbindungen. Er fungiert als SSL-Server, wenn SSL aktiviert ist. Es gibt eingehende Verbindungen zweierlei Art: Druckwebdienstverbindungen mit Druckbefehlen und Druckdatenstromverbindungen mit Druckaufträgen. SSL kann für diese Verbindungen aktiviert werden. SSL schützt die Vertraulichkeit und Integrität dieser Verbindungen. Standardmäßig ist SSL deaktiviert.

Das zum Konfigurieren von SSL verwendete PowerShell-Skript befindet sich auf dem Installationsmedium unter folgendem Dateinamen: `\Support\Tools\SslSupport\Enable-UpsSsl.ps1`.

Konfigurieren von Überwachungsportnummern auf dem universellen Druckserver

Standardports für den XTE-Dienst:

- TCP-Port für Klartext-Druckwebdienst (HTTP): 8080
- TCP-Port für Klartext-Druckdatenströme (CGP): 7229
- TCP-Port für verschlüsselten Druckwebdienst (HTTPS): 8443
- TCP-Port für verschlüsselte Druckdatenströme (CGP): 443

Zum Ändern der vom XTE-Dienst auf dem universellen Druckserver verwendeten Ports führen Sie die folgenden PowerShell-Befehle als Administrator aus (zur Verwendung des PowerShell-Skripts Enable-upsssl.ps1 siehe weiter unten):

1. `Stop-Service CitrixXTEServer, UpSvc`
2. `Enable-UpsSsl.ps1 -Enable -HTTPSPort <port> -CGPSSLPort <port>`
   oder `Enable-UpsSsl.ps1 -Disable -HTTPPort <port> -CGPPort <port>`
3. `Start-Service CitrixXTEServer`

TLS-Einstellungen auf dem universellen Druckserver

Wenn Sie mehrere universelle Druckserver in einer Konfiguration mit Lastausgleich ausführen, müssen die TLS-Einstellungen bei allen gleich konfiguriert sein.

Wenn Sie TLS auf einem universellen Druckserver konfigurieren, werden Berechtigungen für das installierte TLS-Zertifikat geändert. Der universelle Druckdienst erhält Lesezugriff auf den privaten Schlüssel des Zertifikats und wird über Folgendes informiert:

- Das für TLS zu verwendende Zertifikat im Zertifikatspeicher
- Die für TLS-Verbindungen zu verwendenden TCP-Portnummern.

Die Windows-Firewall (wenn sie aktiviert ist) muss so konfiguriert sein, dass eingehende Verbindungen für diese TCP-Ports zugelassen sind. Diese Konfiguration wird für Sie ausgeführt, wenn Sie das PowerShell-Skript Enable-UpsSsl.ps1 verwenden.

- Welche Versionen des TLS-Protokolls zulässig sind.

Der universelle Druckserver unterstützt die TLS-Protokollversionen 1.2, 1.1 und 1.0. Geben Sie die niedrigste zulässige Version an.

Die Standardversion des TLS-Protokolls ist 1.2.

- Welche TLS-Verschlüsselungssammlungen zugelassen werden sollen.

Über eine Verschlüsselungssammlung werden die Kryptografiealgorithmen für eine Verbindung gewählt. VDAs und universeller Druckserver können verschiedene Gruppen von Verschlüsselungssammlungen unterstützen. Wenn ein VDA eine Verbindung herstellt und eine Liste unterstützter TLS-Verschlüsselungssammlungen übermittelt, ordnet der universelle Druckserver eine Verschlüsselungssammlung des Clients einer Sammlung in seiner eigenen Liste konfigurierter Verschlüsselungssammlungen zu und akzeptiert die Verbindung. Gibt es keine übereinstimmende Verschlüsselungssammlung, lehnt der universelle Druckserver die Verbindung ab.

Der universelle Druckserver unterstützt die Verschlüsselungssammlungen GOV (government), COM (commercial) und ALL für die nativen Crypto Kit-Modi OPEN, FIPS und SP800-52. Welche Verschlüsselungssammlungen akzeptiert werden, hängt auch von der Richtlinieneinstellung **SSL FIPS-Modus** und vom Windows-FIPS-Modus ab. Weitere Informationen zum Windows-FIPS-Modus finden Sie in diesem Artikel des Microsoft-Supports.

Verschlüsselungssammlung (in Reihenfolge abnehmender Priorität)	OPEN ALL	OPEN COM	OPEN GOV	FIPS ALL	FIPS COM	FIPS GOV	SP800-52 ALL	SP800-52 COM	SP800-52 GOV
TLS_ECDHE_RSA_AES256_GCM_SHA384	X		X	X		X	X		X
TLS_ECDHE_RSA_AES256_CBC_SHA384	X		X	X		X	X		X
TLS_ECDHE_RSA_AES256_CBC_SHA	X			X	X		X	X	

Konfigurieren von TLS auf einem universellen Druckserver mit dem PowerShell-Skript

Installieren Sie das TLS-Zertifikat im Bereich **Lokaler Computer > Eigene Zertifikate > Zertifikate** des Zertifikatspeichers. Sind mehrere Zertifikate an diesem Speicherort, geben Sie den Fingerabdruck des Zertifikats im PowerShell-Skript `Enable-UpsSsl.ps1` an.

> **Hinweis:**
>
> Das PowerShell-Skript findet das richtige Zertifikat basierend auf dem FQDN des universellen Druckservers. Sie brauchen den Zertifikatfingerabdruck nicht angeben, wenn nur ein Zertifikat für den FQDN des universellen Druckservers vorhanden ist.

Das Skript `Enable-UpsSsl.ps1` aktiviert bzw. deaktiviert TLS-Verbindungen vom VDA zum universellen Druckserver. Dieses Skript ist im Ordner **Support > Tools > SslSupport** auf dem Installationsmedium.

Wenn Sie TLS aktivieren, deaktiviert das Skript alle vorhandenen Windows-Firewallregeln für die angegebenen TCP-Ports des universellen Druckservers. Anschließend werden neue Regeln hinzugefügt, durch die der XTE-Dienst eingehende Verbindungen nur am TLS-, TCP- und UDP-Port annehmen kann. Außerdem werden die Windows-Firewallregeln für Folgendes deaktiviert:

- Klartext-Druckwebdienstverbindungen (Standard: 8080)
- Klartext-Druckdatenstromverbindungen (CGP, Standard: 7229)

Der VDA kann diese Verbindungen nur bei Verwendung von TLS herstellen.

> **Hinweis:**
>
> Das Aktivieren von TLS wirkt sich nicht auf Windows-Druckspooler-RPC- bzw. SMB-Verbindungen vom VDA zum universellen Druckserver aus.
>
> **Wichtig:**
>
> Geben Sie als ersten Parameter **Enable** oder **Disable** an. Der Parameter "CertificateThumbprint" ist optional, wenn nur ein Zertifikat im Zertifikatspeicher "Eigene Zertifikate"des lokalen Computers den FQDN des universellen Druckservers hat. Die übrigen Parameter sind optional.

Syntax

```
1 Enable-UpsSSL.ps1 -Enable [-HTTPPort <port>] [-CGPPort <port>] [-
      HTTPSPort <port>] [-CGPSSLPort <port>] [-SSLMinVersion <version>] [-
      SSLCipherSuite <name>] [-CertificateThumbprint <thumbprint>] [-
      FIPSMode <Boolean>] [-ComplianceMode <mode>]
2 Enable-UpsSSL.ps1 -Disable [-HTTPPort <portnum>] [-CGPPort <portnum>]
```

Parameter	Beschreibung
Smartcard	Aktiviert SSL/TLS auf dem XTE-Server. Es ist dieser Parameter oder der Parameter "Disable" erforderlich.
Deaktivieren	Deaktiviert SSL/TLS auf dem XTE-Server. Es ist dieser Parameter oder der Parameter "Enable" erforderlich.
CertificateThumbprint "<thumbprint>"	Fingerabdruck des TLS-Zertifikats im Zertifikatspeicher "Eigene Zertifikate"des lokalen Computers in Anführungszeichen. Das Skript verwendet den angegebenen Fingerabdruck zur Auswahl des gewünschten Zertifikats.
HTTPPort <port>	Port für den Klartext-Druckwebdienst (HTTP/SOAP). Standard: 8080
CGPPort <port>	Port für Klartext-Druckdatenströme (CGP). Standard: 7229
HTTPSPort <port>	Port für verschlüsselten Druckwebdienst (HTTPS/SOAP). Standard: 8443
CGPSSLPort <port>	Port für verschlüsselte Druckdatenströme (CGP). Standard: 443.

Parameter	Beschreibung
SSLMinVersion "<version>"	Mindestversion des TLS-Protokolls zwischen Anführungszeichen. Gültige Werte: “TLS_1.0”, “TLS_1.1”und “TLS_1.2”. Standard: TLS_1.2.
SSLCipherSuite “ <name>”	Name des TLS-Verschlüsselungssammlungspakets in Anführungszeichen. Gültige Werte: “GOV”, “COM”und “ALL”(Standardwert).
FIPSMode <Boolean>	Aktiviert oder deaktiviert den FIPS 140-Modus im XTE-Server. Gültige Werte: $true zum Aktivieren des FIPS 140-Modus, $false zum Deaktivieren.

Beispiele

Das folgende Skript aktiviert TLS. Der Fingerabdruck (im Beispiel dargestellt als “12345678987654321”) dient zur Auswahl des Zertifikats, das verwendet werden soll.

```
Enable-UpsSsl.ps1 –Enable -CertificateThumbprint "12345678987654321"
```

Das folgende Skript deaktiviert TLS.

```
Enable-UpsSsl.ps1 –Disable
```

Konfigurieren des FIPS-Modus

Durch Aktivieren des FIPS-Modus (US Federal Information Processing Standards) wird sichergestellt, dass nur FIPS 140-konforme Kryptografie für verschlüsselte Verbindungen mit dem universellen Druckserver verwendet wird.

Konfigurieren Sie den FIPS-Modus auf dem Server, bevor Sie ihn auf dem Client konfigurieren.

Informationen zum Aktivieren und Deaktivieren des Windows-FIPS-Modus finden Sie online in der Microsoft-Dokumentation.

Aktivieren des FIPS-Modus auf dem Client

Führen Sie auf dem Delivery Controller Citrix Studio aus und legen Sie die Citrix Richtlinieneinstellung **SSL FIPS-Modus** auf **Aktiviert** fest. Aktivieren Sie die Citrix Richtlinie.

Gehen Sie auf jedem VDA folgendermaßen vor:

1. Aktivieren Sie den Windows-FIPS-Modus.
2. Starten Sie den VDA neu.

Aktivieren des FIPS-Modus auf dem Server

Gehen Sie für jeden universellen Druckserver folgendermaßen vor:

1. Aktivieren Sie den Windows-FIPS-Modus.
2. Führen Sie folgenden PowerShell-Befehl als Administrator aus: `stop-service CitrixXTEServer, UpSvc`
3. Führen Sie das Skript `Enable-UpsSsl.ps1` für jedes Paket mit den Parametern `-Enable -FIPSMode $true` aus:
4. Starten Sie den universellen Druckserver neu.

Deaktivieren des FIPS-Modus auf dem Client

Führen Sie auf dem Delivery Controller Citrix Studio aus und legen Sie die Citrix Richtlinieneinstellung **SSL FIPS-Modus** auf **Deaktiviert** fest. Aktivieren Sie die Citrix Richtlinie. Sie können die Citrix Richtlinieneinstellung **SSL FIPS-Modus** auch löschen.

Gehen Sie auf jedem VDA folgendermaßen vor:

1. Deaktivieren Sie den Windows-FIPS-Modus.
2. Starten Sie den VDA neu.

Deaktivieren des FIPS-Modus auf dem Server

Gehen Sie für jeden universellen Druckserver folgendermaßen vor:

1. Deaktivieren Sie den Windows-FIPS-Modus.
2. Führen Sie folgenden PowerShell-Befehl als Administrator aus: `stop-service CitrixXTEServer, UpSvc`
3. Führen Sie das Skript `Enable-UpsSsl.ps1` für jedes Paket mit den Parametern `-Enable -FIPSMode $false` aus:
4. Starten Sie den universellen Druckserver neu.

Konfigurieren der SSL/TLS-Protokollversion

Die Standardversion des SSL/TLS-Protokolls ist TLS 1.2. TLS 1.2 ist die einzige SSL/TLS-Protokollversion, die für Produktionszwecke empfohlen wird. Zur Problembehandlung muss die SSL/TLS-Protokollversion in einer Umgebung außerhalb der Produktion ggf. vorübergehend geändert werden.

SSL 2.0 und SSL 3.0 werden vom universellen Druckserver nicht unterstützt.

Festlegen der SSL/TLS-Protokollversion auf dem Server

Gehen Sie für jeden universellen Druckserver folgendermaßen vor:

1. Führen Sie folgenden PowerShell-Befehl als Administrator aus: `stop-service CitrixXTEServer , UpSvc`
2. Führen Sie das Skript `Enable-UpsSsl.ps1` für jedes Paket mit den Versionsparametern `-Enable -SSLMinVersion` aus: Vergessen Sie nicht, die Version nach dem Testen wieder auf TLS 1.2 zu setzen.
3. Starten Sie den universellen Druckserver neu.

Festlegen der SSL/TLS-Protokollversion auf dem Client

Gehen Sie auf jedem VDA folgendermaßen vor:

1. Legen Sie auf dem Delivery Controller die Richtlinieneinstellung **SSL-Protokollversion** auf die gewünschte Version fest und aktivieren Sie die Richtlinie.

2. Die Registrierungseinstellungen für Microsoft SCHANNEL SSP werden in dem Artikel Registrierungseinstellungen für Transport Layer Security (TLS) des Microsoft-Supports beschrieben. Aktivieren Sie clientseitig **TLS 1.0, TLS 1.1 oder TLS 1.2** per Registrierungseinstellung.

> **Wichtig:**
>
> Vergessen Sie nicht, die Registrierungseinstellung nach dem Testen wieder auf die ursprüngliche Einstellung zurückzusetzen.

3. Starten Sie den VDA neu.

Problembehandlung

Bei Verbindungsfehlern überprüfen Sie die Protokolldatei (C:\Programme (x86)\Citrix\XTE\logs\error.log) auf dem universellen Druckserver.

Die Fehlermeldung **SSL handshake from client failed** erscheint in der Protokolldatei, wenn der SSL/TLS-Handshake fehlschlägt. Solche Fehler können auftreten, wenn die SSL/TLS-Protokollversion auf dem VDA nicht mit der auf dem universellen Druckserver übereinstimmt.

Verwenden Sie den FQDN des universellen Druckservers in den folgenden Richtlinieneinstellungen, die Hostnamen des universellen Druckservers enthalten:

- Sitzungsdrucker

- Druckerzuordnungen
- Universelle Druckserver für den Lastausgleich

Stellen Sie sicher, dass auf den universellen Druckservern und den VDAs die Systemuhr (Datum, Uhrzeit und Zeitzone) richtig eingestellt ist.

Sicherheit virtueller Kanäle

January 24, 2022

Die Positivliste für virtuelle Kanäle ist standardmäßig deaktiviert. Wenn aktiviert, dürfen nur virtuelle Citrix Kanäle in virtuellen App- und Desktop-Sitzungen geöffnet werden. Ist die Verwendung benutzerdefinierter virtueller Kanäle erforderlich (eigener oder derer eines Dritten), müssen diese der Positivliste hinzugefügt werden.

Hinzufügen virtueller Kanäle zur Positivliste

Zum Hinzufügen eines virtuellen Kanals zur Positivliste benötigen Sie Folgendes:

1. Den Namen des virtuellen Kanals gemäß Definition im Code (bis zu sieben Zeichen lang). Beispiel: `CTXCVC1`.
2. Die Pfade zu den Prozessen, die den virtuellen Kanal auf der VDA-Maschine öffnen. Beispiel: `C:\Program Files\Application\run.exe`.

Wenn Sie die erforderlichen Informationen zur Hand haben, müssen Sie den virtuellen Kanal über die Richtlinieneinstellung für Positivliste virtueller Kanäle der Positivliste hinzufügen. Zum Eintragen eines virtuellen Kanals in die Liste geben Sie den Namen des virtuellen Kanals gefolgt von einem Komma und dem Pfad zu dem Prozess ein, der auf den virtuellen Kanal zugreift. Mehrere Prozesse können durch Kommas getrennt hinzugefügt werden.

> **Hinweis:**
>
> Nachdem Sie Änderungen an der Richtlinie vorgenommen haben, starten Sie den VDA neu, um sicherzustellen, dass die Änderungen wirksam werden.

Im Fall der o. g. Beispiele würden Sie der Liste Folgendes hinzufügen:

```
CTXCVC1,C:\Program Files\Application\run.exe
```

Im Fall mehrerer Prozesse würden Sie Folgendes hinzufügen:

```
CTXCVC1,C:\Program Files\Application\run.exe,C:\Program Files\Application
\run2.exe
```


Überlegungen zu virtuellen Citrix Kanälen

Alle integrierten virtuellen Citrix Kanäle haben eine Vertrauensstellung und können ohne weitere Konfiguration geöffnet werden. Zwei Features erfordern jedoch aufgrund externer Abhängigkeiten einen expliziten Eintrag in der Positivliste:

- Multimediaumleitung
- HDX RealTime Optimization Pack für Skype for Business

Multimediaumleitung

Folgende Informationen sind für den Eintrag in der Liste erforderlich:

- Name des virtuellen Kanals: CTXMM
- Prozess: Pfad zu dem auf dem VDA verwendeten Media Player. Beispiel: C:\Programme (x86)\Windows Media Player\wmplayer.exe
- Eintrag in Positivliste: `CTXMM,C:\Program Files (x86)\Windows Media Player\wmplayer.exe`

HDX RealTime Optimization Pack für Skype for Business

Folgende Informationen sind für den Eintrag in der Liste erforderlich:

- Name des virtuellen Kanals: CTXRMEP
- Prozess: Pfad zu der Exe-Datei von Skype for Business auf der VDA-Maschine. Dieser variiert ggf. je nach Skype for Business-Version bzw. kann ein benutzerdefinierter Installationspfad sein. Beispiel: C:\Programme\Microsoft Office\root\Office16\lync.exe.
- Eintrag in Positivliste: `CTXRMEP,C:\Program Files\Microsoft Office\root\Office16\lync.exe`

Erhalt der Namen und Prozesse virtueller Kanäle

Die einfachste Art und Weise, den Namen eines virtuellen Kanals und den Prozess, der ihn auf der VDA-Maschine öffnet, in Erfahrung zu bringen, ist den Entwickler oder Drittanbieter des Kanals zu fragen.

Alternativ können Sie diese Informationen über die Protokolle des Features und die folgenden Schritte erhalten:

1. Sobald die Client- und Serverkomponenten des benutzerdefinierten virtuellen Kanals bereit sind, starten Sie eine virtuelle Anwendung oder einen virtuellen Desktop.
2. Suchen Sie im Systemereignisprotokoll der VDA-Maschine den Namen des benutzerdefinierten virtuellen Kanals in folgendem Ereignis:

- Bei Einzelsitzungs-VDAs Ereignis-ID 2004 aus Picadd.
- Bei Multisitzungs-VDAs Ereignis-ID 16 aus Rpm.

3. Melden Sie sich von der Sitzung ab.
4. Fügen Sie in der Richtlinieneinstellung für die Positivliste virtueller Kanäle für den gefundenen virtuellen Kanal einen Eintrag mit dessen Namen hinzu.
5. Starten Sie den VDA neu.
6. Starten Sie die virtuelle Anwendung oder den virtuellen Desktop neu.
7. Suchen Sie im Systemereignisprotokoll der VDA-Maschine den Namen des Prozesses, der den virtuellen Kanal zu öffnen versucht, in folgendem Ereignis:

   - Bei Einzelsitzungs-VDAs Ereignis-ID 2002 aus Picadd.
   - Bei Multisitzungs-VDAs Ereignis-ID 14 aus Rpm.

8. Melden Sie sich von der Sitzung ab.
9. Bearbeiten Sie den Eintrag in der Richtlinieneinstellung für die Positivliste virtueller Kanäle unter Hinzufügen des gefundenen Prozesses.
10. Starten Sie den VDA neu.
11. Starten Sie die virtuelle Anwendung oder den virtuellen Desktop, um zu überprüfen, ob der benutzerdefinierte virtuelle Kanal erfolgreich geöffnet wird.

Protokollierung –Positivliste virtueller Kanäle

Die folgenden Ereignisse werden im Ereignisprotokoll eines Einzelsitzungs-VDAs protokolliert:

	Protokolldateiname	System
	ID	2001
	Quelle	Picadd
	Ebene	Information
	Beschreibung	Der benutzerdefinierte virtuelle Kanal <vcName> wurde von Prozess <processName> geöffnet

	Protokolldateiname	System

	ID	2002
	Quelle	Picadd
	Ebene	Warnung
	Beschreibung	Der benutzerdefinierte virtuelle Kanal <vcName> kann von Prozess <processName> nicht geöffnet werden

	Protokolldateiname	System
	ID	2003
	Quelle	Picadd
	Ebene	Information
	Beschreibung	<username> hat den benutzerdefinierten Kanal <vcName> geöffnet

	Protokolldateiname	System
	ID	2004
	Quelle	Picadd
	Ebene	Warnung
	Beschreibung	<username> hat versucht, den benutzerdefinierten virtuellen Kanal <vcName> zu öffnen

Die folgenden Ereignisse werden im Ereignisprotokoll eines Multisitzungs-VDAs protokolliert:

Protokolldateiname	System
ID	13
Quelle	Rpm
Ebene	Information
Beschreibung	Der benutzerdefinierte virtuelle Kanal <vcName> wurde von Prozess <processName> geöffnet

Protokolldateiname	System
ID	14
Quelle	Rpm
Ebene	Warnung
Beschreibung	Der benutzerdefinierte virtuelle Kanal <vcName> kann von Prozess <processName> nicht geöffnet werden

Protokolldateiname	System
ID	15
Quelle	Rpm
Ebene	Information
Beschreibung	<username> hat den benutzerdefinierten Kanal <vcName> geöffnet

Protokolldateiname	System
ID	16
Quelle	Rpm
Ebene	Warnung
Beschreibung	<username> hat versucht, den benutzerdefinierten virtuellen Kanal <vcName> zu öffnen

Bekannte virtuelle Kanäle von Drittanbietern

Die folgenden Drittanbieterlösungen verwenden bekanntermaßen benutzerdefinierte virtuelle Citrix Kanäle. Diese Liste enthält nicht jede Lösung, die einen benutzerdefinierten virtuellen Citrix Kanal verwendet.

- Cerner
- Cisco WebEx-Teams
- Cisco WebEx Meetings Virtual Desktop-Software
- Epic Warp Drive
- Midmark IQPath-Clienterweiterungen
- Nuance PowerMic-Clienterweiterungen
- Nuance Dragon Medical Network Edition 360 vSync
- Zoom Meetings für VDI

Um Details zum Hinzufügen der zugehörigen virtuellen Kanäle zur Positivliste zu erhalten, wenden Sie sich an die Hersteller der jeweiligen Lösung. Alternativ führen Sie die Schritte unter Erhalt der Namen und Prozesse virtueller Kanäle aus.

Geräte

February 19, 2020

HDX bietet eine High Definition-Benutzererfahrung auf jedem Gerät an jedem Ort. Im Abschnitt “Geräte”werden folgende Geräte behandelt:

- Generische USB-Geräte

- Mobile und Touchscreengeräte
- Serielle Geräte
- Spezialtastaturen
- TWAIN-Geräte
- Webcams

Vergleich: optimierte und generische USB-Geräte

Ein optimiertes USB-Gerät ist eines, für das die Citrix Workspace-App spezifische Unterstützung bietet. Beispiel ist die Möglichkeit der Webcamumleitung über den virtuellen HDX-Multimediakanal. Für generische USB-Geräte bietet die Citrix Workspace-App keine spezifische Unterstützung.

Standardmäßig kann die generische USB-Umleitung USB-Geräte mit optimierter Unterstützung für virtuelle Kanäle nur nach einem Wechsel in den generischen Modus umleiten.

Im Allgemeinen erzielen Sie im optimierten Modus eine bessere Leistung für USB-Geräte als im generischen Modus. In Einzelfällen bieten USB-Geräte im optimierten Modus jedoch nicht den vollen Funktionsumfang. Es kann ein Wechsel in den generischen Modus erforderlich sein, um vollen Zugriff auf alle Funktionen zu erhalten.

Für USB-Massenspeichergeräte können Sie die Clientlaufwerkzuordnung, die generische USB-Umleitung oder beides über Citrix Richtlinien verwenden. Die Hauptunterschiede sind folgende:

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 folgende Bedingungen erfüllt sind, wird das Massenspeichergerät mit der generischen USB-Umleitung umgeleitet:

- Sowohl die Richtlinie für die generische USB-Umleitung als auch diejenige für die Clientlaufwerkzuordnung ist aktiviert.
- Es ist ein Gerät für die automatische Umleitung konfiguriert.
- Ein Massenspeichergerät wird entweder vor oder nach dem Start einer Sitzung angeschlossen.

Weitere Informationen finden Sie unter http://support.citrix.com/article/CTX123015.

Feature	Clientlaufwerkszuordnung	Generische USB-Umleitung
Diese Option ist in der Standardeinstellung aktiviert.	Ja	Nein
Konfigurierbare Leserechte	Ja	Nein

Feature	Clientlaufwerkszuordnung	Generische USB-Umleitung
Verschlüsselter Gerätezugriff	Ja, wenn die Verschlüsselung vor dem Zugriff auf das Gerät in der virtuellen Sitzung entsperrt wird	Nur Citrix Virtual Desktops

Generische USB-Geräte

April 19, 2024

HDX-Technologie bietet **optimierte Unterstützung** für die gebräuchlichsten USB-Geräte. Diese Geräte umfassen:

- 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. Weitere Informationen zur generischen USB-Umleitung finden Sie unter Generische USB-Umleitung.

Weitere Informationen zu USB-Geräten und der Citrix Workspace-App für Windows finden Sie unter Konfigurieren der Umleitung von USB-Verbundgeräten und [Konfigurieren der USB-Unterstützung].(/de-de/citrix-workspace-app-for-windows/configure/config-xdesktop/config-usb-support.html)

Mobile und Touchscreengeräte

August 10, 2022

Tabletmodus für Touchscreengeräte mit Windows Continuum

Continuum ist ein Windows 10-Feature, das sich an die Art und Weise der Verwendung des Clientgeräts anpasst. Continuum einschließlich des dynamischen Moduswechsels wird ab VDA Version 7.16 und Citrix Receiver für Windows-Version 4.10 unterstützt.

Der Windows 10-VDA erkennt, wenn eine Tastatur oder Maus an einen Client mit Touchscreen angeschlossen ist, und versetzt den Client in den Desktopmodus. Ist keine Tastatur oder Maus vorhanden, versetzt Windows 10-VDA den Client in den Tablet-/Mobilgerätemodus. Die Erkennung erfolgt bei Verbindung und Wiederverbindung. Sie erfolgt außerdem beim dynamischen Anschließen oder Trennen der Tastatur oder Maus.

Das Feature ist in der Standardeinstellung aktiviert. Zum Deaktivieren dieser Version des Features bearbeiten Sie die Richtlinieneinstellungen für den Tabletmodus.

Zum Deaktivieren der Version des Features in XenApp 7.14 und 7.15 LTSR und XenDesktop 7.14 und 7.15 LTSR verwenden Sie die Registrierungseinstellungen. Weitere Informationen finden Sie unter Tabletmodus für Geräte mit Touchscreen.

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.

Der **Desktopmodus** ist die klassische Benutzeroberfläche, bei der die Interaktion wie bei einem PC mit Tastatur und Maus erfolgt.

Für den Tabletmodus ist als Mindestversion Citrix Hypervisor 8.2 CU1 LTSR erforderlich. Citrix Hypervisor wird im Citrix Virtual Desktops-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 Desktopmodus innerhalb der virtuellen Maschine verwendet.

Die Citrix Workspace-App für HTML5 (Light-Version) unterstützt keine Windows Continuum-Features.

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

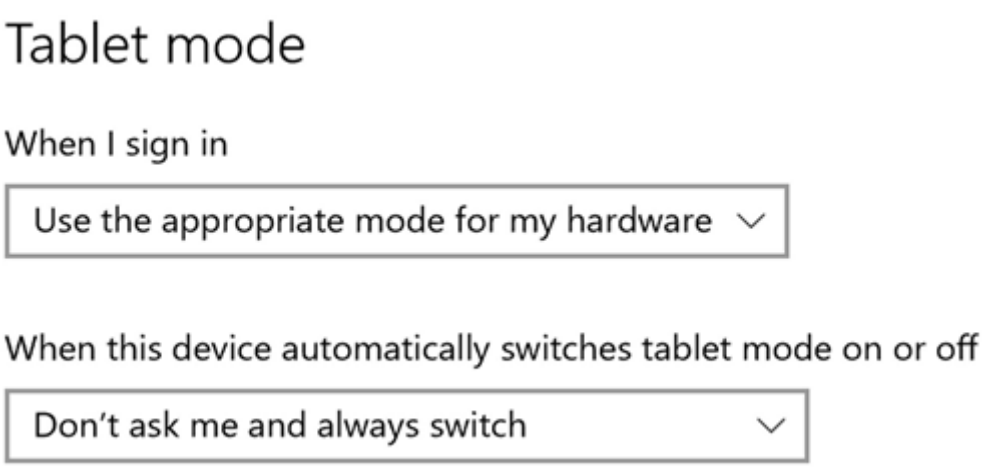
> **Wichtig:**
> Das Aktualisieren des Basisimages eines Maschinenkatalogs nach dem Ändern der Metadateneinstellung hat keine Auswirkungen auf zuvor bereitgestellte VMs. Nachdem Sie das XenServer-VM-Basisimage geändert haben, erstellen Sie einen Katalog, wählen Sie das Basisimage aus, und stellen Sie eine neue MCS-Maschine bereit.

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.



Microsoft Surface Pro und Surface Book-Stifte

Standardstiftfunktionen bei Windows Ink-basierten Anwendungen werden unterstützt. Für diese Funktionalität ist ein Virtual Delivery Agent mit mindestens Microsoft Windows 10 Version 1809 und ein Clientgerät mit mindestens Citrix Workspace-App für Windows Version 1902 erforderlich. Dies umfasst Zeigen, Löschen, Stiftdruck, Bluetooth-Signale und andere Features je nach Betriebssystem-Firmware und Stiftmodell. Der Stiftdruck kann beispielsweise bis zu 4096 Stufen haben. Das Feature ist in der Standardeinstellung aktiviert.

Für eine Demonstration von Windows Ink und der Stiftfunktionalität klicken Sie auf folgende Grafik:

Systemanforderungen

- Citrix Virtual Apps and Desktops: Mindestversion 1903

- Citrix Workspace-App für Windows: Mindestversion 1902
- Microsoft Windows 10: Mindestversion 1809

Deaktivieren oder Aktivieren

Um dieses Feature zu deaktivieren oder zu aktivieren, legen Sie folgenden Registrierungswert fest:

HKEY_LOCAL_MACHINE\Software\ Citrix\Citrix Virtual Desktop Agent\PenApi

Name: DisablePen

Typ: DWORD

Wert:

1 - deaktiviert

0 - aktiviert

Serielle Ports

March 27, 2023

Die meisten neuen PCs haben keine seriellen (COM) Ports. Serielle Ports können problemlos per USB-Konverter hinzugefügt werden. Anwendungen, die für serielle Ports geeignet sind, umfassen häufig Sensoren, Controller, alte Lesegeräte usw. Für manche virtuellen USB-COM-Portgeräte werden herstellerspezifische Treiber anstelle der Windows-Treiber (usbser.sys) verwendet. Mit solchen Treibern können Sie den virtuellen COM-Port des USB-Geräts so festlegen, dass er sich auch bei Anschluss an andere USB-Anschlüsse nicht ändert. Die Einstellung kann über **Geräte-Manager > Anschlüsse (COM & LPT) > Eigenschaften** oder über die Anwendung zur Gerätesteuerung erfolgen.

Mit der Client-COM-Portzuordnung können Geräte, die an einen COM-Port eines Endgeräts angeschlossen sind, in virtuellen Sitzungen verwendet werden. Die Zuordnungen können genau wie andere Netzwerkzuordnungen verwendet werden.

Ein Treiber im Betriebssystem weist jedem COM-Port einen symbolischen Linknamen (COM1, COM2 usw.) zu. Die Anwendungen verwenden den Link, um auf den Port zuzugreifen.

> **Wichtig:**
> Geräte können zwar direkt per USB an Endpunkte angeschlossen werden, dies bedeutet aber nicht, dass sie über die generische USB-Umleitung umgeleitet werden können. Manche USB-Geräte fungieren als virtuelle COM-Ports, auf die Anwendungen wie auf physische serielle Ports zugreifen. Das Betriebssystem kann COM-Ports abstrahieren und sie wie Dateifreigaben behandeln. Zwei gebräuchliche Protokolle für virtuelle COM-Ports sind CDC ACM und MCT.

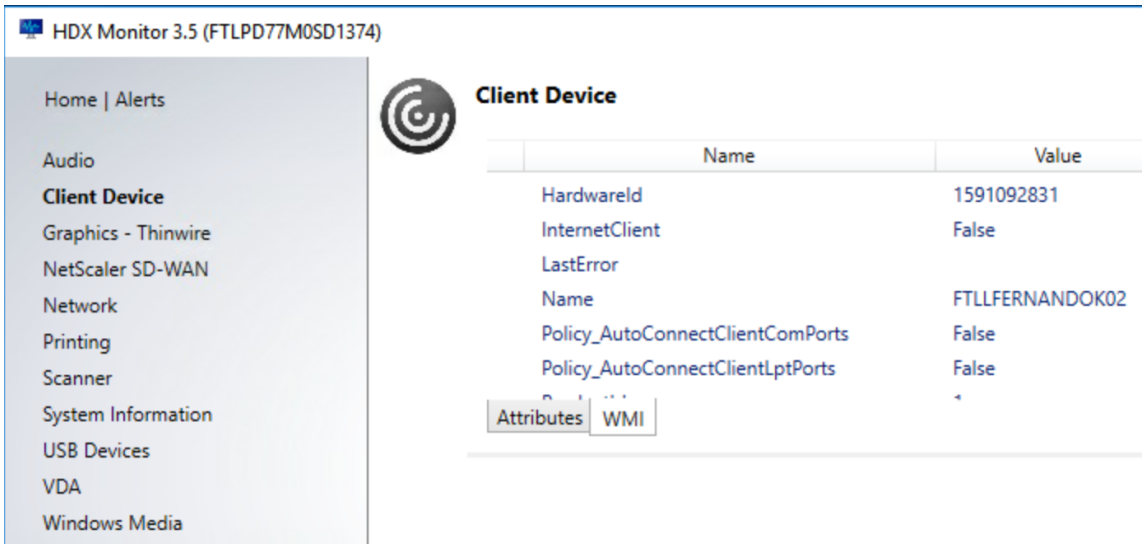
> Bei Anschluss an eine RS-485-Schnittstelle funktionieren Anwendungen evtl. nicht. Mit einem RS-485-zu-RS232-Konverter können Sie RS-485-Schnittstellen als COM-Port verwenden.
> **Wichtig:**
> Einige Anwendungen erkennen ein Gerät (z. B. ein Unterschriftenfeld) nur dann zuverlässig, wenn es über COM1 oder COM2 an der Clientarbeitsstation angeschlossen ist.

Zuordnen eines COM-Ports für Clients zu einem Server-COM-Port

Sie können Client-COM-Ports einer Citrix Sitzung auf dreierlei Weise zuordnen:

- Studio-Richtlinien: Weitere Informationen über Richtlinien finden Sie unter Einstellungen der Richtlinie "Portumleitung".
- VDA-Eingabeaufforderung:
- Konfigurationstool für Remotedesktop (Terminaldienste):

1. Aktivieren Sie die Studio-Richtlinien **Client-COM-Portumleitung** und **Client-COM-Ports automatisch verbinden**. Nach der Anwendung stehen diverse Informationen in HDX Monitor zur Verfügung.



2. Wenn der Port durch **Client-COM-Ports automatisch verbinden** nicht zugeordnet werden kann, können Sie ihn manuell oder über Anmeldeskripts zuordnen. Melden Sie sich beim VDA an und geben Sie in einer Eingabeaufforderung Folgendes ein:

   NET USE COMX: \\CLIENT\COMZ:

   Oder

   NET USE COMX: \\CLIENT\CLIENTPORT:COMZ:

   X ist die Nummer des COM-Ports auf dem VDA (Ports 1 bis 9 stehen für die Zuordnung zur Verfügung). **Z** ist der Name des Client-COM-Ports, den Sie zuordnen möchten.

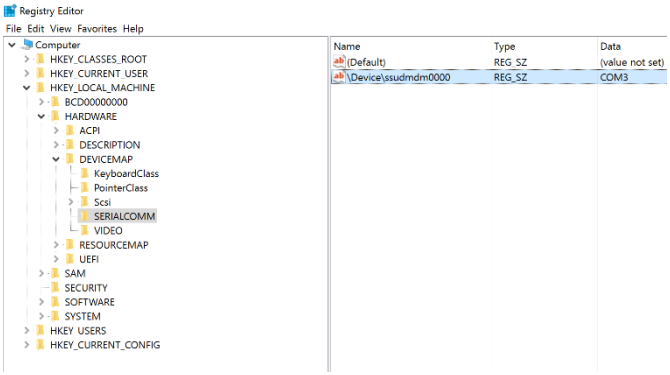
Um zu überprüfen, ob der Vorgang erfolgreich war, geben Sie **NET USE** an einer VDA-Eingabeaufforderung ein. Die angezeigte Liste enthält zugeordnete Laufwerke, LPT- und zugeordnete COM-Ports.

3. Um den COM-Port auf einem virtuellen Desktop oder in einer Anwendung zu verwenden, installieren Sie die Anwendung und verweisen Sie sie auf den zugeordneten Namen. Wenn Sie beispielsweise Port COM1 auf dem Client dem Port COM3 auf dem Server zuordnen, installieren Sie die COM-Portanwendung auf dem VDA und verweisen Sie sie in der Sitzung auf COM3. Verwenden Sie diesen zugeordneten COM-Port dann wie einen COM-Port auf dem Benutzergerät.

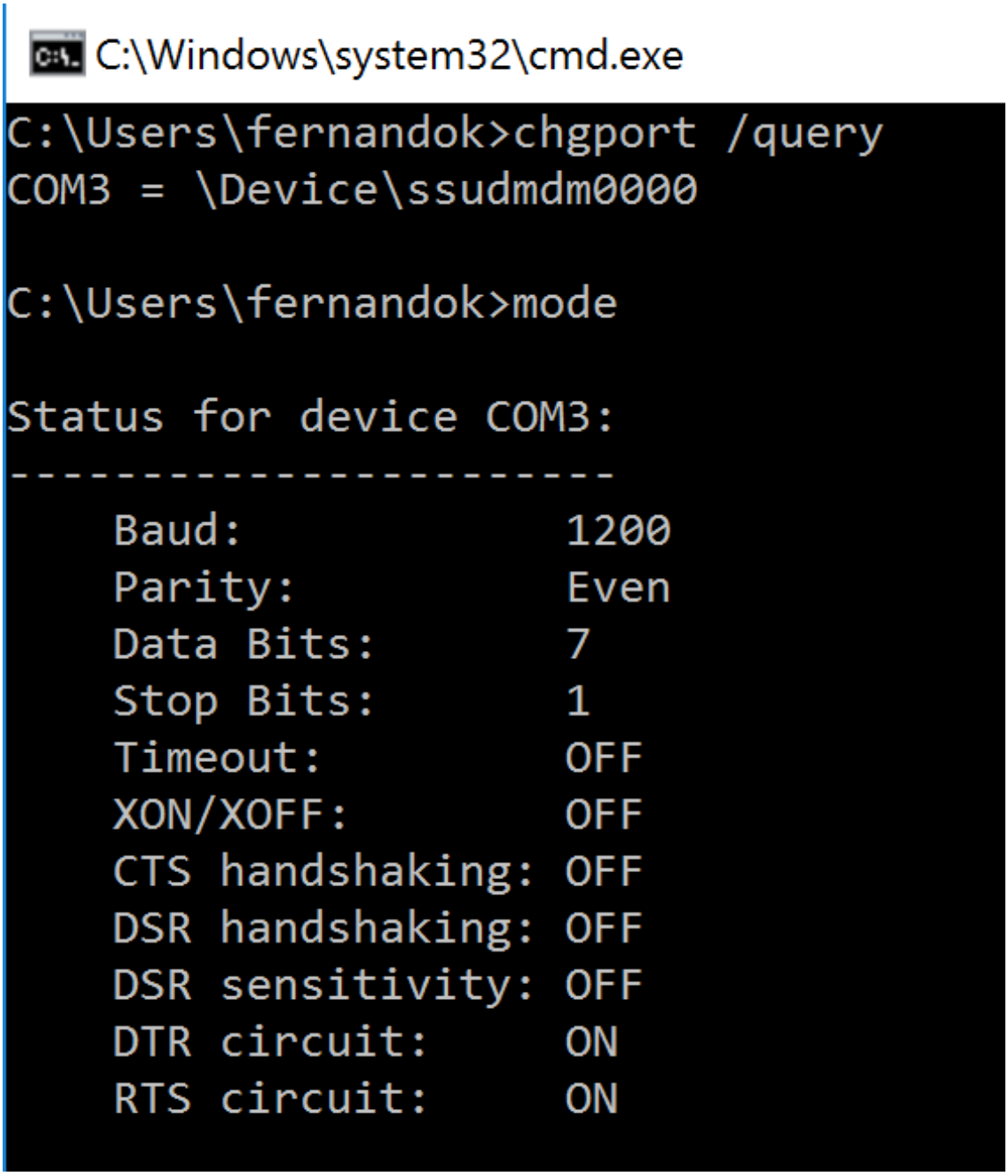
> **Wichtig:**
> Die Zuordnung von COM-Ports ist nicht mit TAPI kompatibel. Sie können TAPI-Geräte (Windows Telephony Application Programming Interface) nicht Client-COM-Ports zuordnen. TAPI definiert eine Standardmethode zur Steuerung von Telefonfunktionen für Daten-, Fax- und Sprachanrufe durch Anwendungen. TAPI übernimmt die Signalverarbeitung (Wählen, Beantworten und Beenden von Anrufen). Außerdem ermöglicht TAPI Dienste wie Halten und Verbinden von Anrufen und Konferenzschaltungen.

Problembehandlung

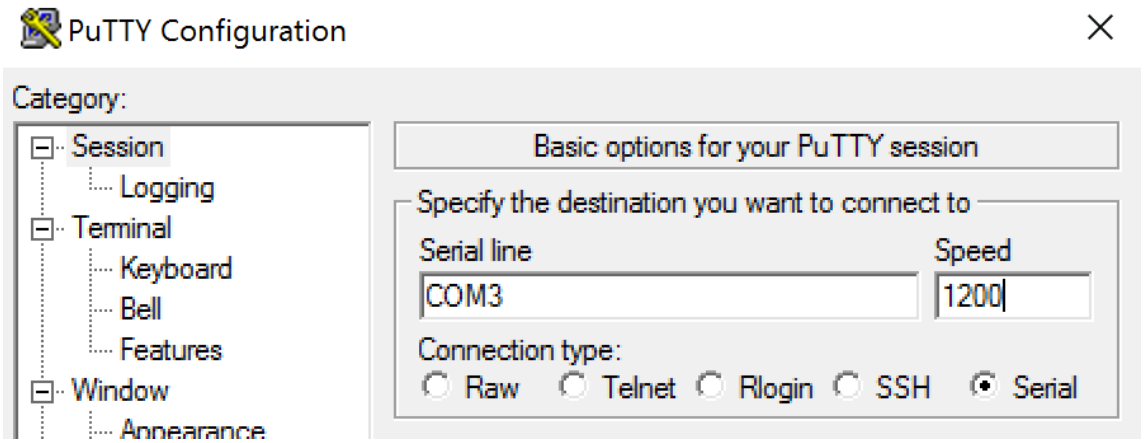
1. Vergewissern Sie sich, dass Sie vom Endpunkt unter Umgehung von Citrix direkt auf das Gerät zugreifen können. Wenn der Port nicht dem VDA zugeordnet ist, sind Sie nicht mit einer Citrix Sitzung verbunden. Folgen Sie allen mit dem Gerät gelieferten Anweisungen zur Problembehandlung und stellen Sie zuerst sicher, dass es lokal funktioniert.
   Wenn ein Gerät an einen seriellen COM-Port angeschlossen wird, wird ein Registrierungsschlüssel mit folgender Struktur erstellt:



Sie finden diese Informationen auch durch Ausführen von chgport **/query** an der Eingabeaufforderung.



Stehen keine Anweisungen zur Fehlerbehebung für das Gerät zur Verfügung, versuchen Sie es mit einer PuTTY-Sitzung. Wählen Sie **Session** und geben Sie für **Serial line** Ihren COM-Port an.



Sie können **MODE** in einem lokalen Befehlsfenster ausführen. Die Ausgabe zeigt den verwendeten COM-Port sowie ggf. die für die PuTTY-Sitzung benötigten Baud/Parity/Data Bits/Stop Bits an. Wenn die PuTTY-Verbindung erfolgreich ist, drücken Sie die **Eingabetaste**, um eine Rückmeldung vom Gerät zu erhalten. Von Ihnen eingegebene Zeichen werden ggf. auf dem Bildschirm wiederholt oder beantwortet. Wenn dies nicht möglich ist, können Sie nicht aus virtuellen Sitzungen auf das Gerät zugreifen.

2. Ordnen Sie den lokalen COM-Port dem VDA zu (mithilfe von Richtlinien oder **NET USE COMX: \\CLIENT\COMZ:**) und wiederholen Sie die PuTTY-Prozeduren im vorherigen Schritt, diesmal jedoch per VDA-PuTTY. Schlägt PuTTY mit dem Fehler **Unable to open connection to COM1. Unable to open serial port** fehl, wird COM1 möglicherweise von einem anderen Gerät verwendet.

3. Führen Sie **chgport /query** aus. Wenn der integrierte Windows-Treiber für serielle Ports auf dem VDA COM1 automatisch \Device\Serial0 zuordnet, gehen Sie folgendermaßen vor:
   A. Öffnen Sie CMD auf dem VDA und geben Sie **NET USE** ein.

   B. Löschen Sie eine ggf. vorhandene Zuweisung (z. B. COM1) auf dem VDA.

   NET USE COM1 /DELETE

   C. Ordnen Sie das Gerät dem VDA zu.

   NET USE COM1: \\CLIENT\COM3:

   D. Verweisen Sie die Anwendung auf dem VDA an COM3.

   Versuchen Sie als Letztes, den lokalen COM-Port (z. B. COM3) einem anderen COM-Port auf dem VDA als COM1 zuzuordnen (z. B. COM3). Stellen Sie sicher, dass Ihre Anwendung darauf verweist:
   NET USE COM3: \\CLIENT\COM3

4. Wenn der Port jetzt als zugeordnet erscheint und PuTTY funktioniert aber keine Daten übertragen werden, kann eine Racebedingung vorliegen. Die Anwendung stellt möglicherweise vor der Portzuordnung eine Verbindung her und öffnet den Port, sodass dieser für die Zuordnung gesperrt ist. Versuchen Sie eine der folgenden Möglichkeiten:

- Öffnen Sie eine zweite Anwendung, die auf demselben Server veröffentlicht wurde. Warten Sie einige Sekunden, bis der Port zugeordnet ist, und öffnen Sie dann die eigentliche Anwendung, die den Port verwenden soll.
- Aktivieren Sie die Richtlinien für die COM-Portumleitung über den Gruppenrichtlinien-Editor in Active Directory anstelle von Studio. Es handelt sich um die Studio-Richtlinien **Client-COM-Portumleitung** und **Client-COM-Ports automatisch verbinden**. Auf diese Weise angewendete Richtlinien werden ggf. vor den Studio-Richtlinien verarbeitet, wodurch sichergestellt wird, dass der COM-Port zugeordnet wird. Citrix Richtlinien werden an den VDA übertragen und an folgenden Orten gespeichert:
  `HKLN\SOFTWARE\Policies\Citrix \<user session ID\>`
- Verwenden Sie dieses Anmeldeskript für den Benutzer oder veröffentlichen Sie anstelle der Anwendung ein BAT-Skript, das zuerst alle Zuordnungen auf dem VDA löscht, den virtuellen COM-Anschluss neu zuordnet und anschließend die Anwendung startet:

```
@echo off
NET USE COM1 /delete
NET USE COM2 /delete
NET USE COM1: \\CLIENT\COM1:
NET USE COM2: \\CLIENT\COM2:
MODE COM1: BAUD=1200 (bzw. jeweils erforderlicher Wert)
MODE COM2: BAUD=9600 PARITY=N Data=8 Stop=1 (bzw. jeweils erforderlicher Wert)
START C:\Program Files\<Your Software Path>\
```

5. Als letzte Möglichkeit können Sie den Prozessmonitor von Sysinternals verwenden. Suchen und filtern Sie mit diesem Tool auf dem VDA Objekte wie COM3, picaser.sys, CdmRedirector und insbesondere <Anwendungsname>.exe. Fehler werden in Form von "Zugriff verweigert"oder ähnlich angezeigt.

Einschränkungen

- COM-Portgeräte müssen vor dem Start der ICA-Sitzung angeschlossen sein.
- Die COM-Portumleitung während der ICA-Wiederverbindung bietet keine dynamische COM-Porterkennung.
- Bei Verbindung von einem Client mit angeschlossenem COM-Portgerät und anschließendem Smoothroaming eines neuen Clients ohne angeschlossenes COM-Portgerät wird die bestehende COM-Portzuordnung nicht entfernt.

Spezialtastaturen

April 19, 2024

Bloomberg-Tastaturen

> **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 Virtual Apps and Desktops unterstützt die Bloomberg-Tastatur 4 (Starboard) und das ältere Modell 3. Mithilfe der Spezialfunktionen dieser Tastatur können Benutzer im Finanzsektor schnell auf Finanzmarktdaten zugreifen und handeln.

Die Tastatur ist mit den KVM-Switches kompatibel und kann in zwei Modi betrieben werden:

- PC (ein USB-Kabel ohne KVM)
- KVM-Modus (zwei USB-Kabel, eines via KVM)

> **Wichtig:**
> Citrix empfiehlt, die Bloomberg-Tastatur nur in einer Sitzung zu verwenden. Von der Verwendung der Tastatur in mehreren Sitzungen gleichzeitig (ein Client für mehrere Sitzungen) wird abgeraten.

Die Bloomberg-Tastatur 4 umfasst als USB-Verbundgerät vier USB-Geräte in einem Gehäuse:

- Tastatur
- Fingerabdruckleser
- Audiogerät mit Tasten zum Erhöhen und Verringern der Lautstärke und zum Stummschalten von Lautsprecher und Mikrofon. Das Gerät umfasst integrierte Lautsprecher, Mikrofon und eine Buchse für Mikrofon und Headset.
- USB-Hub für den Anschluss aller Geräte an das System

Anforderungen:

- Die Sitzung, mit der die Citrix Workspace-App für Windows verbunden ist, muss USB-Geräte unterstützen.

- Mindestens Citrix Workspace-App 1808 für Windows oder Citrix Receiver 4.8 zur Unterstützung von Bloomberg-Tastaturmodellen 3 und 4
- Mindestens Citrix Workspace-App 1808 für Windows oder Citrix Receiver 4.12 für den KVM-Modus (zwei USB-Kabel, von denen eines über KVM geleitet wird) für Modell 4

Weitere Informationen zur Konfiguration von Bloomberg-Tastaturen in der Citrix Workspace-App für Windows finden Sie unter Konfigurieren von Bloomberg-Tastaturen.

Aktivieren der Unterstützung für Bloomberg-Tastaturen:

Standardmäßig ist die Unterstützung für die erweiterte Bloomberg-Tastatur deaktiviert. Aktivieren Sie die Unterstützung durch Bearbeiten des folgenden Registrierungseintrags auf dem Clientcomputer, bevor Sie eine Verbindung herstellen.

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICAClient\GenericUSB

Name: **EnableBloombergHID** (dword)

Wert: 0 = deaktiviert, 1 = aktiviert

Überprüfen der Kompatibilität:

Um festzustellen, ob die Bloomberg-Tastaturunterstützung in der Citrix Workspace-App aktiviert ist, prüfen Sie, ob im Desktop Viewer die Bloomberg-Tastaturgeräte korrekt angezeigt werden.

Desktop:

Öffnen Sie den Desktop Viewer. Wenn die Unterstützung für die Bloomberg-Tastatur aktiviert ist, werden im Desktop Viewer drei Geräte unter dem USB-Symbol angezeigt:

- Bloomberg-Fingerabdruckscanner
- Bloomberg-Tastaturfeatures
- Bloomberg LP Keyboard 2013

Seamlessanwendung:

Öffnen Sie das Menü Connection Center über das Infobereichssymbol der Citrix Workspace-App. Wenn die Unterstützung für die Bloomberg-Tastatur aktiviert ist, werden die drei Geräte im Menü Geräte angezeigt.

Ein Häkchen zeigt an, dass das jeweilige Gerät in einer Sitzung verwendet wird.

TWAIN-Geräte

February 6, 2020

Anforderungen

- Der Scanner muss TWAIN-kompatibel sein.
- Installieren Sie die TWAIN-Treiber auf dem lokalen Gerät. Auf dem Server sind sie nicht erforderlich.
- Schließen Sie den Scanner lokal an (z. B. über USB).
- Stellen Sie sicher, dass der Scanner den lokalen TWAIN-Treiber und nicht den Windows Image Acquisition-Dienst verwendet.
- Stellen Sie sicher, dass auf das für den Test verwendete Benutzerkonto keine Richtlinie angewendet wird, welche die Bandbreite der ICA-Sitzung begrenzt. Beispiel: Bandbreitenlimit für Client-USB-Geräteumleitung.

Informationen zu Richtlinieneinstellungen finden Sie unter Einstellungen der Richtlinie "TWAIN-Geräte".

Webcams

August 22, 2022

HD-Webcamstreaming

Webcams können von innerhalb einer virtuellen Sitzung ausgeführten Videokonferenzanwendungen verwendet werden. Die Anwendung auf dem Server wählt Format und Auflösung von Webcams basierend auf den unterstützten Formatarten. Beim Sitzungsstart sendet der Client die Webcam-Informationen an den Server. Wählen Sie eine Webcam über die Videokonferenzanwendung aus. Wenn Webcam und Anwendung HD-Wiedergabe unterstützen, wird HD in der Anwendung verwendet. Es werden Webcamauflösungen bis zu 1920 x 1080 unterstützt.

Dieses Feature erfordert mindestens Version 4.10 von Citrix Receiver für Windows. Eine Liste der Citrix Workspace-App-Plattformen, die die HDX-Webcamumleitung unterstützen, finden Sie unter Citrix Workspace-App –Featurematrix.

Weitere Informationen zum HD-Webcamstreaming finden Sie unter HDX-Videokonferenzen und Webcam-Videokomprimierung.

> **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 das Feature über einen Registrierungsschlüssel deaktivieren. Die Standardauflösung 352 x 288 wird verwendet:

HKEY_LOCAL_MACHINE\Software\Citrix\HDXRealTime

Name: Disable_HighDefWebcam

Typ: REG_DWORD

Daten: 1 = HD-Webcamstreaming deaktivieren

Anhand der Registrierungsschlüssel auf dem Client können Sie eine bestimmte Auflösung konfigurieren. Stellen Sie sicher, dass die Webcam die angegebene Auflösung unterstützt:

HKEY_CURRENT_USER\Software\Citrix\HDXRealTime

Name: DefaultWidth

Typ: REG_DWORD

Daten (dezimal): gewünschte Breite (zum Beispiel 1280)

Name: DefaultHeight

Typ: REG_DWORD

Daten (dezimal): gewünschte Höhe (zum Beispiel 720)

Grafik

September 21, 2021

Citrix HDX umfasst vielfältige Technologien zur Grafikbeschleunigung und -codierung, die die Bereitstellung reichhaltiger Grafikanwendungen über Citrix Virtual Apps and Desktops 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. 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 Citrix Virtual Apps and Desktops 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 Citrix Virtual Apps and Desktops 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-Einzelsitzungs-OS

Mit HDX 3D Pro können Sie grafikintensive Anwendungen als Teil gehosteter Desktops oder Anwendungen auf Maschinen mit Einzelsitzungs-OS 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-Multisitzungs-OS

Mit HDX 3D Pro können grafikintensive Anwendungen, die in Sitzungen mit Windows-Multisitzungs-OS 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

> **Wichtig:**
>
> Ab Citrix Virtual Apps and Desktops 7 1903 wird Framehawk nicht mehr unterstützt. Verwenden

> Sie stattdessen Thinwire mit aktiviertem adaptivem Transport.

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.

Textbasiertes Sitzungswasserzeichen

Textbasierte Sitzungswasserzeichen zur Verhinderung und Verfolgung von Datendiebstahl: Diese verfolgbaren Informationen erscheinen auf dem Sitzungsdesktop als Abschreckung für Personen, die Daten per Foto oder Screenshot stehlen möchten. Sie können eine Textschicht als Wasserzeichen festlegen. Das Wasserzeichen kann über dem gesamten Sitzungsbildschirm angezeigt werden, ohne das Originaldokument zu ändern. Textbasierte Sitzungswasserzeichen erfordern VDA-Unterstützung.

Verwandte Informationen

- HDX 3D Pro
- GPU-Beschleunigung für Windows-Einzelsitzungs-OS
- GPU-Beschleunigung für Windows-Multisitzungs-OS
- Framehawk
- Thinwire
- Textbasiertes Sitzungswasserzeichen

HDX 3D Pro

September 21, 2021

Mit der HDX 3D Pro-Funktion von Citrix Virtual Apps and Desktops 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.

Informationen zu den HDX 3D Pro-Richtlinieneinstellungen finden Sie unter Optimierung für 3D-Grafikworkload.

Alle unterstützten Citrix Workspace-App-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 der Citrix Workspace-App für Windows

bzw. der Citrix Workspace-App für Linux. Informationen zu den unterstützten Versionen der Citrix Workspace-App finden Sie unter Lifecycle Milestones for Citrix Workspace app.

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 die GPU-Beschleunigung für Maschinen mit Windows-Einzelsitzungs-OS und Windows-Multisitzungs-OS bereit. Weitere Informationen finden Sie unter GPU-Beschleunigung für Windows-Einzelsitzungs-OS sowie GPU-Beschleunigung für Windows-Multisitzungs-OS.

HDX 3D Pro ist mit GPU-Passthrough und der GPU-Virtualisierung folgender Hypervisors und in Bare-Metal-Umgebungen kompatibel:

- Citrix Hypervisor
  - GPU-Passthrough mit NVIDIA GRID, AMD und Intel GVT-d
  - GPU-Virtualisierung mit NVIDIA GRID, AMD und Intel GVT-g
  - Siehe Hypervisor 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-Multisitzungs-OS

September 21, 2021

Mit HDX 3D Pro können grafikintensive Anwendungen, die in Sitzungen mit Windows-Multisitzungs-OS 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.

Da Windows Server ein Mehrbenutzer-Betriebssystem ist, kann eine von Citrix Virtual Apps verwendete 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

Die GPU-Freigabe ermöglicht die GPU-Hardwarewiedergabe von OpenGL- und DirectX-Anwendungen in Remotedesktopsitzungen. Sie 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.

Ein GPU kann der virtuellen Windows Server-Maschine gemäß den Anforderungen des Hypervisor- und GPU-Anbieters im Modus GPU-Passthrough oder Virtual GPU (vGPU) zugewiesen werden. Bare-Metal-Bereitstellungen auf physischen Windows Server-Maschinen werden ebenfalls unterstützt.

GPU Sharing hängt nicht von einer bestimmten Grafikkarte ab.

- Wählen Sie für virtuelle Maschinen eine Grafikkarte, die mit dem verwendeten Hypervisor kompatibel ist. Eine Hardwarekompatibilitätsliste für Citrix Hypervisor finden Sie unter Hypervisor Hardware Compatibility List.
- 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 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: http://www.techpowerup.com/gpuz/.

- 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".

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 Sitzungen mit Windows-Multisitzungs-OS 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-Einzelsitzungs-OS

November 4, 2021

Mit HDX 3D Pro können Sie grafikintensive Anwendungen als Teil gehosteter Desktops oder Anwendungen auf Maschinen mit Einzelsitzungs-OS bereitstellen. HDX 3D Pro unterstützt physische Hostcomputer (einschließlich Desktop-, Blade- und Rack-Arbeitsstationen) und die Virtualisierungstechnologien der folgenden Hypervisors: Citrix Hypervisor, 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.

HDX 3D Pro bietet die folgenden Features:

- Adaptive, auf dem H.264- oder H.265-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 mit H.264 wird für NVIDIA-, Intel- und AMD-Karten verwendet, die NVENC unterstützen. Hardwarecodierung mit H.265 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 mehr Netzwerk- und Verarbeitungsressourcen benötigt.

  Bei Verwendung von verlustfreier Komprimierung:

  - Die Anzeige für Verlustfreiheit (Symbol im Infobereich) gibt 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 HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDX3D\LLIndicator.

  - Name: HKEY_LOCAL_MACHINE_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.
  - 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: Auf Maschinen mit Einzelsitzungs-OS 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 für die NVIDIA vGPU-Architektur HDX 3D Pro unterstützt NVIDIA vGPU-Karten. Weitere Informationen finden Sie unter NVIDIA vGPU für GPU-Passthrough und GPU-Sharing. NVIDIA 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 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 http://www.citrix.com/intel und http:

//www.intel.com/content/www/us/en/servers/data-center-graphics.html.

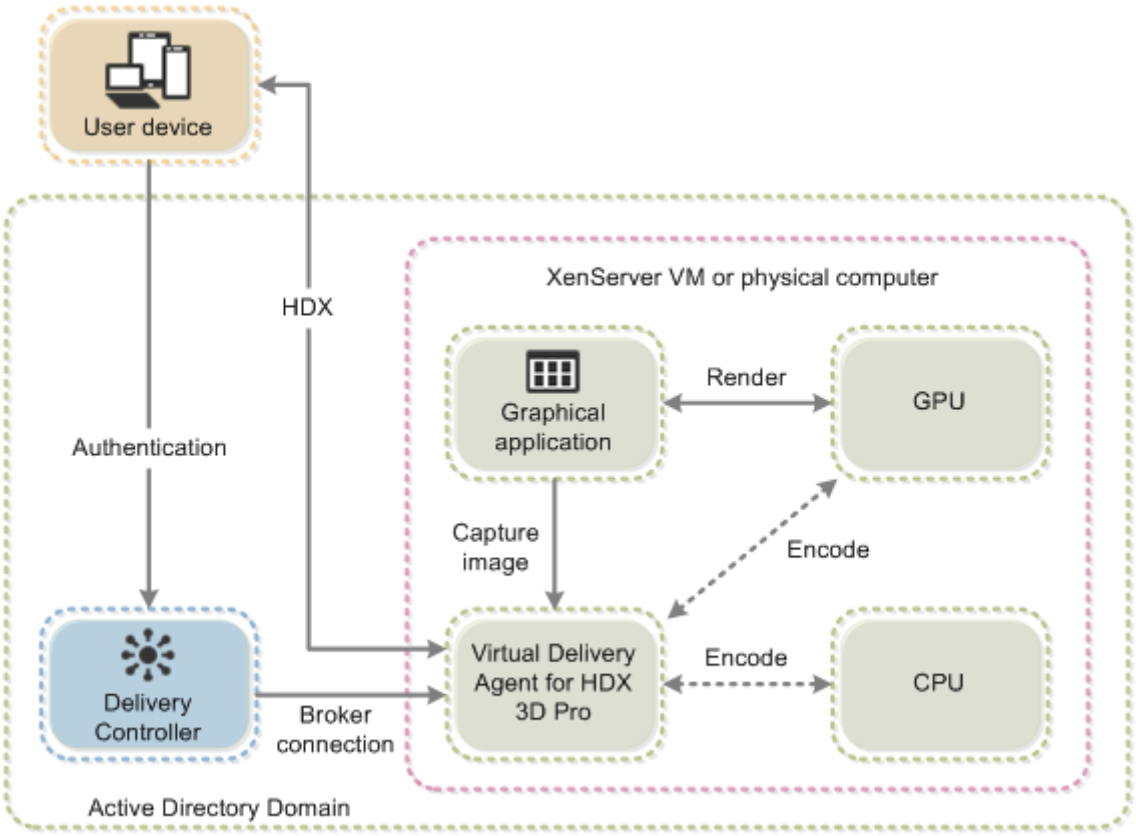
- Unterstützung für AMD RapidFire auf den Serverkarten der AMD FirePro S-Serie. HDX 3D Pro unterstützt den Betrieb von bis zu 6 Bildschirmen, Console Blanking, benutzerdefinierte Auflösungen und hohe Frameraten. Hinweis: HDX 3D Pro-Unterstützung für AMD MxGPU (GPU-Virtualisierung) funktioniert nur bei VMware vSphere vGPUs. Citrix Hypervisor und Hyper-V werden mit GPU-Passthrough unterstützt. Weitere Informationen finden Sie unter AMD Virtualization Solution.
- Zugriff auf einen leistungsfähigen Videoencoder für NVIDIA-, AMD- und Intel Iris Pro-Grafikprozessoren. Das Feature wird durch eine standardmäßig aktivierte Richtlinieneinstellung gesteuert. Es ermöglicht die Verwendung der H.264-Hardwarecodierung (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 der Citrix Workspace-App anmeldet und auf die virtuelle Anwendung oder den virtuellen Desktop zugreift, authentifiziert der Controller den Benutzer. Der Controller kontaktiert dann den VDA für HDX 3D Pro, um eine Verbindung mit dem Computer herzustellen, auf dem die grafische Anwendung gehostet wird.

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 übertragen. Diese Übertragung erfolgt über eine direkte HDX-Verbindung zwischen der Citrix Workspace-App und dem VDA für HDX 3D Pro.



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 während 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 Workspace-App - Desktop Viewer-Einstellungen"ändern.

Wenn mehrere Benutzer eine Verbindung mit beschränkter Bandbreite gemeinsam verwenden, z. B. in einer Zweigstelle, empfehlen wir, die Richtlinieneinstellung **Bandbreitenlimit für Sitzung insgesamt** zu verwenden, um die für die einzelnen Benutzer verfügbare Bandbreite zu beschränken. Mit dieser Einstellung 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.

Wir empfehlen für Benutzer 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, finden Sie im Knowledge Center-Artikel CTX128190.

Thinwire

March 15, 2022

Einführung

Thinwire ist die in Citrix Virtual Apps and Desktops 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 Citrix Virtual Apps and Desktops verwendet.

Thinwire

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.

HDX 3D Pro

In der Standardkonfiguration kann Thinwire 3D- oder hoch interaktive Grafik liefern. Citrix empfiehlt jedoch die Aktivierung des HDX 3D Pro-Modus über die Richtlinie **Optimierung für 3D-Grafikworkload** für Szenarien, in denen GPUs vorhanden sind. Der HDX 3D Pro-Modus verwendet die GPU zur Hardwarebeschleunigung und konfiguriert Thinwire mit optimalen Einstellungen für Grafiken. Dies bietet eine flüssigere Anzeige professioneller 3D-Grafiken. Weitere Informationen finden Sie unter HDX 3D Pro und GPU-Beschleunigung für Windows-Einzelsitzungs-OS.

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.

> **Hinweis:**
>
> In dieser Version wird der Legacygrafikmodus nicht unterstützt. Er ist zum Zweck der Abwärtskompatibilität im Fall einer Verwendung von XenApp 7.15 LTSR, XenDesktop 7.15 LTSR und früheren VDA-Releases mit Windows 7 und Windows 2008 R2 enthalten.

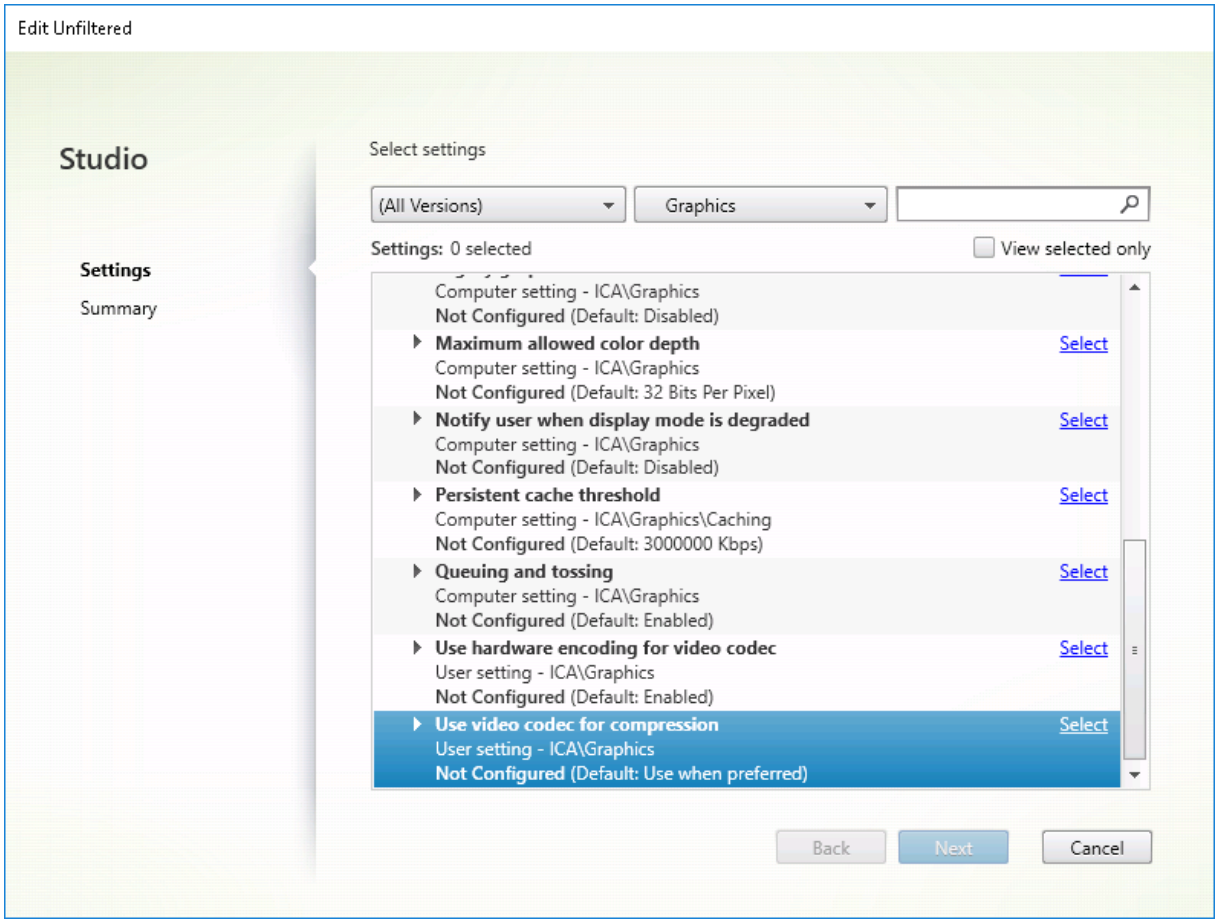
- Die Richtlinieneinstellung, die das Verhalten von Thinwire steuert (**Videocodec zur Komprimierung verwenden**), ist in VDA-Versionen in Citrix Virtual Apps and Desktops 7 1808 und höher bzw. XenApp und XenDesktop 7.6 FP3 und höher verfügbar. Die Option **Videocodec verwenden, wenn bevorzugt** ist die Standardeinstellung für die VDA-Versionen in Citrix Virtual Apps and Desktops 7 1808 und höher bzw. in XenApp und XenDesktop 7.9 und höher.
- Alle Citrix Workspace-App-Versionen unterstützen Thinwire. Einige Citrix Workspace-App-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 der Citrix Workspace-App 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 oder H.265 nur in dem Bildschirmbereich, in dem das Bild sich bewegt.
  - **Für den gesamten Bildschirm**. Thinwire wird mit Vollbild-H.264 oder -H.265 zur Optimierung der Benutzererfahrung und Bandbreite, insbesondere bei intensiver 3D-Grafiknutzung, verwendet.



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

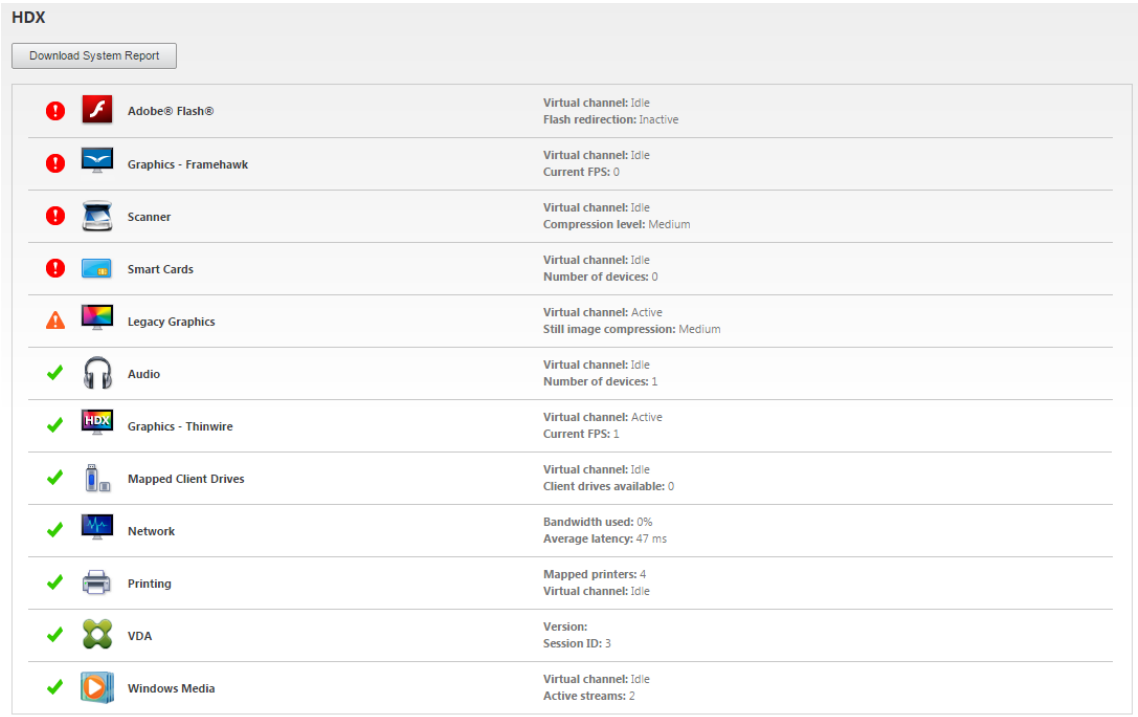
Zur Aktivierung der von Citrix für verschiedene Anwendungsfälle empfohlenen Kombinationen von Richtlinieneinstellungen verwenden Sie die integrierten Citrix Richtlinienvorlagen. Die Vorlagen **Hohe Serverskalierbarkeit** und **Besonders gute High Definition-Benutzererfahrung** verwenden beide Thinwire mit der optimalen Kombination von Richtlinieneinstellungen für die Prioritäten Ihres Unternehmens und die Erwartungen der Benutzer.

Überwachen von Thinwire

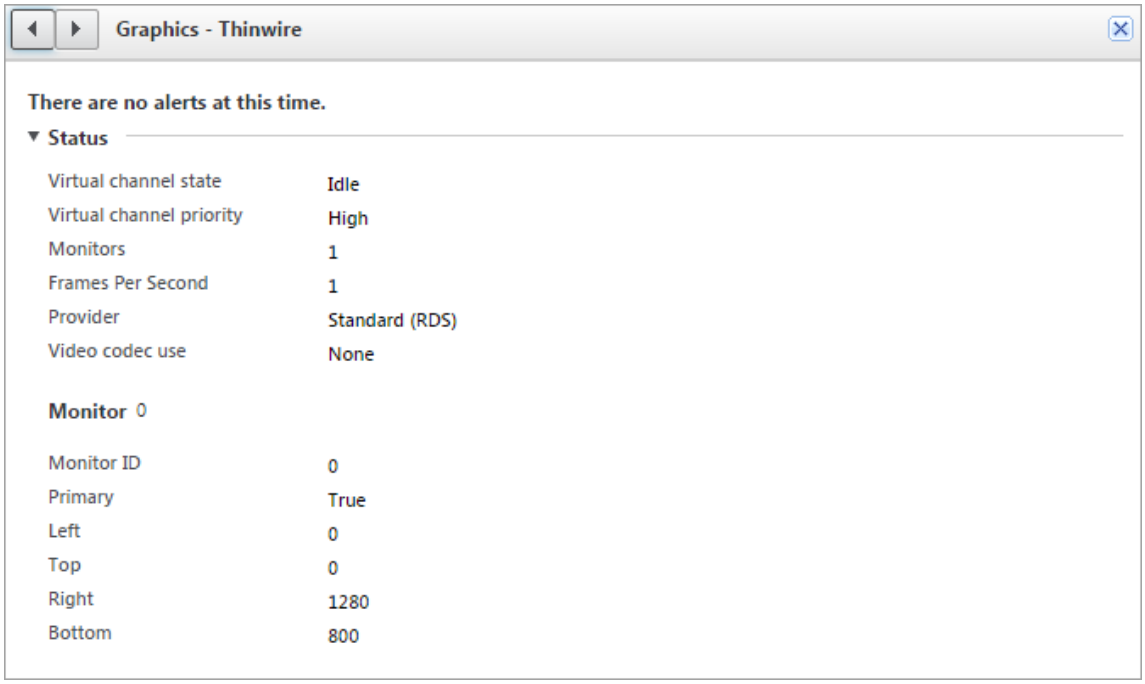
Sie können die Verwendung und Leistung von Thinwire über Citrix Director überwachen. Die Detailansicht für den virtuellen HDX-Kanal enthält nützliche Informationen zur Überwachung und Problembe-

handlung 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.



3. Wählen Sie **Grafiken - Thinwire**.



Codierungsmethoden

In XenApp und XenDesktop 7.16 und früheren Versionen gibt es drei Thinwire-Bitmapcodierungsmodi, die für das Grafikremoting von VDAs für Multisitzungs-OS bzw. Einzelsitzungs-OS verwendet werden:

- Vollbild H.264
- Thinwire Plus
- Thinwire Plus mit selektivem H.264

Bei dem GDI-Remoting älterer Versionen wurde der XPDM-Remotingtreiber und keine Thinwire-Bitmapcodierung verwendet.

In einer normalen Desktopsitzung sind die meisten Bilder einfache Grafiken oder Textbereiche. Wird einer der drei aufgelisteten Bitmapcodierungsmodi verwendet, wählt Thinwire diese Bereiche für die verlustfreie Codierung mit dem 2DRLE-Codec aus. Auf dem Citrix Workspace-App-Client werden diese Elemente mit dem 2DRLE-Decoder der Citrix Workspace-App für die Anzeige in der Sitzung decodiert.

Verlustfreier Komprimierungscodec (MDRLE)

XenApp und XenDesktop 7.17 verfügt über einen neuen MDRLE-Codec mit höherer Komprimierungsrate, der bei normalen Desktopsitzungen weniger Bandbreite verbraucht als der 2DRLE-Codec.

Weniger Bandbreite resultiert in der Regel in einer besseren Sitzungsinteraktivität (insbesondere bei gemeinsam genutzten oder eingeschränkten Verbindungen) und geringeren Kosten. Der erwartete Bandbreitenverbrauch des MDRLE-Codecs ist im Vergleich zu XenApp und XenDesktop 7.15 LTSR bei typischen Office-ähnlichen Workloads ca. 10-15 % geringer.

Für den MDRLE-Codec ist keine Konfiguration erforderlich. Wenn die Citrix Workspace-App die MDRLE-Decodierung unterstützt, verwendet der VDA die MDRLE-Codierung und die Citrix Workspace-App die MDRLE-Decodierung. Unterstützt die Citrix Workspace-App die MDRLE-Decodierung nicht, greift der VDA automatisch auf die 2DRLE-Codierung zurück.

Anforderungen für MDRLE

- Citrix Virtual Apps and Desktops-VDAs ab Version 7 1808
- XenApp und XenDesktop-VDAs ab Version 7.17
- Citrix Workspace-App für Windows: Mindestversion 1808
- Citrix Receiver für Windows: Mindestversion 4.11

Progressiver Modus

Die Sitzungsinteraktivität kann sich bei Verbindungen mit niedriger Bandbreite oder hoher Latenz verschlechtern. Bei einer Verbindung mit einer Bandbreite unter 2 MBit/s oder einer Latenz über 200 ms kann das Scrollen von Webseiten beispielsweise langsam und ungleichmäßig werden oder ganz stocken. Tastatur- und Mausoperationen können hinter Grafikaktualisierungen zurückbleiben.
In Version 7.17 konnten Sie den Bandbreitenverbrauch über Richtlinieneinstellungen verringern, indem Sie für Sitzungen eine niedrige Bildqualität oder eine geringere Farbtiefe festlegen (16- oder 8-Bit-Grafik). Sie mussten jedoch wissen, dass ein Benutzer eine schwache Verbindung hatte. HDX Thinwire konnte die Qualität statischer Bilder nicht auf der Grundlage der Netzwerkbedingungen dynamisch anpassen.
In Version 7.18 wechselt HDX Thinwire standardmäßig in einen dynamischen Aktualisierungsmodus, wenn die Bandbreite unter 2 MBit/s fällt oder die Netzwerklatenz 200 ms überschreitet. In diesem Modus gilt:

- Alle statischen Bilder werden stark komprimiert.
- Die Textqualität wird verringert.

Bewegliche Bilder (Video) werden weiterhin per adaptive Anzeige oder selektives H.264 verarbeitet.

Verwendung des progressiven Modus

Standardmäßig ist der progressive Modus auf Standby für die Bildqualitätsrichtlinieneinstellungen: Hoch, Mittel (Standard) und Niedrig.

Der progressive Modus ist in folgenden Situationen deaktiviert:

- Bildqualität = Immer verlustfrei oder Verlustfrei
- Bevorzugte Farbtiefe für einfache Grafiken = 8-Bit
- Video Codec verwenden = Für den gesamten Bildschirm (wenn Vollbild-H.264 gewünscht wird)

Wenn der progressive Modus auf Standby ist, wird er standardmäßig aktiviert, wenn eine der folgenden Bedingungen eintritt:

- Die verfügbare Bandbreite fällt unter 2 MBit/s.
- Die Netzwerklatenz erhöht sich auf über 200 ms.

Nach einem Moduswechsel bleibt der neue Modus mindestens 10 Sekunden aktiv, selbst wenn die ungünstigen Netzwerkbedingungen nur vorübergehend sind.

Ändern des Verhaltens des progressiven Modus

Sie können den Zustand des progressiven Modus über folgenden Registrierungsschlüssel ändern:

[REG_DWORD] HKEY_LOCAL_MACHINE\Software\Citrix\Graphics\ProgressiveDisplay

Werte:

0 = Immer deaktiviert (niemals verwenden)

1 = Automatisch (Umschalten je nach Netzwerkbedingungen, dies ist der Standardwert)

2 = Immer aktiviert

Im automatischen Modus (1) können Sie über folgenden Registrierungsschlüssel die Schwellenwerte ändern, bei denen ein Moduswechsel stattfindet:

[REG_DWORD] HKEY_LOCAL_MACHINE\Software\Citrix\Graphics\ProgressiveDisplayBandwidthThreshold

Wert: Schwellenwert in KBit/s (Standardwert = 2048)
Beispiel: 4096 = progressiven Modus einschalten, wenn die Bandbreite unter 4 MBit/s fällt

[REG_DWORD] HKEY_LOCAL_MACHINE\Software\Citrix\Graphics\ProgressiveDisplayLatencyThreshold

Wert: <Schwellenwert in ms> (Standard = 200)
Beispiel:100 = schaltet den progressiven Modus ein, wenn die Netzwerklatenz unter 100 ms fällt.

Textbasiertes Sitzungswasserzeichen

September 21, 2021

Textbasierte Sitzungswasserzeichen zur Verhinderung und Verfolgung von Datendiebstahl: Diese verfolgbaren Informationen erscheinen auf dem Sitzungsdesktop als Abschreckung für Personen, die

Daten per Foto oder Screenshot stehlen möchten. Ein Wasserzeichen ist eine Textschicht, die über dem gesamten Sitzungsbildschirm angezeigt wird, ohne eine Änderung des Originaldokuments zu bewirken. Textbasierte Sitzungswasserzeichen erfordern VDA-Unterstützung.

> **Wichtig**
>
> Textbasierte Sitzungswasserzeichen sind kein Sicherheitsfeature. Sie verhindern einen Datendiebstahl nicht vollständig, bieten jedoch ein gewisses Maß an Abschreckung und Rückverfolgbarkeit. Citrix garantiert bei Verwendung des Features zwar keine vollständige Rückverfolgbarkeit von Informationen, empfiehlt jedoch seine Verwendung nach Bedarf in Kombination mit anderen Sicherheitslösungen.

Ein Sitzungswasserzeichen ist Text, der mit Sitzungen an den Benutzer gesendet wird. Sitzungswasserzeichen enthalten Informationen zur Rückverfolgung von Datendiebstahl. Die wichtigste Angabe ist die Identität des angemeldeten Benutzers, in dessen Sitzung das Bildschirmbild erstellt wurde. Zur besseren Rückverfolgung von Datenlecks sollten Sie weitere Informationen wie die IP-Adresse des Servers oder des Clients und die Verbindungszeit einschließen.

Um die Benutzererfahrung anzupassen, verwenden Sie die Einstellungen der Richtlinie Sitzungswasserzeichen, um die Platzierung und Erscheinung von Wasserzeichen auf dem Bildschirm zu konfigurieren.

Anforderungen:

Virtual Delivery Agents:

Multisitzungs-OS 7.17
Einzelsitzungs-OS 7.17

Einschränkungen:

- Sitzungswasserzeichen werden nicht in Sitzungen unterstützt, in denen lokaler App-Zugriff, Windows Media-Umleitung, MediaStream, Browserinhaltsumleitung und HTML5-Videoumleitung verwendet werden. Zur Verwendung von Sitzungswasserzeichen müssen Sie diese Features deaktivieren.
- Sitzungswasserzeichen werden nicht unterstützt und angezeigt, wenn eine Sitzung im Vollbildmodus mit Hardwarebeschleunigung ausgeführt wird (Vollbild-H.264- oder -H.265-Codierung).
- Wenn Sie diese HDX-Richtlinien festlegen, werden die Wasserzeicheneinstellungen nicht wirksam es werden keine Wasserzeichen in Sitzungen angezeigt.

Hardwarecodierung für Videocodec verwenden auf **Aktiviert**
Videocodec zur Komprimierung verwenden auf **Für den gesamten Bildschirm**

- Wenn Sie diese HDX-Richtlinien festlegen, wird das Verhalten gestört und es wird möglicherweise kein Wasserzeichen angezeigt.

Hardwarecodierung für Videocodec verwenden auf **Aktiviert**
Videocodec zur Komprimierung verwenden auf **Videocodec verwenden, wenn bevorzugt**

Um sicherzustellen, dass Wasserzeichen angezeigt werden, legen Sie **Hardwarecodierung für Videocodec verwenden** auf **Deaktiviert** fest oder **Videocodec zur Komprimierung verwenden** auf **Für aktive Änderungsbereiche** oder **Videocodec nicht verwenden**.

- Sitzungswasserzeichen unterstützen nur Thinwire, nicht aber die Grafikmodi Framehawk oder Desktopgestaltungsumleitung.
- Wenn Sie die Sitzungsaufzeichnung verwenden, enthält die aufgezeichnete Sitzung kein Wasserzeichen.
- Wenn Sie Windows-Remoteunterstützung verwenden, wird das Wasserzeichen nicht angezeigt.
- Wenn ein Benutzer die Taste **Druck/S-Abf** drückt, um eine Bildschirmaufnahme zu erstellen, enthält diese VDA-seitig kein Wasserzeichen. Es wird empfohlen, Maßnahmen zu ergreifen, damit Bildschirmaufnahmen nicht kopiert werden.

Multimedia

September 21, 2021

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.

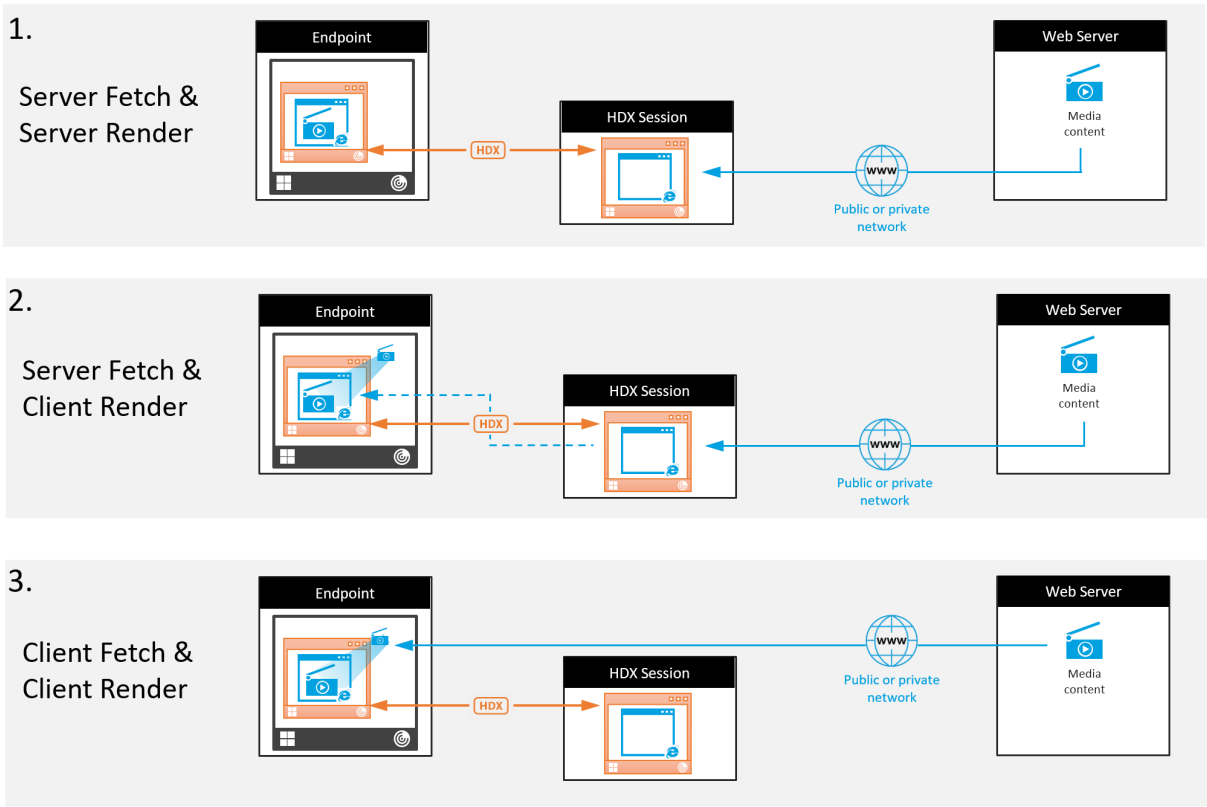
Bei der serverseitigen Wiedergabe wird Audio- und Videoinhalte decodiert und auf dem Citrix Virtual Apps and Desktops-Server von der Anwendung wiedergegeben. Der Inhalt wird dann komprimiert und unter Einsatz des ICA-Protokolls an die Citrix Workspace-App-Instanz auf dem Benutzergerät gesendet. Diese 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, AMD RapidFire 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.
- HTML5-Video ist mittlerweile gängig und Citrix hat eine Umleitungstechnologie für diese Art von Inhalt eingeführt. Citrix empfiehlt die Umleitung von Browserinhalten für Websites, die HTML5, HLS, DASH oder WebRTC verwenden.
- Sie können 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 sie auf den Clients stattfinden 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:

Einzelsitzungs-Betriebssysteme (Windows, Mac OS X und Linux) bieten Multimediaframeworks zum schnelleren 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

	Audioumleitung	Nein
	Browserinhaltsumleitung	Nein
	HDX-Webcamumleitung	Ja
	HTML5-Videoumleitung	Ja
	Windows Media-Umleitung	Ja

Audiofeatures

September 20, 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:**
>
> Wir empfehlen Audio per User Datagram Protocol (UDP) anstelle von TCP zu senden. Nur der Windows Virtual Delivery Agent (VDA) unterstützt Audio über UDP.
>
> Die UDP-Audioverschlüsselung mit DTLS ist nur zwischen Citrix Gateway und der Citrix Workspace-App möglich. In manchen Fällen ist TCP daher möglicherweise vorzuziehen. TCP unterstützt die lückenlose TLS-Verschlüsselung zwischen VDA und der Citrix Workspace-App.

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 Audiokomprim-

ierung können Sie die Audioqualität und die Sitzungsleistung aufeinander abstimmen; verwenden Sie Citrix Richtlinieneinstellungen, um den Komprimierungsgrad für Audiodateien zu konfigurieren.

Standardmäßig ist die **Richtlinieneinstellung für Audioqualität** bei Verwendung von TCP auf "Hoch - High Definition-Audio"eingestellt. Bei Verwendung von UPD (empfohlen) wird die Richtlinie auf "Mittel - für Sprache optimiert"eingestellt. Die Einstellung **High Definition-Audio** bietet Audio in Hi-Fi-Stereoqualität, verbraucht aber mehr Bandbreite als die anderen Einstellungen. Verwenden Sie diese Audioqualitätseinstellung nicht für nicht optimierte Chat- oder Videochat-Anwendungen (z. B. Softphones). Es kann ansonsten zu Latenzen im Audiopfad kommen, die nicht für die Echtzeitkommunikation geeignet sind. Citrix empfiehlt für Echtzeitaudio die Richtlinieneinstellung "für Sprache optimiert"unabhängig vom ausgewählten Transportprotokoll.

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.

Bandbreitenrichtlinien für Audiowiedergabe und -aufnahme:

- Hohe Qualität (Standard)
  - Bitrate: ~100 KBit/s (min. 75, max. 175 KBit/s) für die Wiedergabe/~ 70 KBit/s für Mikrofonaufnahme
  - Anzahl der Kanäle: 2 (Stereo) für Wiedergabe, 1 (Mono) für Mikrofonaufnahme
  - Frequenz: 44100 Hz
  - Bit-Tiefe: 16 Bit
- Mittlere Qualität (empfohlen für VoIP)
  - Bitrate: ~16 KBit/s (min. 20, max. 40 KBit/s) für die Wiedergabe/~ 16 KBit/s für Mikrofonaufnahme
  - Anzahl der Kanäle: 1 (Mono) für Wiedergabe und Aufnahme
  - Frequenz: 16.000 Hz (Breitband)
  - Bit-Tiefe: 16 Bit
- Niedrige Qualität
  - Bitrate: ~ 11 KBit/s (min. 10, max. 25 KBit/s) für die Wiedergabe, ~ 11 KBit/s für die Mikrofonaufnahme
  - Anzahl der Kanäle: 1 (Mono) für Wiedergabe und Aufnahme
  - Frequenz: 8000 Hz (Schmalband)
  - Bit-Tiefe: 16 Bit

Clientaudioumleitung

Damit der Audioempfang von einer Anwendung auf dem Server über Lautsprecher oder andere Soundgeräte auf dem Benutzergerät zugelassen wird, übernehmen Sie für die Einstellung **Clientaudioumleitung** den Wert **Zugelassen**. Dies ist die Standardeinstellung.

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.

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 Geräten haben, auf Mikrofone zugreifen. Die Benutzer können den Zugang akzeptieren oder ablehnen, bevor sie das Mikrofon benutzen. Die Benutzer können die diesbezügliche Warnung in der Citrix Workspace-App deaktivieren.

Informationen zu Einstellungen finden Sie unter Einstellungen der Richtlinie "Audio". Denken Sie daran, die Clientaudioeinstellungen auf dem Benutzergerät zu aktivieren.

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. Dies ist selbst dann möglich, wenn diese erst nach Beginn einer Sitzung angeschlossen werden.

Diese Einstellung gilt nur für Maschinen mit Windows-Multisitzungs-OS.

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.

Audio über UDP - Real-time Transport und Audio-UDP-Portbereich

Standardmäßig ist "Audio über UDP mit Real-Time Transport"zulässig (wenn dies bei der Installation ausgewählt wird). Dadurch wird ein UDP-Port auf dem Server für alle Verbindungen geöffnet, die für die Echtzeitübertragung von Audio über UDP konfiguriert wurden. Zur Gewährleistung der besten Benutzererfahrung bei Netzwerküberlastung oder Paketverlust empfiehlt Citrix, dass Sie UDP/RTP für Audio konfigurieren. Für Echtzeitaudio, z. B. Softphone-Anwendungen wird UDP-Audio gegenüber EDT bevorzugt. Bei UDP ist Paketverlust ohne Neuübertragung möglich, sodass bei Verbindungen mit hohen Paketverlusten keine zusätzliche Latenz entsteht.

> **Wichtig:**
>
> Wenn Citrix Gateway nicht im Pfad ist, werden mit UDP übertragene Audiodaten nicht verschlüsselt. Ist Citrix Gateway für den Zugriff auf Citrix Virtual Apps and Desktops-Ressourcen konfiguriert, wird der Audioverkehr zwischen Endpunktgerät und Citrix Gateway mittels DTLS gesichert.

Mit der Einstellung "Audio-UDP-Portbereich"geben Sie den Bereich der Portnummern an, die der Windows-VDA zum Austausch von Audiopaketdaten mit dem Benutzergerät verwendet.

Der Standardbereich ist 16500 bis 16509.

Weitere Informationen zum Einstellen von Audio über UDP mit Real-Time Transport finden Sie unter Einstellungen der Richtlinie "Audio". Weitere Informationen zum Audio-UDP-Portbereich finden Sie unter Einstellungen der Richtlinie "Multistreamverbindungen". Denken Sie daran, die Clientaudioeinstellungen auf dem Benutzergerät zu aktivieren.

Audio über UDP benötigt den Windows-VDA. Informationen zu unterstützten Richtlinien auf dem Linux VDA finden Sie unter Liste der unterstützten Richtlinien.

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 Komponenten > Citrix Workspace > Benutzererfahrung**.

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.** Aktiviert die Audioumleitung mit den ausgewählten Optionen.
    - **Deaktiviert.** Deaktiviert die Audioumleitung.

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 Citrix Gateway wählen Sie die Option **Echtzeittransport über Gateway zulassen**. Konfigurieren Sie Citrix Gateway mit DTLS. Weitere Informationen finden Sie in diesem Artikel.

Wenn Sie als Administrator auf Endpunktgeräten solche Änderungen nicht vornehmen können, aktivieren Sie UDP-Audio über die default.ica-Attribute von StoreFront. Beispiel: BYOD-Geräte oder Heimcomputer.

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:

    ; aktiviert Real-Time Transport

    EnableRtpAudio=true

    ; aktiviert Real-Time Transport über Gateway

    EnableUDPThroughGateway=true

    ; legt die Audioqualität auf “Mittel”fest

    AudioBandwidthLimit=1

    ; UDP-Portbereich

    RtpAudioLowestPort=16500

    RtpAudioHighestPort=16509

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. Stellen Sie sicher, dass die Geräte nicht zu nah beieinander oder zu weit voneinander entfernt sind.

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.

Citrix Virtual Apps and Desktops unterstützt verschiedene Bereitstellungsmethoden für Softphones.

- **Steuermodus:** Das gehostete Softphone steuert ein physisches Telefon. In diesem Modus werden keine Audiodaten über den Citrix Virtual Apps and Desktops-Server gesendet.

- **Softphone-Unterstützung mit HDX RealTime-Optimierung (empfohlen).** Die Media Engine wird auf dem Benutzergerät ausgeführt und der VoIP-Datenverkehr erfolgt Peer-to-Peer. Beispiele:
  - Optimierung für Microsoft Teams
  - HDX RealTime Optimization Pack zur Optimierung der Bereitstellung von Microsoft Skype for Business.
  - Cisco Jabber Softphone für VDI (früher VXME)
  - Cisco Webex Meetings for VDI
  - Avaya VDI Equinox (früher VDI Communicator)
  - Zoom-VDI-Plug-In
  - Genesys PureEngage Cloud
  - Nuance Dragon PowerMic-Diktiergerät
- **Lokaler App-Zugriff:** Citrix Virtual Apps and Desktops-Funktion, welche die lokale Ausführung von Softphones und ähnlichen Anwendungen auf dem Windows-Gerät eines Benutzers ermöglicht, wobei die Anwendung nahtlos in dessen virtuellen/veröffentlichten 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 der Citrix Workspace-App 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 Citrix Virtual Apps and Desktops sind zwei Punkte zu beachten:

- Art der Bereitstellung des Softphones auf dem virtuellen/veröffentlichten Desktop
- Art der Übermittlung der Audiodaten zwischen dem Kopfhörer, Mikrofon, Lautsprecher und/oder USB-Telefon des Benutzers

Citrix Virtual Apps and Desktops umfasst 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 Workspace-App-Versionen für Windows, Linux, Chrome und Mac sind auch VoIP-fähig. Die Citrix Workspace-App 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, servicebasiertes 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 der Citrix Workspace-App 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 Workspace-App-Version und eines hochwertigen Headsets mit akustischer Echounterdrückung (AEC). Die Citrix Workspace-App-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 Citrix Virtual Desktops-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 die Verwendung von NetScaler SD-WAN zwischen dem Datencenter und dem Remotestandort. Dies gewährleistet eine hohe Servicequalität. NetScaler 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.

Verwenden Sie Director oder HDX Monitor zum Überprüfen der HDX-Konfiguration.

Remotebenutzerverbindungen:
Citrix Gateway unterstützt DTLS für die native (ohne TCP-Einkapselung) Bereitstellung von UDP/RTP-Datenverkehr.
Öffnen Sie Firewalls bidirektional für UDP-Datenverkehr über Port 443.

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 gute 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:** unterstützt Audiogeräte mit Tasten und/oder Bildschirm, wenn zwischen Benutzergerät und Citrix Virtual Apps and Desktops-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. Mit generischem HDX RealTime werden Audiodaten vom Headset oder Mikrofon des Benutzers komprimiert. Sie werden dann 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). Der 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. Dieser Ansatz beschränkt sich auf Benutzer im LAN. Der Grund dafür ist, dass das USB-Protokoll latenzempfindlich ist und eine beträchtliche Netzwerkbandbreite erfordert. Die isochrone USB-Umleitung funktioniert bei einigen Softphones gut. Diese Umleitung bietet eine hervorragende Sprachqualität und geringe Latenz. Citrix Audio Virtual Channel wird jedoch bevorzugt, da es für Audiodatenverkehr optimiert ist. Die primäre Ausnahme bildet die Verwendung von Audiogeräten mit Tasten. Beispiel: ein an ein mit dem Datenzentrum über LAN verbundenes Benutzergerät angeschlossenes USB-Telefon. 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. Es besteht kein Problem bei Tasten, die lokal auf dem Gerät funktionieren.

Einschränkung

> **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 installieren ein Audiogerät auf dem Client, aktivieren die Audioumleitung und starten eine RDS-Sitzung. Die Audiodateien können möglicherweise nicht wiedergegeben werden und eine Fehlermeldung wird angezeigt.

Fügen Sie als Workaround folgenden Registrierungsschlüssel auf der RDS-Maschine hinzu und starten Sie diese anschließend neu:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SCMConfig

Name: EnableSvchostMitigationPolicy

Typ: REG_DWORD

Wert: 0

Umleitung des Browserinhalts

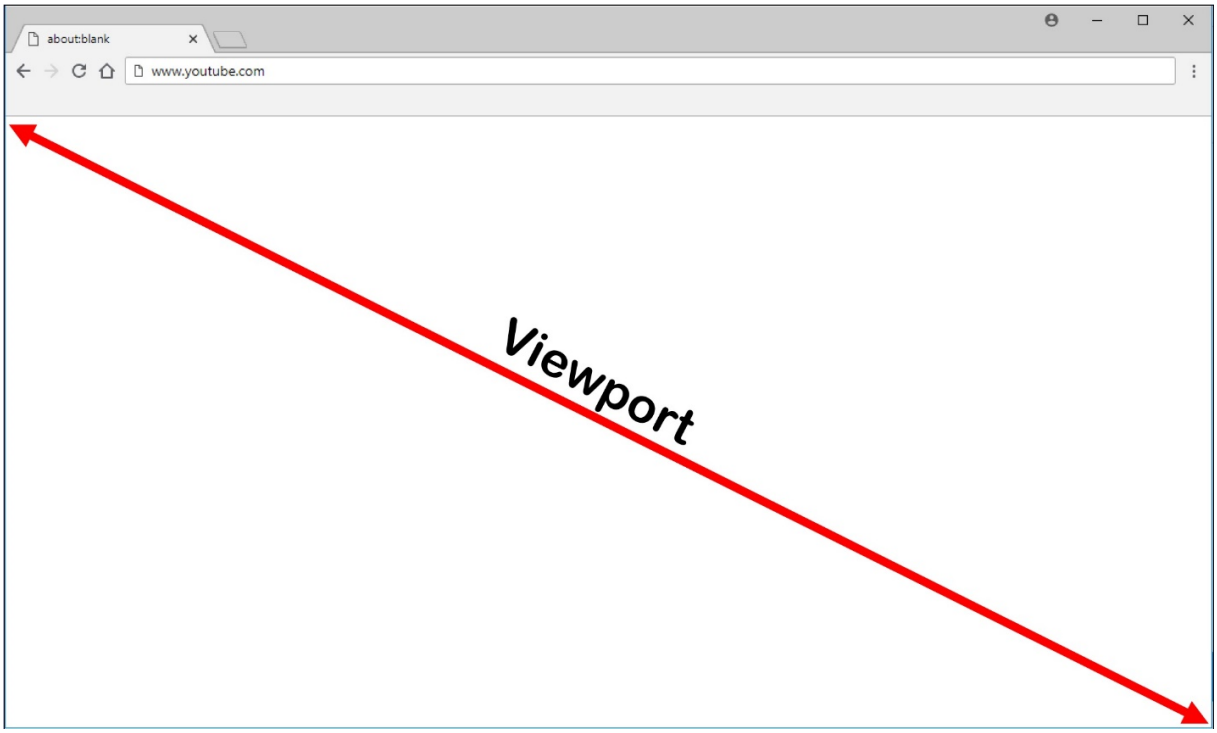
March 15, 2022

Die Umleitung des Browserinhalts verhindert die VDA-seitige Wiedergabe von Webseiten auf einer Positivliste. Dabei wird von der Citrix Workspace-App clientseitig die Instanz einer entsprechenden Renderingengine erzeugt, die den HTTP- und HTTPS-Inhalt von der URL abruft.

> **Hinweis:**
>
> Sie können festlegen, dass Webseiten mithilfe einer Sperrliste an den VDA (jedoch nicht clientseitig) umgeleitet werden.

Diese Overlay-Weblayoutengine wird statt auf dem VDA auf dem Endpunktgerät ausgeführt und verwendet dessen CPU, GPU, Arbeitsspeicher und Netzwerk.

Es wird nur der Browserviewport umgeleitet. Der Viewport ist der rechteckige Browserbereich, in dem der Inhalt angezeigt wird. Der Viewport enthält keine Elemente wie Adressleiste, Favoriten-Symbolleiste und Statusleiste. Diese Elemente sind Teil der Benutzeroberfläche und werden weiterhin auf dem VDA im Browser ausgeführt.

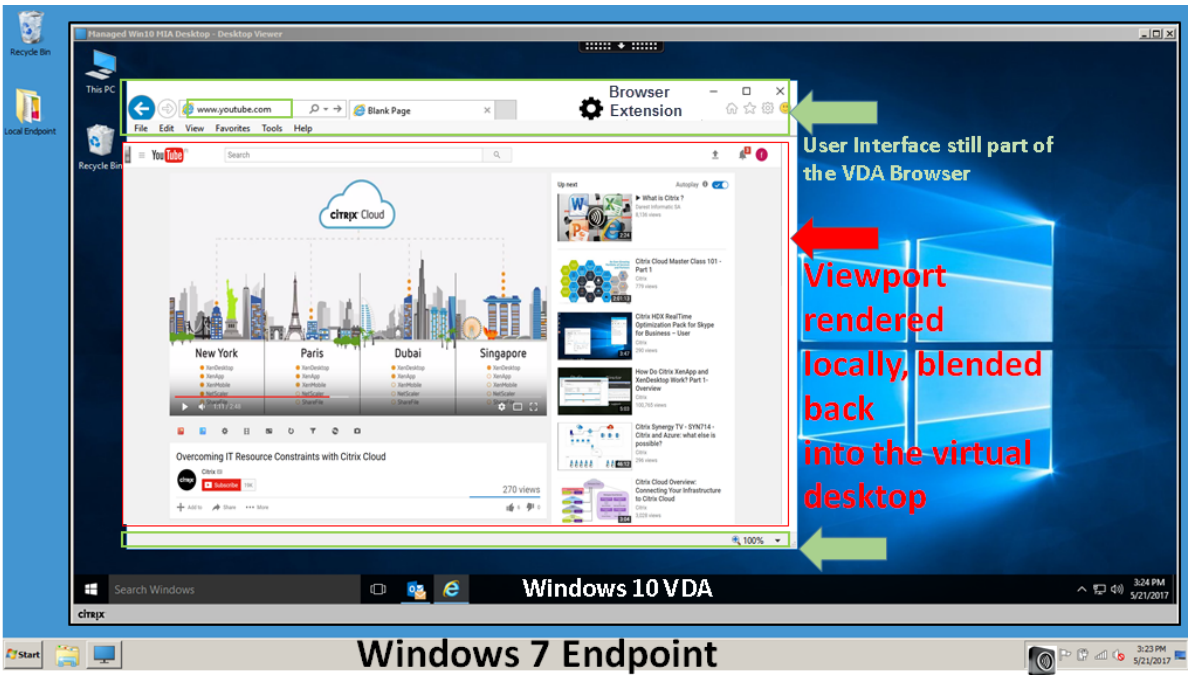


1. Konfigurieren Sie eine Studio-Richtlinie mit der Positivliste der umzuleitenden URLs bzw. mit einer Sperrliste nicht umzuleitender URL-Pfade. Der Abgleich der von den Benutzern angesteuerten URLs gegen die Positiv- oder Sperrliste wird von einer Browsererweiterung durchgeführt. Die Browsererweiterung (BHO) für Internet Explorer 11 ist auf dem Installationsmedium enthalten und wird automatisch installiert. Die Browsererweiterung für Chrome steht im Chrome Web Store zur Verfügung und kann über Gruppenrichtlinien und ADMX-Dateien bereitgestellt werden. Chrome-Erweiterungen werden für einzelne Benutzer installiert. Das Update eines Gold-Masterimages zum Hinzufügen oder Entfernen einer Erweiterung ist nicht erforderlich.
2. Wird eine Übereinstimmung in der Positivliste gefunden (z. B. `https://www.mycompany.com/`) und keine Übereinstimmung mit einer URL in der Sperrliste (z. B. `https://www.mycompany.com/engineering`), weist ein virtueller Kanal (CTXCSB) die Citrix Workspace-App an, dass eine Umleitung erforderlich ist und leitet die URL weiter. Die Citrix Workspace-App erzeugt dann eine lokale Renderingengine-Instanz und zeigt die Website an.
3. Anschließend fügt die Citrix Workspace-App die Website nahtlos in den Inhaltsbereich des virtuellen Desktopbrowsers ein.

Die Farbe des Logos gibt den Status der Chrome-Erweiterung an. Folgende drei Farben sind möglich:

- Grün: Aktiv und verbunden.
- Grau: Nicht aktiv/Leerlauf auf der aktuellen Registerkarte.
- Rot: Defekt/außer Betrieb.

Sie können Debugprotokolle mit den **Optionen** im Erweiterungsmenü festlegen.



> **Wichtig:**
>
> Die folgenden Einstellungen gelten nur für 1912 LTSR CU1 oder höher.

Szenarien für den Inhaltsabruf durch die Citrix Workspace-App:

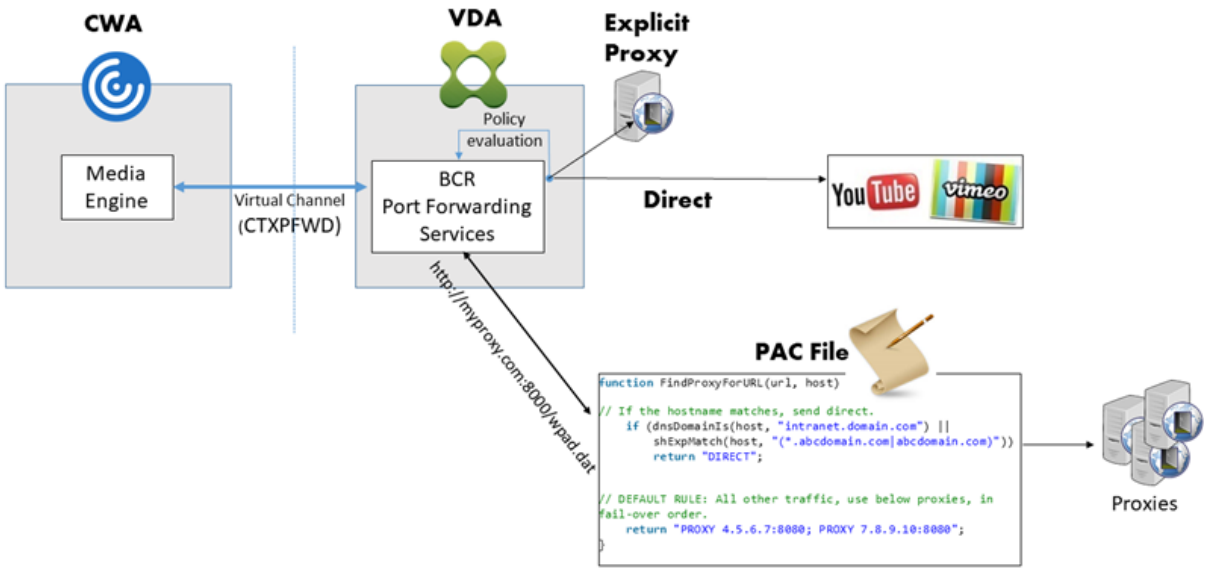
- **Abruf und Wiedergabe auf dem Server:** Es findet keine Umleitung statt, weil die Site nicht auf der Positivliste steht oder ein Fehler aufgetreten ist. Die Wiedergabe findet dann auf dem VDA statt und das Grafikremoting mithilfe von Thinwire. Verwenden Sie Richtlinien, um dieses Fallbackverhalten zu steuern. Es fällt ein hoher CPU-, RAM- und Bandbreitenverbrauch auf dem VDA an.
- **Abruf auf dem Server, Wiedergabe auf dem Client:** Die Citrix Workspace-App ruft den Inhalt über den VDA und einen virtuellen Kanal (CTXPFWD) vom Webserver ab. Diese Option ist nützlich, wenn Clients keinen Internetzugang haben (z. B. Thin Clients). Der CPU- und RAM-Verbrauch auf dem VDA ist niedrig, jedoch wird Bandbreite im virtuellen ICA-Kanal verbraucht.

  Es gibt drei Betriebsmodi für dieses Szenario. Der Begriff "Proxy"bezieht sich hier auf ein Proxygerät, auf das der VDA für den Internetzugang zugreift.

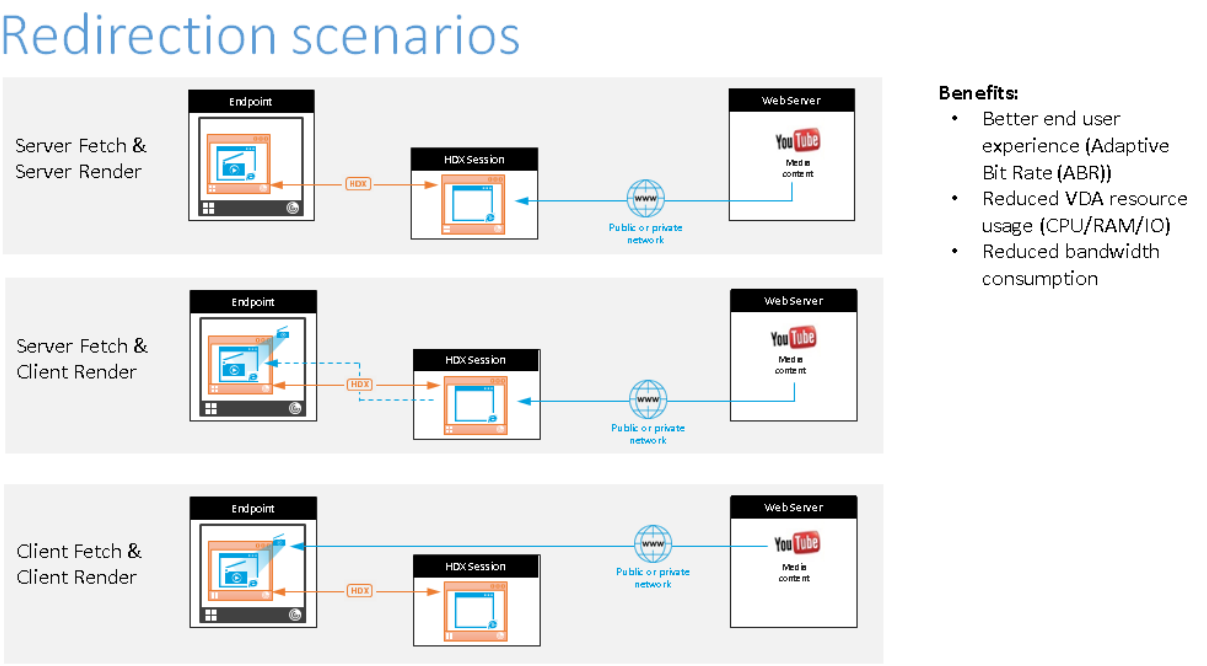
  Geeignete Richtlinienoption:

  - Expliziter Proxy: Wenn Sie einen einzelnen expliziten Proxy im Datencenter haben. Hiermit leiten Sie den Datenverkehr der Browserinhaltsumleitung über den VDA an den angegebenen Webproxy weiter.

- Direkt oder transparent: Wenn Sie keine Proxys haben oder transparente Proxys verwenden. Hiermit leiten Sie den Datenverkehr der Browserinhaltsumleitung über den VDA direkt an den Webserver weiter, der den Inhalt hostet.
- PAC-Dateien: Wenn Sie PAC-Dateien verwenden, sodass Browser auf dem VDA automatisch den geeigneten Proxyserver zum Abrufen einer angegebenen URL auswählen können. Hiermit leiten Sie den Datenverkehr der Browserinhaltsumleitung über den VDA an den durch Auswertung der angegebenen PAC-Datei ermittelten Webproxy weiter.



- **Abruf und Wiedergabe auf dem Client:** Da die Citrix Workspace-App direkt auf den Webserver zugreift, ist Internetzugang erforderlich. In diesem Szenario wird die gesamte Netzwerk-, CPU- und RAM-Last von der XenApp und XenDesktop-Site abgeladen.



Fallbackmechanismus:

Es kann vorkommen, dass die Clientumleitung fehlschlägt. Wenn der Client beispielsweise keinen direkten Internetzugriff hat, kann eine Fehlerantwort an den VDA zurückgegeben werden. In einem solchen Fall kann der Browser auf dem VDA die Seite auf dem Server neu laden und wiedergeben.

Verwenden Sie die Richtlinie **Verhindern von Fallback auf Windows Media**, um eine serverseitige Wiedergabe von Videoelementen zu verhindern. Legen Sie diese Richtlinie auf **Alle Inhalte nur auf Client wiedergeben** oder **Nur Inhalte auf Client wiedergeben, auf die Client Zugriff hat** fest. Diese Einstellungen verhindern die Wiedergabe von Videoelementen auf dem Server, wenn die Clientumleitung fehlschlägt. Diese Richtlinie wird nur wirksam, wenn Sie die Browserinhaltsumleitung aktivieren und die Richtlinie **Zugriffssteuerungsliste** die URL für ein Fallback enthält. Die URL darf nicht in der Sperrlistenrichtlinie enthalten sein.

Systemanforderungen:

Windows-Endpunkte:

- Windows 7, 8.x oder 10
- Citrix Workspace-App 1809 für Windows oder höher
- Citrix Receiver für Windows 4.10 oder später

> **Hinweis:**
>
> Die Citrix Workspace-App 1912 LTSR für Windows und sämtliche kumulativen Updates für die Citrix Workspace-App 1912 LTSR unterstützen keine Browserinhaltsumleitung.

Linux-Endpunkte:

- Citrix Workspace-App 1808 für Linux oder später
- Citrix Receiver für Linux 13.9 oder später
- Thin Client-Terminals müssen WebKitGTK+ enthalten.

Citrix Virtual Apps and Desktops 7 1808 und XenApp und XenDesktop 7.15 CU5, 7.18, 7.17, 7.16:

- VDA-Betriebssystem: Windows 10 (mindestens Version 1607), Windows Server 2012 R2, Windows Server 2016
- Browser auf dem VDA:
  - Google Chrome v66 oder höher (Chrome erfordert Citrix Workspace-App 1809 für Windows auf dem Benutzerendpunkt, Citrix Virtual Apps and Desktops 7 1808-VDA und Erweiterung für die Browserinhaltsumleitung)
  - Explorer 11 mit folgender Konfiguration:
    * Deaktivieren von **Erweiterter geschützter Modus** unter **Internetoptionen** > **Erweitert > Sicherheit**
    * Aktivieren von **Browsererweiterungen von Drittanbietern aktivieren** unter **Internetoptionen > Erweitert > Browsen**

Problembehandlung:

Informationen zur Problembehandlung finden Sie unter https://support.citrix.com/article/CTX230052

Chrome-Erweiterung für die Browserinhaltsumleitung

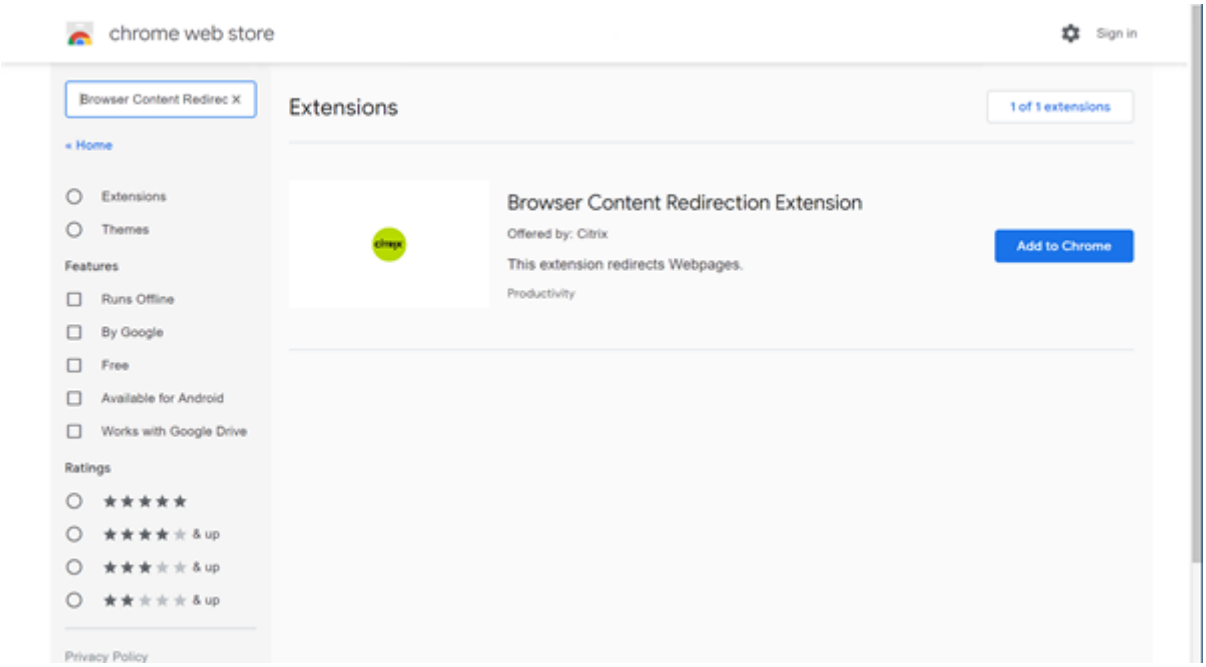
Zur Verwendung der Browserinhaltsumleitung in Chrome fügen Sie die entsprechende Browsererweiterung aus dem Chrome Web Store hinzu. Klicken Sie auf **Zu Chrome hinzufügen** in der Citrix Virtual Apps and Desktops-Umgebung.

Die Erweiterung ist nur auf dem VDA und **nicht** auf dem Client des Benutzers erforderlich.

Systemanforderungen

- Chrome v66 oder höher
- Erweiterung für die Browserinhaltsumleitung
- Citrix Virtual Apps and Desktops 7 1808 oder höher
- Citrix Workspace-App 1809 für Windows oder höher

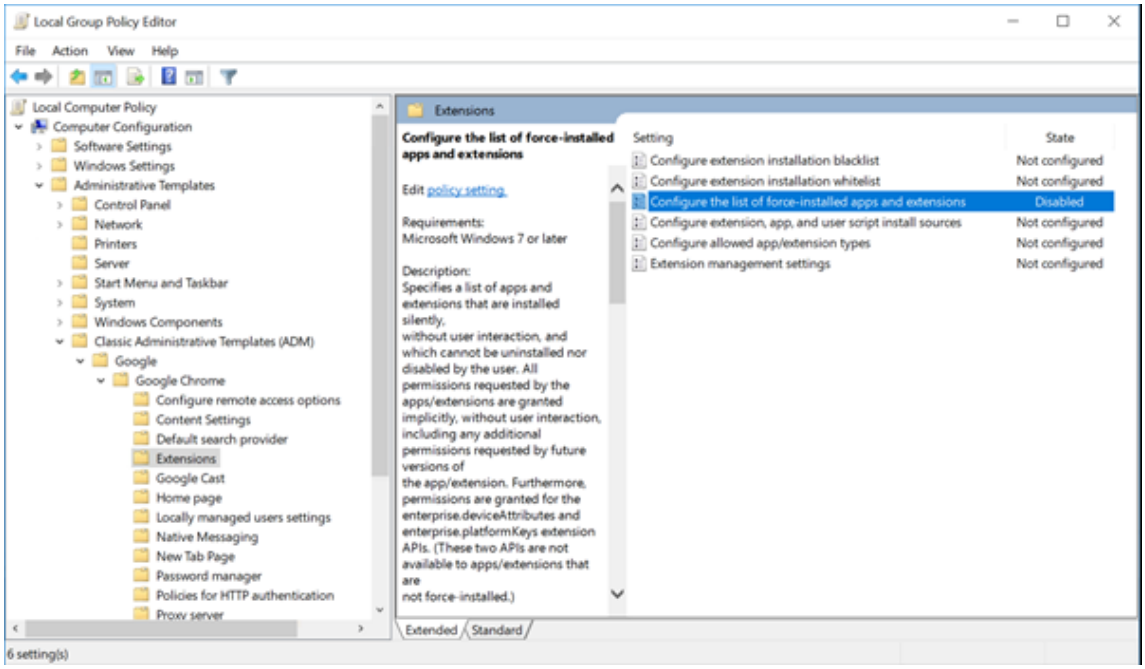
> **Hinweis:**
>
> Die Citrix Workspace-App 1912 LTSR für Windows und sämtliche kumulativen Updates für die Citrix Workspace-App 1912 LTSR unterstützen keine Browserinhaltsumleitung.



Diese Methode funktioniert für einzelne Benutzer. Um die Erweiterung für eine große Benutzergruppe bereitzustellen, verwenden Sie die Gruppenrichtlinie.

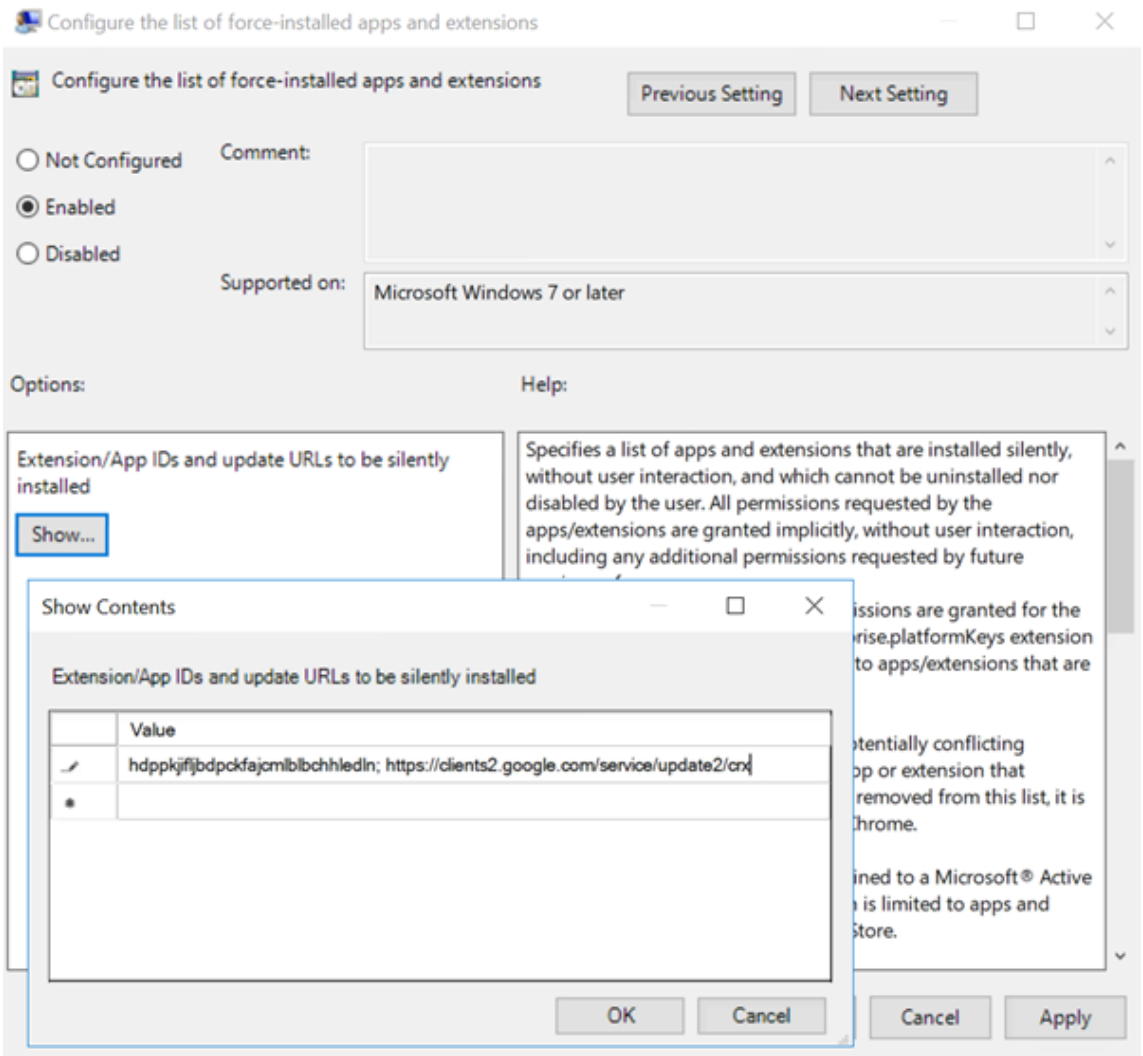
Bereitstellen der Erweiterung per Gruppenrichtlinie

1. Importieren Sie die Google Chrome-ADMX-Dateien in Ihre Umgebung. Informationen zum Herunterladen, Installieren und Konfigurieren von Richtlinienvorlagen im Gruppenrichtlinien-Editor finden Sie unter https://support.google.com/chrome/a/answer/187202?hl=en.
2. Öffnen Sie die Gruppenrichtlinien-Verwaltungskonsole und wechseln Sie zu **Benutzerkonfiguration\Administrative Vorlagen\Klassische administrative Vorlage (ADM)\Google\Google Chrome\Erweiterungen**. Aktivieren Sie die Einstellung **Configure the list of force-installed apps and extensions**.



3. Klicken Sie auf **Show** und geben Sie die folgende Zeichenfolge ein (= Erweiterungs-ID). Aktualisieren Sie die URL für die Browserinhaltsumleitungserweiterung.

   ```
   hdppkjifljbdpckfajcmlblbchhledln; https://clients2.google.com/service/update2/crx
   ```

4. Übernehmen Sie die Einstellung. Nach einer **gpudate**-Aktualisierung erhält der Benutzer automatisch die Erweiterung. Beim Starten des Chrome-Browsers in der Benutzersitzung wird die Erweiterung angewendet und kann vom Benutzer nicht entfernt werden.

   Alle Updates der Erweiterung werden automatisch auf den Maschinen der Benutzer über die Update-URL installiert, die Sie in der Einstellung angegeben haben.

   Wird für die Einstellung **Configure the list of force-installed apps and extensions** der Wert **Disabled** festgelegt, wird die Erweiterung automatisch für alle Benutzer entfernt.

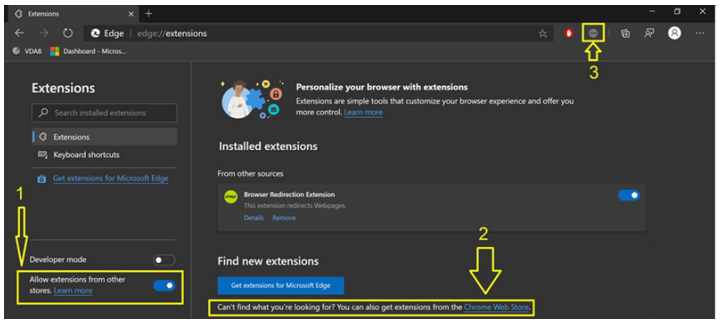
Edge Chromium-Erweiterung für die Browserinhaltsumleitung

Um die Erweiterung zur Browserinhaltsumleitung in Edge zu installieren, müssen Sie Version **83.0.478.37** oder höher des Edge-Browsers verwenden.

1. Klicken Sie im Menü auf die Option **Extensions**, und aktivieren Sie **Allow extensions from other**

stores.

2. Klicken Sie auf den Link **Chrome Web Store** und die Erweiterung wird in der Leiste oben rechts angezeigt.
   Weitere Informationen zu Microsoft Edge-Erweiterungen finden Sie unter Erweiterungen.



Umleitung des Browserinhalts und DPI

> **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.

Bei Verwendung der Browserinhaltsumleitung mit einer DPI-Skalierung von mehr als 100 % auf der Maschine des Benutzers wird der umgeleitete Browserinhalt fehlerhaft angezeigt. Richten Sie die DPI nicht ein, wenn Sie die Browserinhaltsumleitung verwenden, um dieses Problem zu vermeiden. Eine weitere Möglichkeit besteht darin, die GPU-Beschleunigung der Browserinhaltsumleitung für Chrome zu deaktivieren, indem Sie den folgenden Registrierungsschlüssel auf der Maschine des Benutzers erstellen:

\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\HdxMediaStream

Name: GPU

Typ: DWORD

Wert: 0

HDX-Videokonferenzen und Webcam-Videokomprimierung

September 21, 2021

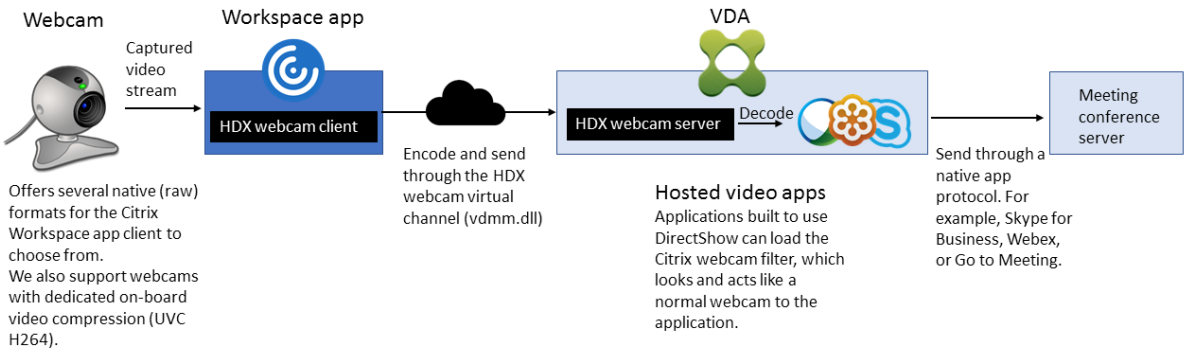
> **Warnung:**
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen 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.

Webcams können in Anwendungen, die innerhalb virtueller Sitzungen ausgeführt werden, unter Einsatz der HDX-Webcamvideokomprimierung oder der per HDX Plug-n-Play verfügbaren generischen USB-Umleitung verwendet werden. Verwenden Sie **Citrix Workspace-App > Einstellungen > Geräte** zum Umschalten zwischen diesen Modi.
Citrix empfiehlt, nach Möglichkeit die HDX-Webcamvideokomprimierung zu verwenden.
Um zu verhindern, dass Benutzer die HDX-Webcamvideokomprimierung ändern, deaktivieren Sie die Umleitung von USB-Geräten über die Richtlinieneinstellungen unter ICA > USB-Geräte. Citrix Workspace-App-Benutzer können das Standardverhalten außer Kraft setzen, wenn sie in Desktop Viewer unter **Mikrofon & Webcam** die Einstellung **Mikrofon und Webcam nicht verwenden** auswählen.

HDX-Webcamvideokomprimierung

Die HDX-Webcamvideokomprimierung wird auch als **optimierter** Webcammodus bezeichnet. Bei dieser Webcamvideokomprimierung wird die Multimediaframework-Technologie des Clientbetriebssystems verwendet, um Videos von Aufnahmegeräten zu erfassen, zu transcodieren und zu komprimieren. Hersteller von Aufnahmegeräten liefern Treiber, die sich in die Betriebssystem-Kernelstreaming-Architektur einfügen.

Der Client übernimmt die Kommunikation mit der Webcam. Der Client sendet Videos nur an Server, die es ordnungsgemäß anzeigen können. Der Server ist nicht direkt mit der Webcam verbunden, doch er ist integriert, so dass die gleiche Erfahrung auf dem Desktop geliefert wird. Die Workspace-App komprimiert Videos zum Einsparen von Bandbreite und zur Gewährleistung einer besseren Ausfallsicherheit in WANs.



HDX-Webcam-Videokomprimierung erfordert, dass die folgenden Richtlinieneinstellungen aktiviert sind (alle sind standardmäßig aktiviert).

- Multimediakonferenzen
- Windows Media-Umleitung

Bei Hardware-verschlüsselungsfähigen Webcams verwendet HDX-Videokomprimierung die Hardware-Codierung standardmäßig. Die Hardwarecodierung kann mehr Bandbreite verbrauchen als die Softwarecodierung. Zum Erzwingen der Softwarekomprimierung fügen Sie dem folgenden Registrierungsschlüssel den folgenden DWORD-Wert hinzu:

HKEY_CURRENT_USER\Software\Citrix\HdxRealTime: DeepCompress_ForceSWEncode=1

Anforderungen für die HDX RealTime-Webcamvideokomprimierung

Unterstützte Clients: Citrix Workspace-App für Windows, Citrix Workspace-App für Mac, Citrix Workspace-App für Chrome und Citrix Workspace-App für Linux

> **Hinweis:**
>
> Die Webcamumleitung für 64-Bit-Apps wird nur von der Citrix Workspace-App für Windows, Citrix Workspace-App für Chrome und Citrix Workspace-App für Mac 2006 oder höher unterstützt.

Unterstützte Videokonferenzanwendungen (32 und 64 Bit):

- Adobe Connect
- Cisco Webex und Webex für Teams
- GoToMeeting
- Google Hangouts und Hangouts Meet
- IBM Sametime
- Microsoft Skype for Business Server 2015
- Microsoft Lync 2010 und 2013
- Microsoft Skype 7 oder höher

- Media Foundation-basierte Videoanwendungen auf Windows 8.x oder höher und Windows Server 2012 R2 oder höher

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

  Daten: 240

  Name: DefaultWidth, Typ: REG_DWORD

  Daten: 320

- Serverregistrierungsschlüssel HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Vd3d\Kompatibilität

  Name: skype.exe,

  Typ: REG_DWORD

  Daten: auf 0 festlegen

Andere Anforderungen an Benutzergeräte:

- Geeignete Hardware für die Audiowiedergabe
- DirectShow-kompatible Webcam (Webcam-Standardeinstellungen verwenden). Hardware-codierungsfähige Webcams senken die clientseitige CPU-Nutzung.
- Installieren Sie für die HDX-Webcamvideokomprimierung möglichst die Webcamtreiber des Herstellers auf dem Client.

HD-Webcamstreaming

Die Videokonferenzanwendung auf dem Server wählt Format und Auflösung von Webcams basierend auf den unterstützten Formatarten. Beim Sitzungsstart sendet der Client die Webcam-Informationen an den Server. Sie wählen eine Webcam über die Anwendung aus. Wenn Webcam und Anwendung HD-Wiedergabe unterstützen, wird HD in der Anwendung verwendet. Es werden Webcamauflösungen bis zu 1920 x 1080 unterstützt.

Dieses Feature erfordert mindestens Citrix Workspace-App für Windows 1808 bzw. Version 4.10 von Citrix Receiver für Windows.

Sie können das Feature über einen Registrierungsschlüssel deaktivieren. Die Standardauflösung 352 x 288 wird verwendet:

HKEY_LOCAL_MACHINE\Software\Citrix\HDXRealTime

Name: Enable_HighDefWebcam

Typ: REG_DWORD

Daten: 0 = HD-Webcamstreaming deaktivieren

Anhand der Registrierungsschlüssel auf dem Client können Sie eine bestimmte Auflösung konfigurieren. Stellen Sie sicher, dass die Webcam die angegebene Auflösung unterstützt:

HKEY_CURRENT_USER\Software\Citrix\HDXRealTime

Name: DefaultWidth

Typ: REG_DWORD

Daten (dezimal): gewünschte Breite (zum Beispiel 1280)

Name: DefaultHeight

Typ: REG_DWORD

Daten (dezimal): gewünschte Höhe (zum Beispiel 720)

Generische HDX-USB-Umleitung für Plug & Play

Die generische HDX-USB-Umleitung für Plug & Play wird auch als **generischer** Webcammodus bezeichnet. Der Vorteil der per HDX Plug-n-Play verfügbaren generischen USB-Umleitung besteht darin, dass Sie keine Treiber auf dem Thin Client bzw. Endpunkt installieren müssen. Der USB-Stack wird so virtualisiert, dass alles, was Sie an den lokalen Client anschließen, an die Remote-VM umgeleitet wird. Auf dem Remotedesktop erscheint dies, als ob Sie das Gerät nativ angeschlossen hätten. Der Windows-Desktop übernimmt die gesamte Interaktion mit der Hardware und sucht anhand der Plug-and-Play-Logik die richtigen Treiber. Die meisten Webcams funktionieren, wenn die Treiber vorhanden sind und über ICA funktionieren. Der generische Webcammodus verbraucht wesentlich mehr Bandbreite (viele Megabits pro Sekunde), da unkomprimierte Videodaten mit dem USB-Protokoll über das Netzwerk gesendet werden.

HTML5-Multimediaumleitung

June 27, 2024

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 dem Laufwerk 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. Zum Untersuchen von Videoelementen auf Webseiten und Ermitteln von deren Quelle (ein MP4-Containerformat) im HTML5-Video-Tags verwenden Sie die Browser-Entwicklertools:

Vergleich von HTML5 und Flash

Feature	HTML5	Flash
Proprietärer Player erforderlich	Nein	Ja
Läuft auf Mobilgeräten	Ja	Auf einigen
Wiedergabegeschwindigkeit auf unterschiedlichen Plattformen	Hoch	Slow
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.

Folgendes wird unterstützt und durch Richtlinien gesteuert. Weitere Informationen finden Sie unter Richtlinieneinstellungen für Multimedia.

- Serverseitige Wiedergabe
- Serverseitiger Abruf/clientseitige Wiedergabe
- Clientseitiger Abruf und clientseitige Wiedergabe

Mindestversionen von Citrix Workspace-App und Citrix Receiver:

- Citrix Workspace-App 1808 für Windows
- Citrix Receiver für Windows 4.5
- Citrix Workspace-App 1808 für Linux
- Citrix Receiver für Linux 13.5

Mindest-VDA-Browserversion	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
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
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

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

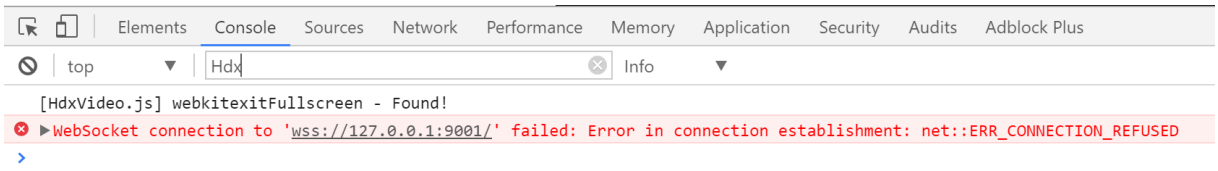
In diesem Release ist dieses Feature nur für Webseiten verfügbar, die unter Ihrer Kontrolle stehen. Die Aktivierung erfordert das Hinzufügen der JavaScript-Datei HdxVideo.js (auf dem Citrix Virtual Apps and Desktops-Installationsmedium enthalten) zu Webseiten mit HTML5-Multimediainhalt. Beispiel: Videos 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:



Optimierung für Microsoft Teams

April 5, 2024

> **Wichtig:**
>
> Die Optimierung für Microsoft Teams erfordert mindestens Microsoft Teams Version 1.2.00.31357.

Citrix bietet eine Optimierung für die Verwendung der Desktopversion von Microsoft Teams in Citrix Virtual Apps and Desktops und der Citrix Workspace-App. Standardmäßig werden alle erforderlichen Komponenten in die Citrix Workspace-App und den Virtual Delivery Agent (VDA) gepackt.

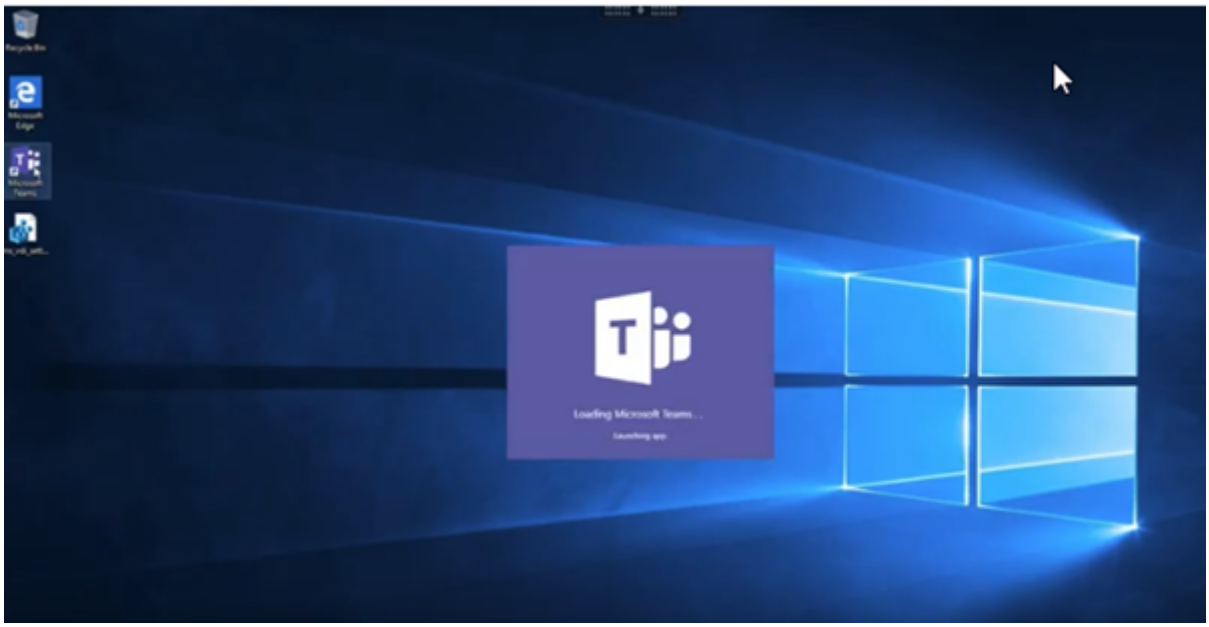
Die Optimierung für Microsoft Teams enthält VDA-seitige HDX-Dienste und -API, die als Schnittstelle mit der von Microsoft Teams gehosteten App zum Empfangen von Befehlen fungieren. Diese Komponenten öffnen einen virtuellen Steuerungskanal (CTXMTOP) zur Media Engine der Citrix Workspace-App. Der Endpunkt decodiert Multimedia lokal und gibt sie lokal wieder, wobei das Fenster der Citrix Workspace-App in die gehostete Microsoft Teams-App zurückverschoben wird.

Authentifizierung und Signalisierung erfolgen nativ in der von Microsoft Teams gehosteten App, genau wie die anderen Microsoft Teams-Dienste (zum Beispiel Chat oder Teamarbeit). Die Audio-/Videoumleitung hat auf sie keine Auswirkungen.

CTXMTOP ist ein virtueller Command-and-Control-Kanal. Dies bedeutet, dass Medien nicht zwischen der Citrix Workspace-App und dem VDA ausgetauscht werden.

Nur Clientabruf und Clientwiedergabe sind verfügbar.

In diesem Video wird gezeigt, wie Microsoft Teams in einer virtuellen Citrix Umgebung funktioniert.



Installation von Microsoft Teams

> **Hinweis:**
>
> Wir empfehlen, den VDA zu installieren, bevor Teams im goldenen Image installiert wird. Diese Installationsreihenfolge ist notwendig, damit das Flag **ALLUSER=1** wirksam wird. Wenn Teams auf der virtuellen Maschine vor dem VDA installiert wurde, deinstallieren Sie Teams und installieren

> Sie es neu. Wenn Sie App Layering verwenden, finden Sie in den App Layering-Anleitungen am Ende dieses Abschnitts weitere Details.

Wir empfehlen, die Richtlinien zur maschinenweiten Installation von Microsoft Teams zu befolgen und nicht das EXE-Installationsprogramm zu verwenden, mit dem Teams in `AppData` installiert wird. Installieren Sie die Software stattdessen an der Befehlszeile mit dem Flag **ALLUSER=1** unter `C:\Program Files (x86)\Microsoft\Teams`.

```
msiexec /i <path_to_msi> /l*v <install_logfile_name> ALLUSER=1
ALLUSERS=1
```

In diesem Beispiel wird auch der Parameter **ALLUSERS=1** verwendet. Wenn Sie diesen Parameter festlegen, wird das maschinenweite Installationsprogramm von Teams für alle Benutzer des Computers in der Systemsteuerung unter **Programme und Funktionen** und in den Windows-Einstellungen unter **Apps und Features** angezeigt. Alle Benutzer können Teams dann deinstallieren, wenn sie über Administratorrechte verfügen. Es ist wichtig, den Unterschied zwischen **ALLUSERS=1** und **ALLUSER=1** zu verstehen. Sie können den Parameter **ALLUSERS=1** in Nicht-VDI- und in VDI-Umgebungen verwenden. Den Parameter **ALLUSER=1** verwenden Sie nur in VDI-Umgebungen, um eine Installation pro Maschine festzulegen.

Im Modus **ALLUSER=1** wird die Teams-Anwendung nicht automatisch aktualisiert, sobald eine neue Version vorhanden ist. Dieser Modus wird für nicht persistente Umgebungen empfohlen. Dazu gehören gehostete freigegebene Apps oder Desktops aus zufälligen/gepoolten Katalogen mit Windows Server oder Windows 10. Weitere Informationen finden Sie unter Installieren von Microsoft Teams mit MSI (Abschnitt VDI-Installation).

Sie verfügen über dedizierte persistente VDI-Umgebungen mit Windows 10. Wenn Sie die Teams-Anwendung automatisch aktualisieren und pro Benutzer unter `Appdata/Local` installieren möchten, verwenden Sie das `.exe`-Installationsprogramm oder das MSI ohne **ALLUSER =1**.

Für App Layering:

> **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.

Erstellen Sie einen leeren Registrierungsschlüssel mit dem Namen `PortICA` (lassen Sie die Standardeinstellungen für Name, Typ und Wert).

Wenn Sie Citrix App Layering zum Verwalten von VDA- und Microsoft Teams-Installationen auf

verschiedenen Ebenen verwenden, stellen Sie diesen Registrierungsschlüssel unter Windows bereit, bevor Sie Teams mit **ALLUSER = 1**installieren:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

Oder

`HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\PortICA`

Empfehlungen zur Profilverwaltung

Es empfiehlt sich, das maschinenweite Installationsprogramm für Windows Server- und gepoolte VDI-Umgebungen mit Windows 10 zu verwenden.

Wenn das Flag **ALLUSER =1** an der Befehlszeile (maschinenweites Installationsprogramm) an das MSI übergeben wird, wird die Teams-App unter `C:\Program Files (x86)` installiert (~300 MB). Die App verwendet `AppData\Local\Microsoft\TeamsMeetingAddin` für Protokolle und `AppData\Roaming\Microsoft\Teams` (~600–700 MB) für benutzerspezifische Konfigurationen, das Zwischenspeichern von Elementen der Benutzeroberfläche usw.

Maschinenweites Installationsprogramm

Im Folgenden finden Sie ein Beispiel für Ordner, Desktopverknüpfungen und Registrierungen, die bei der Installation von Teams mit dem maschinenweiten Installationsprogramm auf einer VM mit Windows Server 2016 64-Bit erstellt werden:

Ordner:

- `C:\Program Files (x86)\Microsoft\Teams`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

Desktopverknüpfung:

`C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe`

Registrierung:

- `HKEY_LOCAL_MACHINE \SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`

Empfehlungen

- Es wird empfohlen, den automatischen Start durch Löschen der Teams-Registrierungsschlüssel zu deaktivieren. Dadurch verhindert, dass "Anmeldestürme"zu Beginn der Bürozeit zu Auslastungsspitzen bei der VM-CPU führen.
- Wenn der virtuelle Desktop keinen GPU/vGPU hat, wird empfohlen, die Einstellung **GPU-Hardwarebeschleunigung deaktivieren** in den **Einstellungen** von Teams festzulegen, um die Leistung zu verbessern. Die Einstellung (`"disableGpu":true`) wird in `%Appdata%\Microsoft\Teams` in der Datei `desktop-config.json` gespeichert. Sie können diese Datei mit einem Anmeldeskript bearbeiten und den Wert auf true festlegen.
- Wenn Sie Citrix Workspace Environment Management (WEM) verwenden, aktivieren Sie **CPU Spikes Protection**, um die Prozessornutzung durch Teams zu verwalten.

> **Wichtig:**
>
> Wenn Sie das Flag **ALLUSER=1** nicht übergeben, speichert die MSI das Teams.exe-Installationsprogramm und `setup.json` unter `C:\Program Files (x86)\Teams Installer`.
> Ein Registrierungsschlüssel (TeamsMachineInstaller) wird unter:
> `HKEY_LOCAL_MACHINE \SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run`
> hinzugefügt.
> Eine nachfolgende Benutzeranmeldung löst stattdessen die endgültige Installation in **AppData** aus.

Installationsprogramm pro Benutzer

Das `.exe`-Installationsprogramm funktioniert völlig anders, alle Dateien werden in AppData gespeichert.

Ordner:

- `C:\Users\<username>\AppData\Local\Microsoft\Teams`
- `C:\Users\<username>\AppData\Local\Microsoft\TeamsPresenceAddin`
- `C:\Users\<username>\AppData\Local\Microsoft\TeamsMeetingAddin`
- `C:\Users\<username>\AppData\Local\SquirrelTemp`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

Desktopverknüpfung:

```
C:\Users\<username>\AppData\Local\Microsoft\Teams\Update.exe --processStart "Teams.exe"
```

Registrierung:

```
HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```


Bewährte Methoden

Die Empfehlungen bewährter Methoden basieren auf den Anwendungsfällen.
Die Verwendung von Teams mit flüchtigem Setup erfordert einen Profilcaching-Manager für die effiziente Synchronisierung der Teams-Laufzeitdaten. Ein Profilcaching-Manager gewährleistet, dass die richtigen benutzerspezifischen Informationen (z. B. Benutzerdaten, Profil und Einstellungen) während der Benutzersitzung zwischengespeichert werden. Es müssen die Daten in den folgenden beiden Ordnern synchronisiert werden:

- `C:\Users\<username>\AppData\Local\Microsoft\IdentityCache`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

Ausschlussliste für zwischengespeicherte Teams-Inhalte bei flüchtigem Setup:

Schließen Sie die nachfolgend aufgeführten Elemente aus dem Teams-Cachingordner `%AppData%/Microsoft/Teams` aus. Durch Ausschließen dieser Elemente wird die Größe des Benutzercaches reduziert und das flüchtige Setup weiter optimiert.

Ausschlussliste - Dateien

- Roaming\Microsoft\Teams*.txt

Ausschlussliste - Verzeichnisse

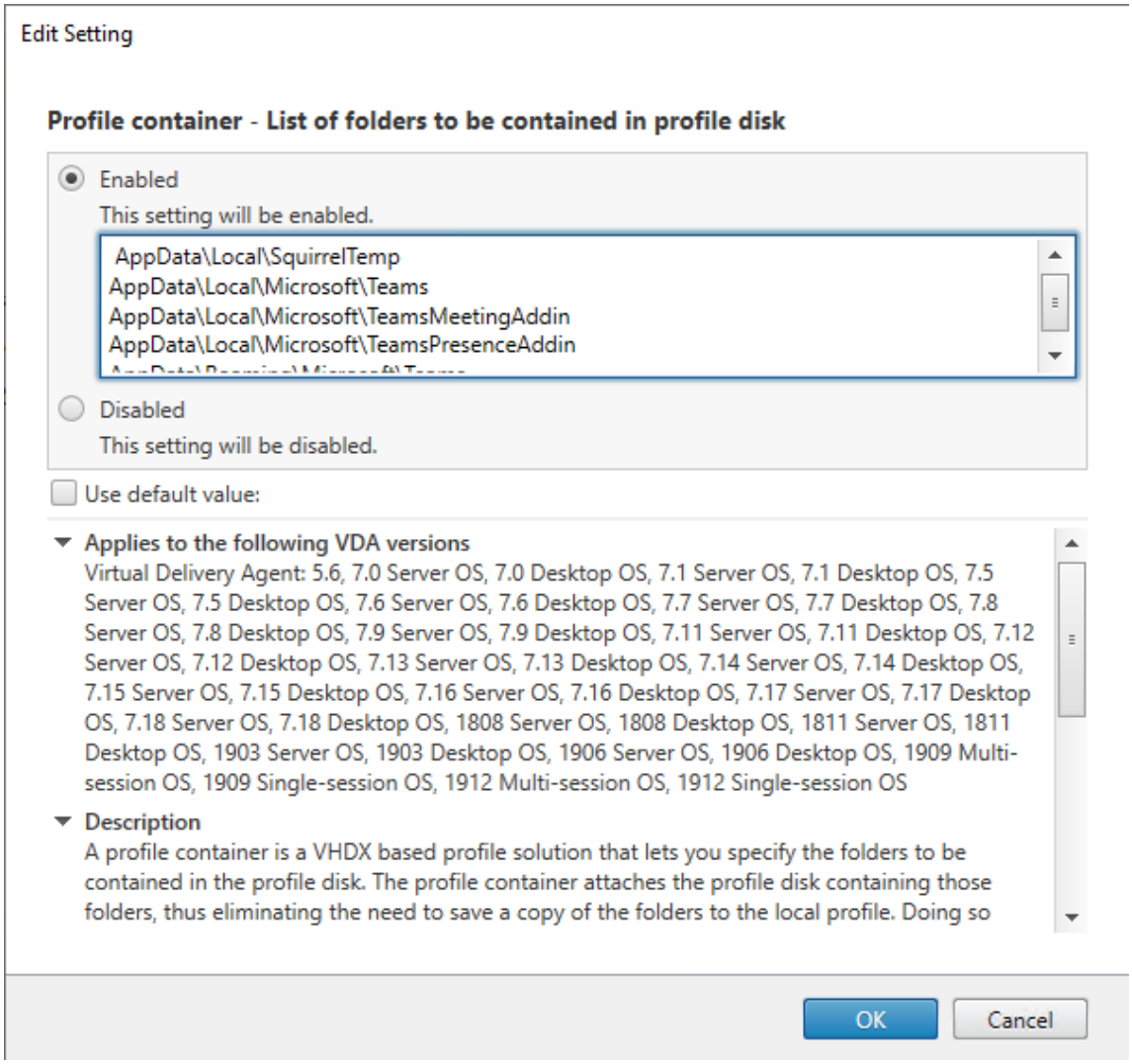
- Roaming\Microsoft\Teams\Logs
- Roaming\Microsoft\Teams\media-stack
- Roaming\Microsoft\Teams\Service Worker\CacheStorage
- Roaming\Microsoft\Teams\Application Cache
- Roaming\Microsoft\Teams\Cache
- Roaming\Microsoft\Teams\GPUCache
- Roaming\Microsoft\Teams\meeting-addin\Cache (kritisch bei Problemen, bei denen das Add-In in Outlook fehlt)

Anwendungsfall Einzelsitzung:

In diesem Szenario verwendet der Endbenutzer Microsoft Teams an einem Ort. Es ist nicht notwendig, Teams in zwei verschiedenen Windows-Sitzungen gleichzeitig auszuführen. Beispielsweise wird gewöhnlich jedem Benutzer ein virtueller Desktop zugewiesen und Teams im virtuellen Desktop als Anwendung bereitgestellt.
Wir empfehlen, Citrix Profilcontainer zu aktivieren und die o. g. Benutzerverzeichnisse in den Container umzuleiten.

1. Stellen Sie das maschinenweite Microsoft Teams-Installationsprogramm (**ALLUSER=1**) im Gold-Image bereit.

2. Aktivieren Sie die Citrix Profilverwaltung und richten Sie den Benutzerprofilspeicher mit den korrekten Berechtigungen ein.
3. Aktivieren Sie folgende Richtlinieneinstellung für die Profilverwaltung: **Dateisystem > Synchronisierung > Profilcontainer - Liste der Ordner, die auf dem Profildatenträger enthalten sein sollen**.



Diese Liste muss alle o. g. Ordner enthalten. Alternativ können Sie diese Einstellungen mit Citrix Workspace Environment Management (WEM) konfigurieren.

4. Wenden Sie die Einstellungen auf die richtige Bereitstellungsgruppe an.
5. Melden Sie sich an, um die Bereitstellung zu überprüfen.

Systemanforderungen

Empfohlene Mindestversion: Delivery Controller 1906.2 (bei Verwendung einer früheren Version siehe Aktivieren der Optimierung für Microsoft Teams):

Unterstützte Betriebssysteme:

- Windows Server 2019, 2016, 2012R2 Standard und Datacenter Edition und mit der Server Core-Option

Mindestversion –VDA 1906.2:

Unterstützte Betriebssysteme:

- Windows 10 64-Bit, Versionen 1607 und höher. (VM-gehostete Anwendungen werden nicht unterstützt.)
- Windows Server 2019, 2016 und 2012 R2, Standard und Datacenter Edition

Anforderungen:

- BCR_x64.msi: Das MSI mit dem Microsoft Teams-Optimierungscode. Es startet automatisch von der GUI. Wenn Sie die Befehlszeilenschnittstelle für die VDA-Installation verwenden, schließen Sie es nicht aus.

Empfohlene Version –Citrix Workspace-App 2006.1 für Windows, Mindestversion –Citrix Workspace-App 1907 für Windows:

- Windows 7, 8 und 10, 32-Bit- und 64-Bit-Editionen (inkl. Embedded Edition)
- Windows 10 IoT Enterprise 2016 LTSB (v1607) und 2019 LTSC (v1809)
- Unterstützte Prozessorarchitekturen: x86 und x64 (ARM wird nicht unterstützt)
- Endpunkt: Dual-Core-CPU (ca. 2,2–2,4 GHz), die 720p-HD-Auflösung für Peer-to-Peer-Videokonferenzen unterstützt.
- Dual- oder Quad-Core-CPUs mit niedrigerem Basistakt (~1,5 GHz), ausgestattet mit Intel Turbo Boost oder AMD Turbo Core für eine Steigerung bis mindestens 2,4 GHz.
- HP Thin Clients-geprüft: t630/t640, t730/t740, mt44/mt45.
- Dell Thin Clients-geprüft: 5070, 5470 Mobile TC.
- 10ZiG Thin Clients-geprüft: 4510 und 5810q.
- Eine vollständige Liste aller geprüften Endpunkte finden Sie unter Thin Clients.
- Die Citrix Workspace-App benötigt mindestens 600 MB freien Speicherplatz und 1 GB RAM.
- Mindestanforderungen für Microsoft .NET Framework ist Version 4.6.2. Die Citrix Workspace-App lädt .NET Framework automatisch herunter und installiert es, wenn es nicht vorhanden ist.

Mindestversion —Citrix Workspace-App 2006 für Linux:

Weitere Informationen finden Sie unter Optimierung für Microsoft Teams in der Dokumentation zur Citrix Workspace-App für Linux.

Software:

- GStreamer 1.0 oder höher oder Cairo 2
- libc++-9.0 oder höher
- libgdk 3.22 oder höher
- OpenSSL 1.1.1d
- x64 Linux-Distribution

Hardware:

- Mindestens 1,8 GHz Dual-Core-CPU, die 720p HD-Auflösung während eines Peer-to-Peer-Videokonferenzanrufs unterstützen kann.
- Dual- oder Quad-Core-CPU mit einer Basisgeschwindigkeit von 1,8 GHz und einer hohen Intel Turbo Boost Geschwindigkeit von mindestens 2,9 GHz.

Weitere Informationen finden Sie unter Voraussetzungen für die Installation der Citrix Workspace-App.

Mindestversion –Citrix Workspace-App 2012 für Mac:

Unterstützte Betriebssysteme

- macOS Catalina (10.15)
- macOS Big Sur Beta 8 in test environments only. Nicht in Produktionsumgebungen verwenden.

Unterstützte Features:

- Audio
- Video
- Optimierung der Bildschirmfreigabe (eingehend und ausgehend)

Die Optimierung für Teams ist standardmäßig aktiviert, wenn der Benutzer die Citrix Workspace-App 2012 oder später und macOS 10.15 verwendet.

Um die Optimierung für Teams zu deaktivieren, führen Sie diesen Befehl im Terminal aus und starten die Workspace-App neu:

```
defaults write com.citrix.receiver.nomas mtopEnabled -bool NO
```

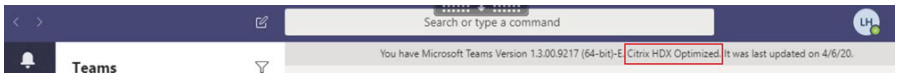
Aktivieren der Optimierung für Microsoft Teams

Verwenden Sie die unter Microsoft Teams-Umleitungsrichtlinie beschriebene Studio-Richtlinie (Standardeinstellung **Ein**), um die Optimierung für Microsoft Teams zu aktivieren. Zusätzlich zu der Aktivierung dieser Richtlinie überprüft HDX, ob die Version der Citrix Workspace-App der Mindestversion entspricht. Wenn Sie die Richtlinie aktiviert haben und die Version der Citrix Workspace-App unterstützt wird, wird **HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream\MSTeamsRedirSupport**

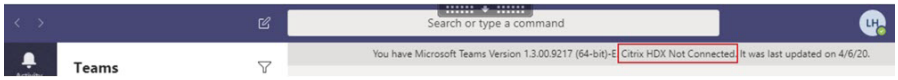
auf dem VDA automatisch auf **1** festgelegt. Microsoft Teams liest den Schlüssel zum Laden im VDI-Modus.

> **Hinweis:**
>
> Wenn Sie VDAs der Version 1906.2 oder höher mit älteren Controller-Versionen (z. B. Version 7.15) verwenden, für die die Richtlinie in Studio nicht verfügbar ist, ist die Optimierung immer noch möglich, da die HDX-Optimierung für Microsoft Teams standardmäßig im VDA aktiviert.

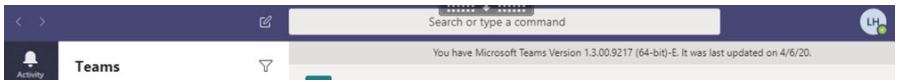
Wenn Sie auf **Info > Version** klicken, wird die Legende **Citrix HDX Optimized** angezeigt:



Wenn stattdessen **Citrix HDX Not Connected** angezeigt wird, wurde die Citrix API in Teams geladen (= erster Schritt zur Umleitung), doch in den nachfolgenden Teilen des Stacks ist ein Fehler aufgetreten. Der Fehler trat höchstwahrscheinlich in VDA-Diensten oder der Citrix Workspace App auf).



Wenn keine Legende angezeigt wird, konnte Teams die Citrix API nicht laden. Klicken Sie mit der rechten Maustaste auf das Symbol für den Infobereich, um Teams zu beenden und neu starten. Stellen Sie sicher, dass die Studio-Richtlinie nicht auf **Nicht zugelassen**festgelegt ist und dass die Citrix Workspace-App-Version unterstützt wird.



Netzwerkanforderungen

Microsoft Teams benötigt Medienprozessor-Server unter Office 365 für Besprechungen oder Anrufe mit mehreren Teilnehmern. Microsoft Teams benötigt Office 365-Transport-Relays für folgende Szenarios:

- Zwei Peers in einem Point-to-Point-Anruf ohne direkte Verbindung
- Ein Teilnehmer ohne direkte Verbindung zum Medienprozessor

Daher hängt die Anrufgüte von der Integrität des Netzwerks zwischen dem Peer und der Office 365-Cloud ab.

Wir empfehlen eine Analyse der Umgebung auf Risiken und Anforderungen bezüglich der gesamten Sprach- und Videobereitstellung über die Cloud.
Verwenden Sie das Skype for Business Network Assessment Tool, um zu testen, ob Ihr Netzwerk sich für Microsoft Teams eignet. Weitere Informationen zum Support finden Sie unter Support.

Zusammenfassung der wichtigsten Netzwerkempfehlungen für den Datenverkehr mit RTP (Realtime Transport Protocol):

- Stellen Sie von der Zweigstelle eine möglichst direkte Verbindung zum Office 365-Netzwerk her.
- Wenn Sie folgende Funktionen in der Zweigstelle verwenden, muss der RTP/UDP Teams-Verkehr ungehindert erfolgen. HdxTeams.exe berücksichtigt keine expliziten Proxys, die auf dem Endpunkt konfiguriert sind.
  - Proxyserver umgehen
  - Netzwerk-SSL abfangen
  - DPI-Geräte (Deep Packet Inspection)
  - VPN-Hairpins (nach Möglichkeit Split-Tunneling verwenden)
- Sie müssen ausreichend Bandbreite einplanen und bereitstellen.
- Überprüfen Sie Qualität und Konnektivität des Netzwerks für jede Zweigstelle.

Die WebRTC Media Engine in der Workspace-App (HdxTeams.exe) verwendet das Protokoll SRTP (Secure Real-Time Transport Protocol) für Multimediastreams, die an den Client ausgelagert werden. SRTP bietet Vertraulichkeit und Authentifizierung für RTP. Es verwendet symmetrische Schlüssel (128 Bit) zum Verschlüsseln von Medien und Steuerungsmeldungen und nutzt die AES-Verschlüsselung im Counter Modus.

Folgende Metriken werden für eine positive Benutzererfahrung empfohlen:

Metrik	Endpunkt zu Office 365
Latenz (ein Weg)	< 50 ms
Latenz (RTT)	< 100 ms
Paketverlust	< 1 % während eines Intervalls von 15 s
Paket-Interarrival-Jitter	<30 ms während eines Intervalls von 15 s

Weitere Informationen finden Sie unter Vorbereiten des Netzwerks für Microsoft Teams.

Bezüglich Bandbreitenanforderungen kann die Optimierung für Microsoft Teams eine Vielzahl von Codecs für Audio (OPUS/G.722/PCM G711) und Video (H264/VP9) verwenden.

Die Peers handeln diese Codecs während der Einrichtung des Anrufs über SDP (Session Description Protocol) aus.
Mindestempfehlungen von Citrix pro Benutzer:

Typ	Bandbreite	Codec
Audio (bidirektional)	~ 90 KBit/s	G.722
Audio (bidirektional)	~ 60 KBit/s	Opus*
Video (bidirektional)	~ 700 KBit/s	H264 360p bei 30 F/s 16:9
Video (bidirektional)	~ 2,500 KBit/s	VP9 720p bei 30 F/s 16:9
Bildschirmfreigabe	~ 300 KBit/s	H264 1080p bei 15 F/s

* Opus unterstützt die Codierung mit konstanter und variabler Bitrate von 6 KBit/s bis 510 KBit/s.

Opus und VP9 sind die bevorzugten Codecs für Peer-to-Peer-Anrufe zwischen zwei optimierten VDI-Benutzern.

G.722 und H264 sind die bevorzugten Codecs für einen VDI-Benutzer, der einer Besprechung beitritt.

Citrix Gateway

Das Vorhandensein von on-premises Citrix Gateway oder Citrix Gateway Service als HDX-Proxy hat keine Auswirkungen auf die Optimierung von Microsoft Teams. Dies liegt daran, dass zwischen der Workspace-App und dem VDA nur ein virtueller Command-and-Control-Kanal eingerichtet ist.

Alle Audio- oder Videostreams werden an den Client zur lokalen Verarbeitung ausgelagert. Daher gibt es kein serverseitiges Rendern.

Abhängig von der Konfiguration in Ihrer Umgebung fließt der virtuelle Command-and-Control-Kanal über einer der folgenden Optionen durch das Citrix Gateway:

- TLS für TCP
- DTLS für EDT

Wenn Sie auch Citrix Gateway für VPN verwenden, muss die Clientmaschine die O365 Microsoft Teams-Server direkt erreichen können. Sie erreichen dies durch Split-Tunneling oder andere Methoden.

Proxyserver

Berücksichtigen Sie je nach Standort des Proxys Folgendes:

- Proxykonfiguration auf dem VDA:

  Wenn Sie einen expliziten Proxyserver im VDA konfigurieren und Verbindungen über einen Proxy an localhost weiterleiten, schlägt die Umleitung fehl. Um den Proxy richtig zu konfigurieren,

müssen Sie die Einstellung **Proxyserver für lokale Adressen umgehen** unter **Internetoptionen > Verbindungen > LAN-Einstellungen > Proxyserver** auswählen und sicherstellen, dass `127.0.0.1:9002` umgangen wird.

Wenn Sie eine PAC-Datei verwenden, muss Ihr VDA-Proxykonfigurationsskript aus der PAC-Datei **DIRECT** für `wss://127.0.0.1:9002` zurückgeben. Wenn nicht, schlägt die Optimierung fehl. Um sicherzustellen, dass das Skript **DIRECT**zurückgibt, verwenden Sie `shExpMatch(url, "wss://127.0.0.1:9002/*")`.

- Proxykonfiguration in der Citrix Workspace-App:

  Wenn eine Zweigstelle für den Zugriff auf das Internet ein Proxy verwendet, unterstützen Citrix Workspace-App für Windows Version 2012 (Negotiate/Kerberos, NTLM, Basic und Digest), Citrix Workspace-App für Linux Version 2101 (anonyme Authentifizierung) und Citrix Workspace-App für Mac Version 2104 (anonyme Authentifizierung) Proxyserver. Clientgeräte mit früheren Versionen der Citrix Workspace-App können keine Proxykonfigurationen lesen. Diese Geräte senden Datenverkehr direkt an Office 365 TURN-Server.

  > **Wichtig:**
  >
  > Stellen Sie sicher, dass das Clientgerät für die DNS-Auflösung eine Verbindung zum DNS-Server herstellen kann. Ein Clientgerät muss drei FQDNs des Microsoft Teams TURN-Servers auflösen können: `worldaz.turn.teams.microsoft.com`, `usaz.turn.teams.microsoft.com` und `euaz.turn.teams.microsoft.com`.

Anrufeinrichtung und Medienflusspfad

Wenn möglich, versucht die HDX Media Engine in der Citrix Workspace-App (HdxTeams.exe), eine direkte Netzwerkverbindung mit SRTP über UDP in einem Peer-to-Peer-Anruf herzustellen. Wenn die UDP-Ports blockiert sind, fällt die Media Engine auf TCP 443 zurück.

Die HDX Media Engine unterstützt ICE, STUN (Session Traversal Utilities for NAT) und TURN (Traversal Using Relays around NAT) für die Kandidatendiscovery und den Verbindungsaufbau.

Wenn der Benutzer einem Anruf oder einer Besprechung mit mehreren Teilnehmern beitritt und kein direkter Pfad zwischen zwei Peers oder zwischen einem Peer und einem Konferenzserver vorliegt, verwendet HdxTeams.exe einen Transport-Relay-Server von Microsoft Teams in Office 365, um den anderen Peer oder den Medienprozessor (den Host der Besprechung) zu erreichen. Der Clientcomputer des Benutzers muss auf zwei Office 365-Subnetz-IP-Adressbereiche und 4 UDP-Ports zugreifen können. Weitere Informationen finden Sie im Architekturdiagramm unter “Call Setup”sowie Office 365 URLs and IP address ranges ID 11.

ID	Kategorie	Adressen	Zielports
11	Optimieren erforderlich	13.107.64.0/18, 52.112.0.0/14, 52.120.0.0/14	**UDP:** 3478, 3479, 3480, 3481, **TCP:** 443 (Fallback)

Diese Bereiche enthalten Transport-Relays und Medienprozessoren.
Teams Transport-Relays bieten die Funktionen STUN und TURN, sie sind aber keine ICE-Endpunkte. Teams Transport-Relays beenden auch keine Medien und führen keine Transcodierung durch. Relays können als Bridge zwischen TCP (wenn HdxTeams.exe TCP verwendet) und UDP fungieren, wenn sie den Datenverkehr an andere Peers oder Medienprozessoren weiterleiten.

HdxTeams.exe kontaktiert das nächstgelegene Microsoft Teams Transport-Relay in der Office 365-Cloud. HdxTeams.exe verwendet Anycast-IP und Port 3478-3481 UDP (verschiedene UDP-Ports pro Workload, wobei Multiplexing möglich ist) oder 443 TCP TLSv1.2 für Fallbacks. Die Anrufqualität hängt vom zugrunde liegenden Netzwerkprotokoll ab. Da UDP über TCP immer empfehlenswert ist, sollten Sie Ihre Netzwerke so gestalten, dass UDP-Datenverkehr in der Zweigstelle möglich ist.

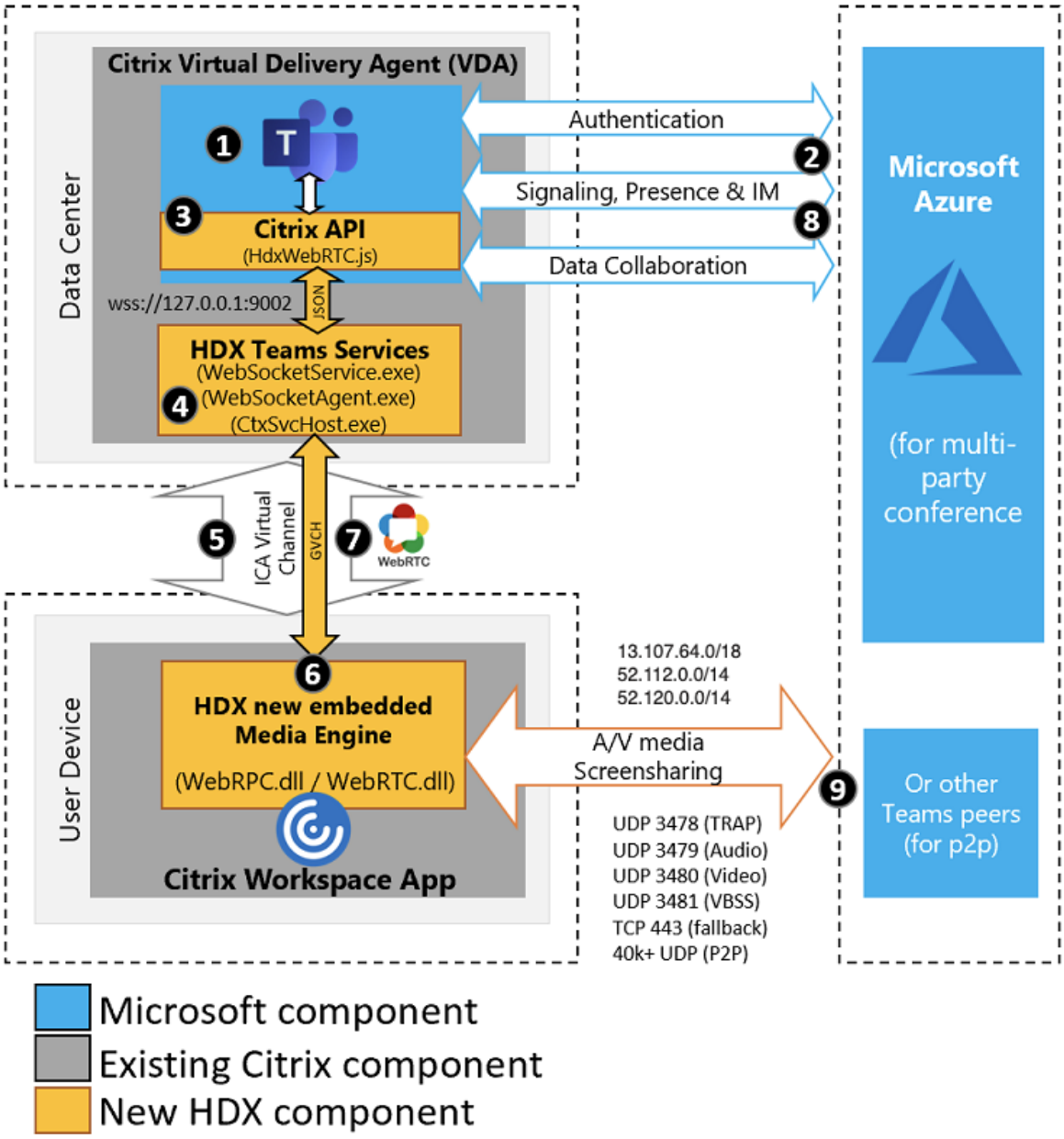
Wenn Teams im optimierten Modus geladen ist und HdxTeams.exe auf dem Endpunkt ausgeführt wird, können ICE-Fehler (Interactive Connectivity Establishment) zum Fehlschlagen des Anrufs oder zu einseitigem Audio/Video führen. Wenn ein Anruf nicht zustande kommt oder der Medienfluss keinen vollen Duplexmodus bietet, sollten Sie zuerst die **Wireshark-Trace** auf dem Endpunkt prüfen.

> **Hinweis:**
>
> Wenn die Endpunkte keinen Internetzugang haben, können Benutzer unter Umständen dennoch einen Peer-to-Peer-Anruf tätigen, wenn sie sich in demselben LAN befinden. Besprechungen schlagen fehl. In diesem Fall gibt es ein Timeout von 30 Sekunden, bevor der Anruf eingerichtet wird.

Einrichten von Anrufen

Dieses Architekturdiagramm dient als visuelle Referenz für die Flusssequenz bei einem Anruf. Die entsprechenden Schritte sind im Diagramm angegeben.

Architektur:



1. Starten Sie Microsoft Teams.
2. Teams authentifiziert sich bei O365. Mandantenrichtlinien werden an den Teams-Client übertragen, und relevante TURN- und Signalkanalinformationen werden an die App weitergeleitet.
3. Teams erkennt, dass es in einem VDA ausgeführt wird, und sendet API-Aufrufe an die Citrix JavaScript-API.
4. Citrix JavaScript in Teams öffnet eine sichere WebSocket-Verbindung zu WebSocketService.exe, das auf dem VDA (127.0.0.1:9002) ausgeführt wird. Dies generiert WebSocketAgent.exe in der Benutzersitzung.
5. WebSocketAgent.exe instanziiert einen generischen virtuellen Kanal, indem es den Citrix HDX-

Teams-Umleitungsdienst (CtxSvcHost.exe) aufruft.

6. Die HDX-Engine der Citrix Workspace-App (wfica32.exe) erzeugt einen neuen Prozess namens HdxTeams.exe. Dies ist die neue WebRTC-Engine, die für die Teamoptimierung verwendet wird.
7. HdxTeams.exe und Teams.exe verfügen über einen 2-Wege-Pfad für virtuelle Kanäle und beginnen mit der Verarbeitung von Multimediaanfragen.

   ——Benutzeranrufe——

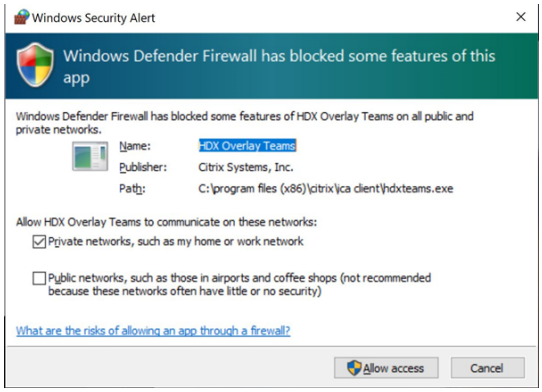
8. **Peer A** klickt auf die **Anruftaste**. Teams.exe kommuniziert mit den Teams-Diensten in Office 365, die einen End-to-End-Signalpfad mit **Peer B** einrichten. Teams schickt eine Anfrage an HdxTeams zu diversen unterstützten Anrufparametern (Codecs, Auflösungen usw.). Dies wird auch als Angebot des Protokolls SDP (Session Description Protocol) bezeichnet. Die Anrufparameter werden dann über den Signalpfad an die Teams-Dienste in Office 365 und von dort an den anderen Peer weitergeleitet.
9. SDP-Angebot/Antwort (Single-Pass-Verfahren) erfolgt über den Signalkanal, und die ICE-Konnektivitätsprüfungen werden abgeschlossen (Netzwerkadressübersetzung und Firewalldurchquerung durch Bindungsanfragen für STUN (Session Traversal Utilities for NAT)). Anschließend erfolgt der Medienfluss per SRTP (Secure Real-Time Transport Protocol) direkt zwischen HdxTeams.exe und dem anderen Peer (oder Office 365-Konferenzservern im Falle einer Besprechung).

Microsoft-Telefonsystem

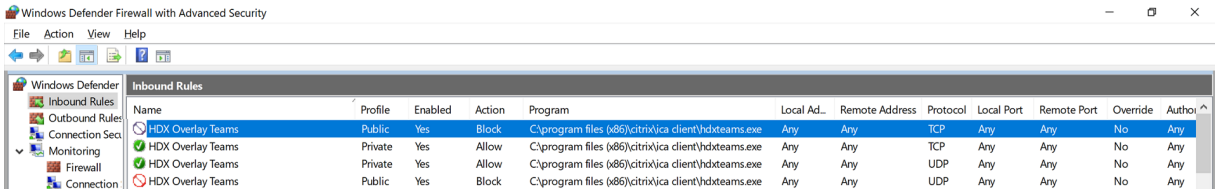
Das Microsoft-Telefonsystem aktiviert die Anrufsteuerung und PBX-Funktionen in der Office 365-Cloud mit Microsoft Teams. Die Optimierung für Microsoft Teams unterstützt Microsoft Phone System mithilfe von Office 365-Anrufplänen oder Direct Routing. Beim direktem Routing können Sie jeden unterstützten Session Border Controller (SBC) ohne zusätzliche On-Premises-Software mit Microsoft Phone System verbinden.

Überlegungen zu Firewalls

Wenn Benutzer zum ersten Mal einen optimierten Anruf mit dem Microsoft Teams-Client initiieren, wird möglicherweise eine Warnung mit den **Windows-Firewalleinstellungen** angezeigt. In der Warnung werden Benutzer aufgefordert, die Kommunikation für HdxTeams.exe (HDX Overlay Teams) zuzulassen.



Die folgenden vier Einträge werden unter **Eingehende Regeln** in der Konsole **Windows Defender Firewall > Erweiterte Sicherheit** hinzugefügt. Sie können auf Wunsch restriktivere Regeln anwenden.

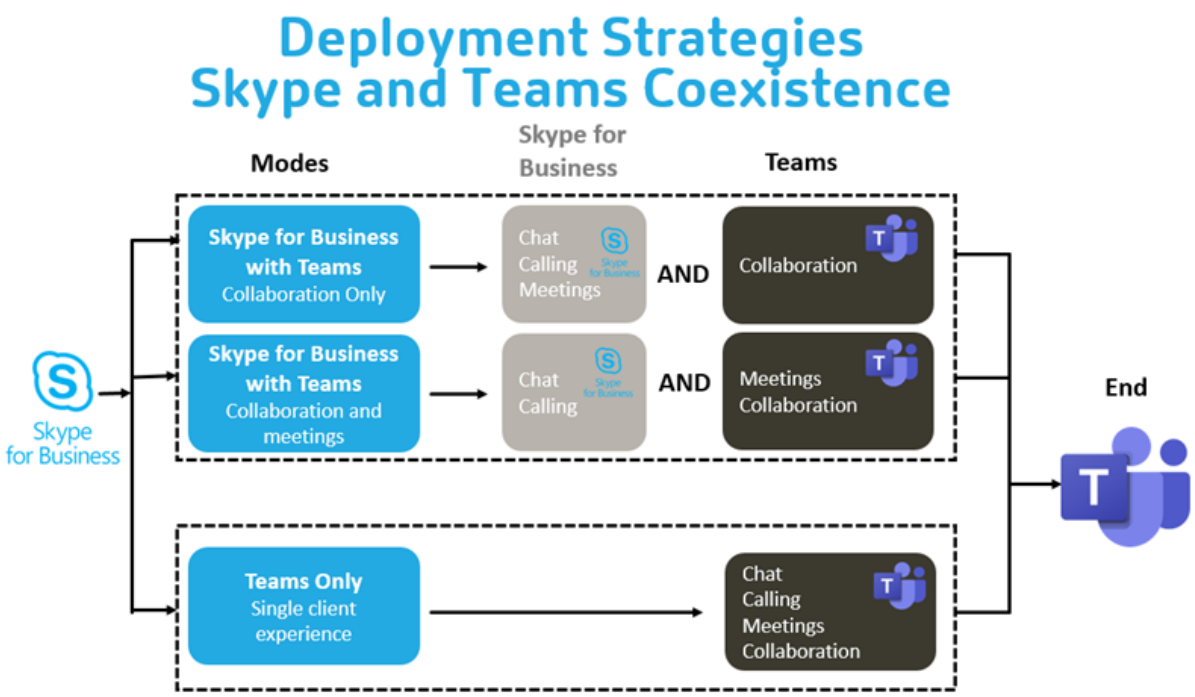


Koexistenz von Microsoft Teams und Skype for Business

Sie können Microsoft Teams und Skype for Business nebeneinander als separate Lösungen mit Funktionsüberschneidungen bereitstellen. Weitere Informationen finden Sie unter Hinweise zur Koexistenz und Interoperabilität von Microsoft Teams und Skype for Business.

Die Multimedia-Engines Citrix RealTime Optimization Pack und HDX-Optimierung für Teams setzen dann die Konfiguration um, die in Ihrer Umgebung eingerichtet ist (z. B. Islands Mode, Skype for Business & Teams Collaboration, Skype for Business & Teams Collaboration and Meetings).

Zugriff auf Peripheriegeräte kann jeweils nur einer Anwendung gleichzeitig gewährt werden. Wenn beispielsweise die RealTime Media Engine bei einem Anruf auf die Webcam zugreift, wird dadurch das Imaginggerät während des Anrufs gesperrt. Wenn das Gerät freigegeben wird, steht es für Teams zur Verfügung.



Citrix SD-WAN: optimierte Netzwerkkonnektivität für Microsoft Teams

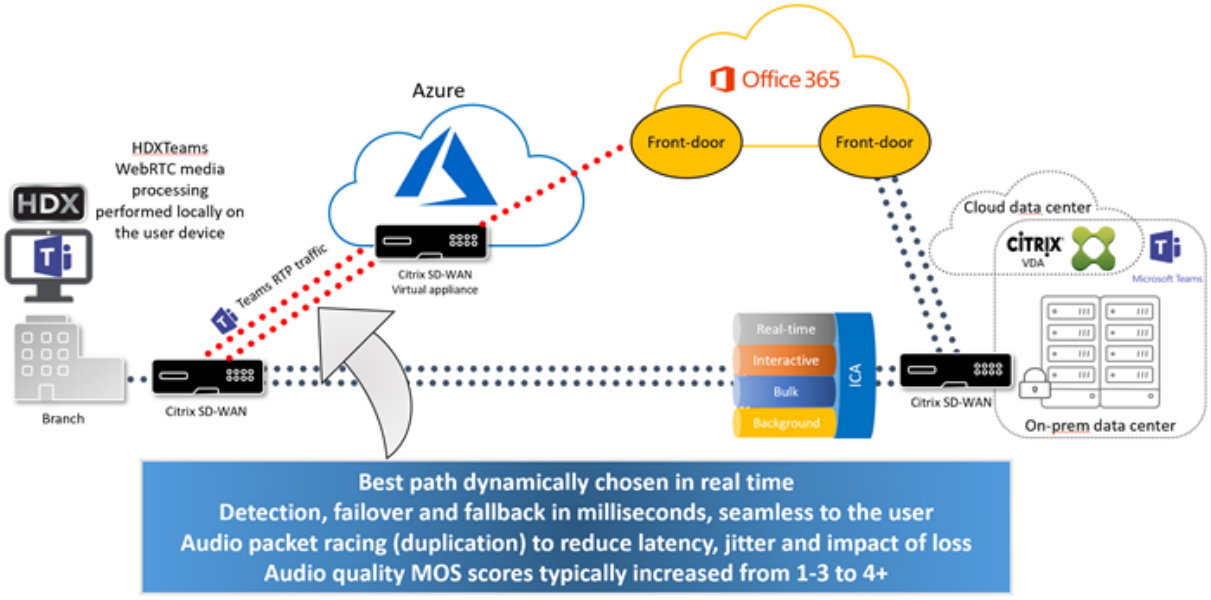
Eine optimale Audio- und Videoqualität erfordert eine Netzwerkverbindung zur Office 365-Cloud mit geringer Latenz, wenig Jitter und geringem Paketverlust. Wenn Citrix Workspace App-Benutzer in Zweigstellen für den Microsoft Teams-RTP-Datenverkehr (Audio/Video) einen Backhaul zum Datencenter benötigen, bevor sie ins Internet gehen, kann dies zu übermäßiger Latenz und zur Überlastung von WAN-Verbindungen führen. Citrix SD-WAN optimiert die Konnektivität für Microsoft Teams gemäß den Netzwerkverbindungsprinzipien für Microsoft Office 365. Citrix SD-WAN verwendet die Microsoft REST-basierte Office 365-IP-Adresse samt Webdienst und naheliegender DNS, um den Microsoft Teams-Datenverkehr zu identifizieren, zu kategorisieren und zu steuern.

Breitband-Internetverbindungen von Unternehmen verzeichnen immer wieder Paketverluste, exzessiven Jitter und Ausfälle.

Citrix SD-WAN bietet zwei Lösungen, um die Audio-/Videoqualität in Microsoft Teams auch bei variabler oder verschlechterter Netzwerkintegrität zu erhalten.

- Wenn Sie Microsoft Azure verwenden, bietet ein in Azure VNET bereitgestelltes virtuelles Gerät (Citrix SD-WAN-VPX) erweiterte Möglichkeiten zur Konnektivitätsoptimierung. Dazu gehören ein Seamless-Link-Failover und “Packet Racing”für Audiopakete.
- Alternativ können Citrix SD-WAN-Kunden sich über Citrix Cloud Direct Service mit Office 365 verbinden. Dieser Dienst bietet eine zuverlässige und sichere Bereitstellung für den gesamten Datenverkehr ins Internet.

Bei guter Qualität der Internetverbindung der Zweigstelle reicht es möglicherweise aus, die Latenz zu minimieren, indem der Microsoft Teams-Datenverkehr direkt vom Citrix SD-WAN-Zweigstellengerät zur nächstgelegenen Office 365-Frontdoor geleitet wird. Weitere Informationen finden Sie unter Citrix SD-WAN Office 365-Optimierung.



Katalogansicht und aktive Sprecher in Microsoft Teams

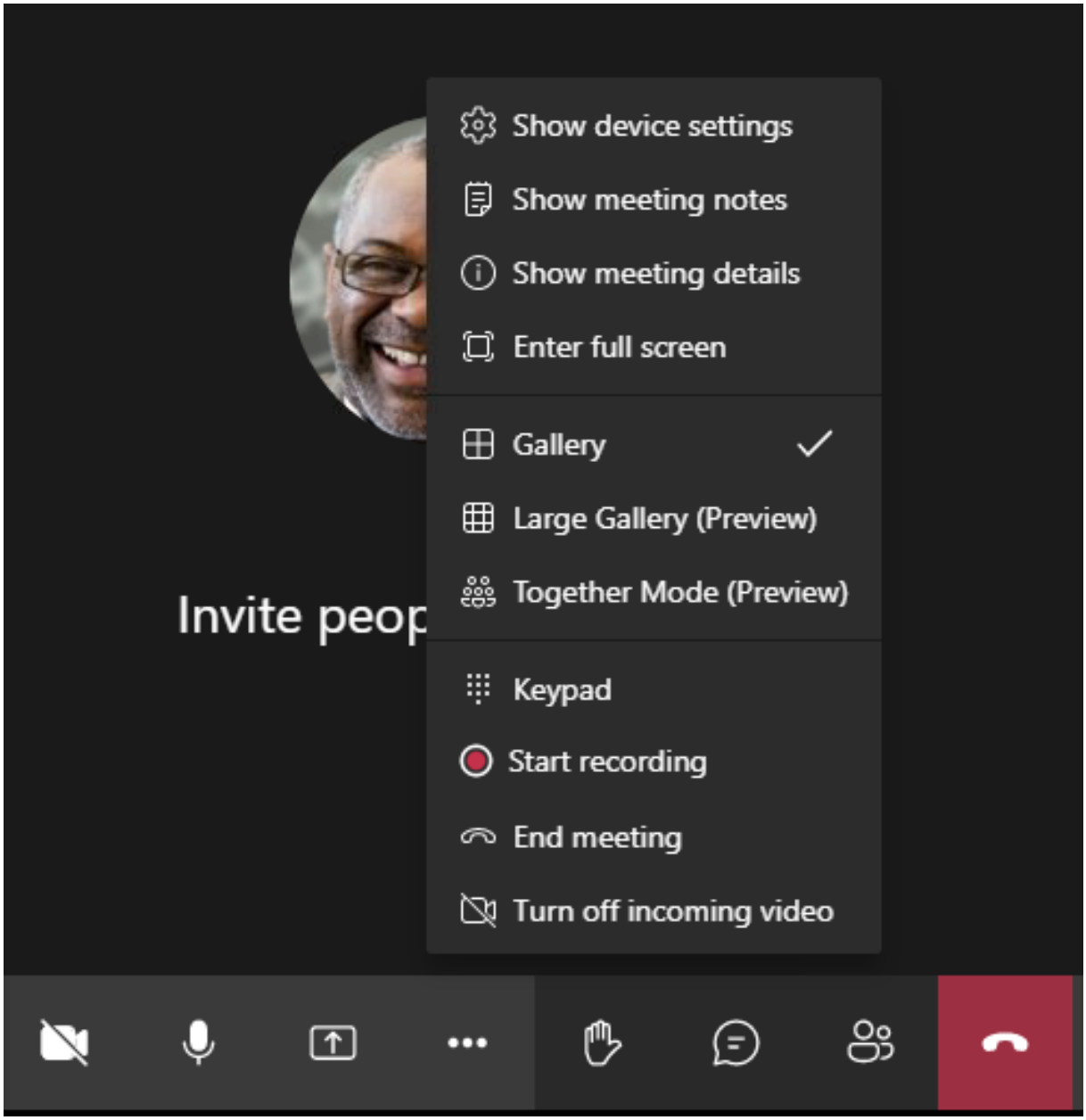
Microsoft Teams unterstützt Layouts **Gallery**, **Large gallery** und **Together mode**.

In Microsoft Teams wird ein 2x2-Raster mit Videostreams von vier Teilnehmern angezeigt (= Gallery). In diesem Modus sendet Teams vier Videostreams zur Decodierung an das Clientgerät. Bei mehr als vier Teilnehmern werden nur die letzten vier aktivsten Sprecher auf dem Bildschirm angezeigt.

Microsoft Teams bietet auch die Ansicht "Large Gallery"mit einem Raster bis zu 7x7. Der Teams-Konferenzserver stellt dann einen einzigen Videofeed zusammen und sendet ihn zur Decodierung an das Clientgerät, was zu einem geringeren CPU-Verbrauch führt. Dieser "Hollywood square"-Feed kann auch das Eigenvorschauvideo des Benutzers enthalten.

Microsoft Teams unterstützt auch den Together-Modus als Teil der neuen Benutzeroberfläche "New Meeting Experience". Mithilfe von KI-Segmentierungstechnologie zur digitalen Platzierung der Teilnehmer auf einen gemeinsamen Hintergrund werden alle Teilnehmer in dasselbe Auditorium platziert.

Diese Modi können während einer Telefonkonferenz über die Optionen **Gallery**, **Large Gallery** und **Together mode** im Menü (…) auswählt werden.



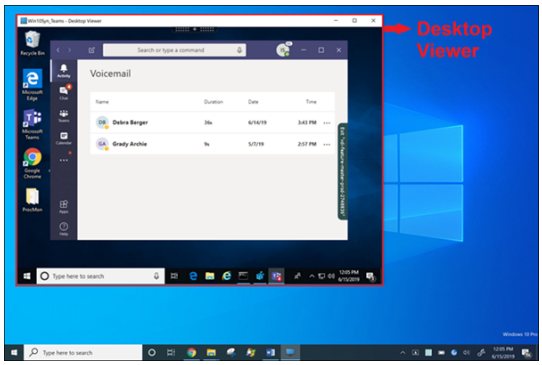
Bildschirmfreigabe in Microsoft Teams

Microsoft Teams verwendet die videobasierte Bildschirmfreigabe (VBSS), um den freigegebenen Desktop mit Videocodecs wie H264 zu codieren und einen High-Definition-Stream zu erstellen. Bei der HDX-Optimierung wird die eingehende Bildschirmfreigabe als Videostream behandelt. Wenn Sie also in einem Videoanrufs sind und der andere Peer beginnt, den Desktop freizugeben, wird der Videofeed der ursprünglichen Kamera angehalten. Stattdessen wird der Videofeed für die Bildschirmfreigabe angezeigt. Der Peer muss die Kamerafreigabe dann manuell fortsetzen.

Die ausgehende Bildschirmfreigabe ist ebenfalls optimiert und in die Citrix Workspace-App (Version

1907 oder höher) ausgelagert. In diesem Fall erfasst und überträgt HdxTeams.exe nur das Fenster des Citrix Desktop Viewer (CDViewer.exe). Wenn Sie eine lokale Anwendung freigeben möchten, die auf Ihrem Clientcomputer ausgeführt wird, können Sie sie über CDViewer legen, und sie wird ebenfalls erfasst.

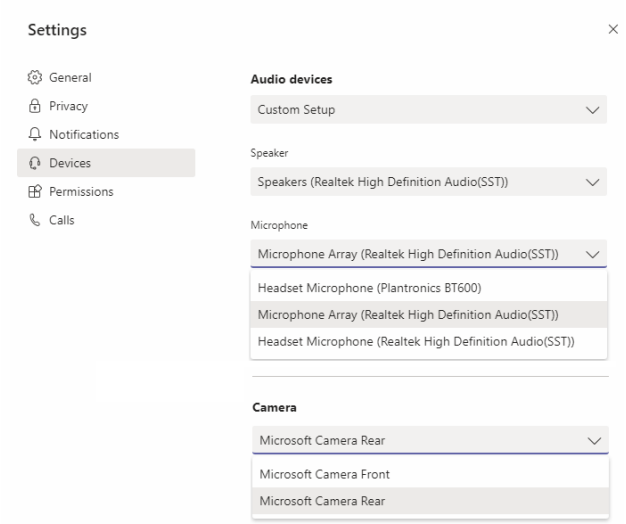
Multimonitoranzeige: Wenn CDViewer im Vollbildmodus ausgeführt wird und die Anzeige sich über mehrere Monitore erstreckt, wird nur der primäre Monitor freigegeben. Benutzer müssen die gewünschte Anwendung im virtuellen Desktops auf den primären Monitor ziehen, damit der andere Gesprächsteilnehmer sie sehen kann.



> **Hinweis:**
>
> Wenn Sie Teams als eigenständige Seamlessanwendung veröffentlichen, erfasst die Bildschirmfreigabe den lokalen Desktop Ihres physischen Endpunkts in der Citrix Workspace-App (ab Version 1909).

Peripheriegeräte in Microsoft Teams

Wenn die Optimierung für Microsoft Teams aktiv ist, greift die Citrix Workspace-App auf die Peripheriegeräte (Headset, Mikrofon, Kameras, Lautsprecher usw.) zu. Anschließend werden die Peripheriegeräte ordnungsgemäß in der Benutzeroberfläche von Microsoft Teams (**Einstellungen > Geräte**) enumeriert.



Microsoft Teams greift nicht direkt auf die Geräte zu. Stattdessen verwendet es HdxTeams.exe, um die Medien zu erfassen, aufzuzeichnen und zu verarbeiten. Microsoft Teams listet die Geräte auf, die der Benutzer auswählen kann.

Empfehlungen:

- Microsoft Teams-zertifizierte Headsets mit integrierter Echounterdrückung. Bei Konfigurationen mit mehreren Peripheriegeräten, bei denen sich Mikrofon und Lautsprecher in separaten Geräten befinden, kann es zu einem Echo kommen. Dies können zum Beispiel eine Webcam mit integriertem Mikrofon und ein Bildschirm mit Lautsprechern sein. Wenn Sie externe Lautsprecher verwenden, stellen Sie sie so weit wie möglich entfernt vom Mikrofon und von jeder Oberfläche, die den Ton auf das Mikrofon lenken könnte, auf.
- Microsoft Teams-zertifizierte Kameras, obwohl für Skype for Business zertifizierte Peripheriegeräte mit Microsoft Teams kompatibel sind.
- Eine Entlastung des Hauptprozessors durch Onboard-H.264-Codierung der Webcams (UVC 1.1 und 1.5) kann HdxTeams.exe nicht nutzen.

> **Hinweis:**
>
> HdxTeams.exe unterstützt nur diese spezifischen Audiogeräteformate (Kanäle, Bit-Tiefe und Abtastrate):
>
> - Wiedergabegeräte: bis zu 2 Kanäle, 16 Bit, Frequenzen bis 96000 Hz
> - Aufnahmegeräte: bis zu 4 Kanäle, 16 Bit, Frequenzen bis 96000 Hz
>
> Wenn ein Lautsprecher oder Mikrofon nicht mit den erwarteten Einstellungen übereinstimmt, schlägt die Geräteaufzählung in Teams fehl und unter **Einstellungen > Geräte** wird **Keine** angezeigt.
>
> **Webrpc**-Protokolle in **HdxTeams.exe** enthalten folgende Art von Informationen:


```
Mar 27 20:58:22.885 webrtcapi.WebRTCEngine Info: init. initializing
...
Mar 27 20:58:23.190 webrtcapi.WebRTCEngine Error: init. couldn't
create audio module!
```

Um dieses Problem zu umgehen, öffnen Sie in der Systemsteuerung die Option **Sound** (mmsys.cpl), wählen das Wiedergabe- oder Aufnahmegerät, gehen zu **Eigenschaften > Erweitert** und wählen einen unterstützten Modus. Alternativ können Sie das spezifische Gerät auch deaktivieren.

Fallbackmodus

Wenn Microsoft Teams nicht im optimierten VDI-Modus geladen werden kann, fällt der VDA ältere HDX-Technologien wie Webcamumleitung und Clientaudio/-mikrofonumleitung zurück. Im nicht optimierten Modus werden die Peripheriegeräte dem VDA zugeordnet. Die Peripheriegeräte werden in der Microsoft Teams-App so angezeigt, als wären sie lokal an den virtuellen Desktop angeschlossen.

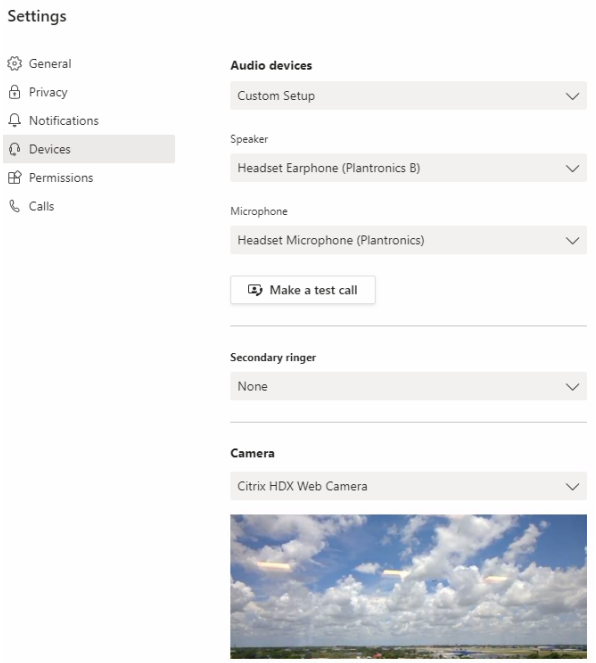
Sie können jetzt den Fallbackmechanismus granular steuern, indem Sie einen der folgenden DWORD-Registrierungswerte im VDA festlegen:

HKLM\SOFTWARE\Microsoft\Teams\DisableFallback

HKCU\SOFTWARE\Microsoft\Office\Teams\DisableFallback

Um den Fallbackmodus zu deaktivieren, setzen Sie den Wert auf 1. Um nur Audio zu aktivieren, setzen Sie den Wert auf 2. Wenn der Wert nicht vorhanden oder auf 0 gesetzt ist, wird der Fallbackmodus aktiviert. Für diese Funktion ist die Teams-Version 1.3.0.13565 oder höher erforderlich.

Um festzustellen, ob Sie im optimierten oder nicht optimierten Modus sind, ist der größte Unterschied der Kameraname in Teams auf der Registerkarte **Einstellungen > Geräte**. Wenn Microsoft Teams im nicht optimierten Modus geladen werden, starten ältere HDX-Technologien. Der Webcam-Name hat das Suffix **Citrix HDX**, wie in der folgenden Grafik dargestellt. Die Lautsprecher- und Mikrofongerätenamen können sich geringfügig vom optimierten Modus unterscheiden (oder gekürzt angezeigt werden).



Wenn ältere HDX-Technologien verwendet werden, werden die Audio-, Video- und Bildschirmfreigabeverarbeitung von Microsoft Teams nicht auf die WebRTC Media Engine der Citrix Workspace-App des Endpunkts übertragen. Stattdessen verwenden HDX-Technologien serverseitiges Rendering. Erwarten Sie einen hohen CPU-Verbrauch auf dem VDA, wenn Sie Video einschalten. Die Echtzeitaudioleistung ist möglicherweise nicht optimal.

Bekannte Einschränkungen

Citrix Einschränkungen

Einschränkungen bei der Citrix Workspace-App:

- DTMF-Töne werden nicht unterstützt.
- HID-Schaltflächen - “Antworten”und “Anruf beenden”werden nicht unterstützt. Der Lautstärkeregler (lauter/leiser) wird unterstützt.
- Bei einer Bildschirmfreigabe im Multimonitormodus wird nur der Hauptmonitor freigegeben.
- Es wird nur ein Videostream unterstützt, von einer eingehenden Kamera oder einer Bildschirmfreigabe. Bei eingehender Bildschirmfreigabe wird die Bildschirmfreigabe anstelle des Videos des aktiven Sprechers angezeigt.
- Sekundärer Klingelton (**Teams > Einstellungen > Geräte**) wird nicht unterstützt
- QoS-Einstellungen im Microsoft Teams Admin Center gelten nicht für VDI-Benutzer.
- App-Schutz-Add-On für die Citrix Workspace-App verhindert ausgehende Bildschirmfreigabe.
- Die Zoomfunktion in Teams wird nicht unterstützt.

Beschränkung auf dem VDA:

- Wenn Sie die Einstellung "Hoher DPI-Wert"der Citrix Workspace-App auf **Ja** oder auf **Nein, native Auflösung verwenden** konfigurieren, scheint das umgeleitete Videofenster am falschen Ort zu sein, wenn der DPI-Skalierungsfaktor des Monitors auf einen Wert über 100 % festgelegt ist.

Einschränkungen bei Citrix Workspace-App und VDA:

- Ausgehende Bildschirmfreigabe: Das Freigeben einer Anwendung wird nicht unterstützt.
- Sie können die Lautstärke bei optimierten Anrufen nur über die Lautstärkeleiste auf dem Client steuern, nicht über die auf dem VDA.

Microsoft-Einschränkungen

- Die Optionen zum Verwischen oder Anpassen des Hintergrunds werden nicht unterstützt.
- Eine 3x3-Galerieansicht wird nicht unterstützt. Teams-Abhängigkeit –wenden Sie sich an Microsoft, wann ein 3x3-Raster erwartet wird
- Die Interoperabilität mit Skype for Business beschränkt sich auf Audioanrufe (kein Videomodus).
- Die maximale Auflösung für eingehende und ausgehende Videostreams beträgt 720 p. Teams-Abhängigkeit –wenden Sie sich an Microsoft, wann 1080p erwartet wird
- PSTN-Freizeichen wird nicht unterstützt.
- Medienumgehung für Direct Routing wird nicht unterstützt.

Citrix und Microsoft-Einschränkungen

- Bei der Bildschirmfreigabe ist die Option **Systemaudio einschließen** nicht verfügbar.
- Pop-out-Chat (auch "Multi-Window-Chat"oder "New Meeting Experience") wird nicht unterstützt.
- Separate Räume werden für VDI-Teilnehmer unterstützt. Teams unterstützt keine separaten Räume, wenn der Organisator ein VDI-Benutzer ist.
- Steuerung übergeben und Steuerung übernehmen: Wird in Sitzungen mit Desktop-Bildschirmfreigabe oder Anwendungsfreigabe nicht unterstützt. Wird nur in Sitzungen mit PowerPoint-Freigabe unterstützt.
- E911 und Location-Based Routing werden nicht unterstützt.

Angekündigtes EOL für Einzelfenster in Microsoft Teams

Microsoft unterstützt ab 31.01.2024 nur noch den Mehrfenstermodus bei Verwendung von optimiertem Microsoft Teams für VDI. Die Unterstützung der Einzelfenster-Benutzeroberfläche wird eingestellt. Dies wurde am 08.09.2023 im M365s Admin Center (Post-ID: MC674419) von Microsoft

bekannt gegeben.
Informationen zum Mehrfensterfeature sind in diesem Tech Community-Artikel veröffentlicht: New Meeting and Calling Experience in Microsoft Teams.

Sie müssen Ihren VDA und die Citrix Workspace-App auf die unterstützten Versionen aktualisieren, um Microsoft Teams weiterhin im optimierten Modus für Videoanrufe und die Bildschirmfreigabe zu verwenden. Wenn Sie Ihre Infrastruktur und Endpunkte nicht so aufrüsten, dass sie mehrere Fenster unterstützen, können Sie nur Audioanrufe einrichten. Sie können die optimierte Video- und Bildschirmfreigabefunktion dann nicht verwenden.

Die folgende Tabelle enthält die erforderliche Mindest-, LTSR- und empfohlene Version von VDA und Citrix Workspace-App, um weiterhin optimierte Anrufe in Microsoft Teams auf Citrix VDI zu verwenden:

Komponente	Mindestversion	Version für LTSR	Empfohlene Version
Microsoft Teams	1.5.00.11865	Nicht zutreffend	Aktuell
VDA	1912 CU6 LTSR, 2112 CR	1912 CU7+, 2203 CU2+	2308 CR+
Citrix Workspace-App für Windows	2205 CR	2203 CU2+	2309 CR+
Citrix Workspace-App für Mac	2209 CR	Nicht zutreffend	2308 CR+
Citrix Workspace-App für Linux	2209 CR	Nicht zutreffend	2308 CR+
Citrix Workspace-App für ChromeOS oder HTML5	2303 CR	Nicht zutreffend	2309 CR+

Angekündigte Einstellung des SDP-Formats (Plan B) von WebRTC

Das aktuelle SDP-Format (Plan B) von WebRTC wird in zukünftigen Versionen nicht mehr von Citrix unterstützt. Sie müssen Unified Plan in WebRTC verwenden, um optimierte Microsoft Teams-Funktionen zu unterstützen.

Betroffene Produkte

In einem zukünftigen Release der Citrix Workspace-App werden Anrufe zwischen Endpunkten mit dem kommenden Release der Citrix Workspace-App und Endpunkten mit der Citrix Workspace-App bis Version 2108 nicht unterstützt. Diese Anrufinkompatibilität umfasst Clients mit der Citrix Workspace-App (CWA) 1912 LTSR. Die folgenden CWA-Clients sind betroffen:

- Citrix Workspace-App für Windows
- Citrix Workspace-App für Linux
- Citrix Workspace-App für Mac
- Citrix Workspace-App für Chrome

Ersatz für Plan B

Bei Verwendung der Citrix Workspace-App vor Version 2109 müssen Sie ein Upgrade auf eine unterstützte Version durchführen (vorzugsweise das neueste CR-Release). Andernfalls können alle Anrufe mit einem zukünftigen Release oder neueren Endpunkten fehlschlagen. Anrufe zwischen zukünftigen Releases und Ihren Verbundkommunikationspartnern können ebenfalls fehlschlagen, wenn der Citrix Workspace Ihrer Verbundpartner nicht aktualisiert wurde.

Version 2108 der Citrix Workspace-App wird seit März 2023 nicht mehr unterstützt und muss auf eine neuere Version aktualisiert werden. Weitere Informationen zu unterstützten Versionen der Citrix Workspace-App finden Sie unter Workspace-App.

Weitere Informationen zur eingestellten Unterstützung für Plan B finden Sie in der Dokumentation zu WebRTC.

Weitere Informationen

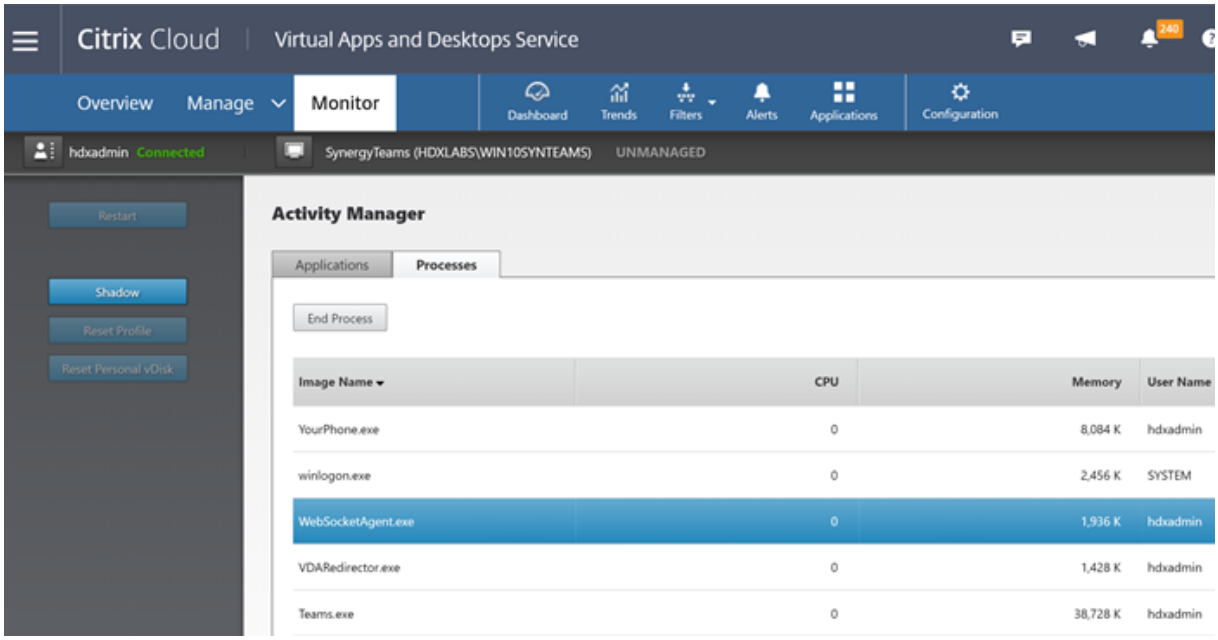
- Microsoft Teams überwachen sowie Problembehandlung und Support
- Bereitstellen der Teams-Desktopanwendung auf der VM
- Installieren von Microsoft Teams mit MSI (Abschnitt VDI-Installation)
- Thin Clients
- Skype for Business Network Assessment Tool
- Hinweise zur Koexistenz und Interoperabilität von Microsoft Teams und Skype for Business

Überwachung, Problembehandlung und Support für Microsoft Teams

March 15, 2022

Überwachen von Teams

Dieser Abschnitt enthält Richtlinien zum Überwachen der Microsoft Teams-Optimierung mit HDX. Wenn der Benutzer im optimierten Modus ausgeführt wird und auf dem Clientcomputer `HdxTeams.exe` ausgeführt wird, wird in der Sitzung der VDA-Prozess `WebSocketAgent.exe` ausgeführt. Verwenden Sie den **Aktivitätsmanager** in Director, um die Anwendung anzuzeigen.



Mit dem VDA (Mindestversion 1912) können Sie in Teams aktive Anrufe mit Citrix HDX Monitor (Mindestversion 3.11) überwachen. Das ISO-Image von Citrix Virtual Apps and Desktops enthält die neueste Version von `hdxmonitor.msi` im Ordner `layout\image-full\Support\HDX Monitor`.

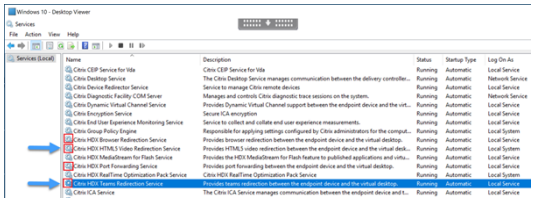
Weitere Informationen finden Sie im Knowledge Center-Artikel CTX253754 unter *Monitoring*.

Problembehandlung

Dieser Abschnitt enthält Tipps zur Behandlung von Problemen, die bei der Verwendung der Optimierung für Microsoft Teams auftreten können.
Weitere Informationen finden Sie in CTX253754.

Virtual Delivery Agent

Von BCR_x64.msi werden vier Dienste installiert. Nur zwei sind für die Microsoft Teams- Umleitung auf dem VDA verantwortlich.



- **Citrix HDX Teams Redirection Service** richtet den virtuellen Kanal ein, der in Microsoft Teams verwendet wird. Der Dienst basiert auf CtxSvcHost.exe.

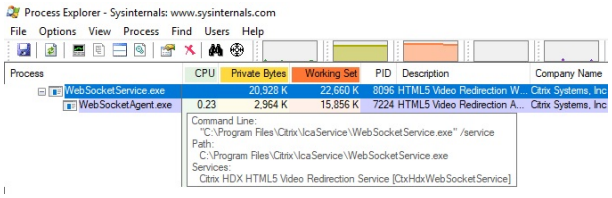
- **Citrix HDX HTML5 Video Redirection Service** wird als WebSocketService.exe ausgeführt und überwacht 127.0.0.1:9002 TCP. WebSocketService.exe führt zwei Hauptfunktionen aus:

  i. **TLS termination for secure WebSockets** empfängt eine sichere WebSocket-Verbindung von vdiCitrixPeerConnection.js, einer Komponente in der Microsoft Teams-App. Sie können sie mit der Prozessüberwachung verfolgen. Weitere Informationen zu Zertifikaten finden Sie im Abschnitt "TLS- und HTML5-Videoumleitung und Browserinhaltsumleitung"unter Kommunikation zwischen Controller und VDA.

  Einige Antiviren- und Desktop-Sicherheitsprogramme beeinträchtigen die Funktion von `WebSocketService.exe` und zugehörigen Zertifikaten. Während der Citrix HDX HTML5-Videoumleitungsdienst in der Konsole von `services.msc` möglicherweise ausgeführt wird, ist der Localhost-TCP-Socket `127.0.0.1:9002` nie im Listener-Modus, wie in netstat zu sehen ist. Beim versuchten Neustart des Diensts hört er auf zu reagieren ("Stopping …"). Stellen Sie sicher, dass Sie die richtigen Ausschlussbedingungen für den Prozess `WebSocketService.exe` verwenden.

  ii. **Benutzersitzungszuordnung.** Wenn die Anwendung Microsoft Teams startet, startet WebSocketService.exe den Prozess WebSocketAgent.exe in der Benutzersitzung auf dem VDA. WebSocketService.exe wird in Sitzung 0 als LocalSystem-Konto ausgeführt.

  Sie können mit **netstat** überprüfen, ob der WebSocketService.exe-Dienst auf dem VDA aktiv überwacht.

  Führen Sie mit erhöhten Rechten an der Eingabeaufforderung `netstat -anob -p tcp` aus:

```
 TCP    127.0.0.1:9001         0.0.0.0:0              LISTENING       11740
[WebSocketService.exe]
 TCP    127.0.0.1:9002         0.0.0.0:0              LISTENING       11740
[WebSocketService.exe]
```

  Bei einer erfolgreichen Verbindung ändert sich der Status in ESTABLISHED:

```
 TCP    127.0.0.1:9002         127.0.0.1:58069        ESTABLISHED     8096
[WebSocketService.exe]
 TCP    127.0.0.1:58069        127.0.0.1:9002         ESTABLISHED     748
[Teams.exe]
```


> **Wichtig:**
>
> WebSocketService.exe überwacht die beiden TCP-Sockets 127.0.0.1:9001 und 127.0.0.1:9002. Port 9001 wird für die Browserinhaltsumleitung und die HTML5-Videoumleitung verwendet. Port 9002 wird für die Microsoft Teams-Umleitung verwendet. Stellen Sie sicher, dass das Windows-Betriebssystem des VDA keine Proxykonfigurationen enthält, die eine direkte Kommunikation zwischen Teams.exe und WebSocketService.exe verhindern. Wenn Sie einen expliziten Proxy in Internet Explorer 11 konfigurieren (**Internetoptionen > Verbindungen > LAN-Einstellungen > Proxyserver**), können Verbindungen eventuell über einen zugewiesenen Proxyserver laufen. Stellen Sie sicher, dass **Proxyserver für lokale Adressen umgehen** aktiviert ist, wenn Sie eine manuelle und explizite Proxyeinstellung verwenden.

Speicherorte und Beschreibung der Dienste

Service	Pfad zu Programmdatei in Windows Server-Betriebssystem	Anmelden als	Beschreibung
Citrix HTML5-Videoumleitungsdienst	"C:\Programme (x86)\Citrix\System32\WebSocketService.exe" /service	Lokales Systemkonto	Bietet mehrere HDX Multimedia-Dienste mit dem Framework, das für die Durchführung der Medienumleitung zwischen dem virtuellen Desktop und dem Endgerät erforderlich ist.
Citrix HDX-Browserumleitungsdienst	"C:\Programme (x86)\Citrix\System32\CtxSvcHost.exe" -g BrowserRedirSvcs	Dieses Konto (lokaler Dienst)	Ermöglicht die Browserinhaltsumleitung zwischen dem Endpunktgerät und dem virtuellen Desktop.

Service	Pfad zu Programmdatei in Windows Server-Betriebssystem	Anmelden als	Beschreibung
Citrix Portweiterleitungsdienst	"C:\Programme (x86)\Citrix\System32\CtxSvcHost.exe" -g PortFwdSvcs	Dieses Konto (lokaler Dienst)	Ermöglicht die Portweiterleitung zwischen dem Endpunktgerät und dem virtuellen Desktop für die Browserinhaltsumleitung.
Citrix HDX-Teams-Umleitungsdienst	"C:\Programme (x86)\Citrix\System32\CtxSvcHost.exe" -g TeamsSvcs	Lokales Systemkonto	Ermöglicht die Microsoft Teams-Umleitung zwischen dem Endpunktgerät und dem virtuellen Desktop.

Citrix Workspace-App

Auf dem Endpunkt des Benutzers instanziiert die Citrix Workspace-App für Windows einen neuen Dienst namens HdxTeams.exe. Dies geschieht, wenn Microsoft Teams auf dem VDA gestartet wird und der Benutzer versucht, in der Eigenvorschau einen Anruf zu tätigen oder auf Peripheriegeräte zuzugreifen. Wenn dieser Dienst nicht angezeigt wird, überprüfen Sie Folgendes:

1. Die Workspace-App Version 1905 für Windows wurde installiert. Enthält der Installationspfad der Workspace-App HDXTeams.exe und die webrpc.dll-Binärdateien?
2. Wenn Sie Schritt 1 überprüft haben, gehen Sie folgendermaßen vor, um zu prüfen, ob HDX-Teams.exe gestartet wird.

    a) Beenden Sie Microsoft Teams auf dem VDA.
    b) Starten Sie services.msc auf dem VDA.
    c) Beenden Sie den Citrix HDX-Teams-Umleitungsdienst.
    d) Trennen Sie die ICA-Sitzung.
    e) Verbinden Sie die ICA-Sitzung.
    f) Starten Sie den Citrix HDX-Teams-Umleitungsdienst.
    g) Starten Sie den Citrix HDX HTML5-Videoumleitungsdienst neu.

h) Starten Sie Microsoft Teams auf dem VDA.

3. Wird HDXTeams.exe auf dem Clientendpunkt immer noch nicht gestartet, gehen Sie wie folgt vor:

   a) Starten Sie den VDA neu.
   b) Starten Sie den Clientendpunkt neu.

Support

Citrix und Microsoft unterstützen gemeinsam die Bereitstellung von Microsoft Teams über Citrix Virtual Apps and Desktops mithilfe der Optimierung für Microsoft Teams. Diese gemeinsame Unterstützung ist das Ergebnis einer engen Zusammenarbeit zwischen den beiden Unternehmen. Wenn Sie gültige Supportverträge haben und ein Problem mit dieser Lösung auftritt, öffnen Sie ein Supportticket bei dem Anbieter, in dessen Code Sie die Ursache des Problems vermuten. Das heißt, Microsoft für Teams und Citrix für die Optimierungskomponenten.

Citrix oder Microsoft erhält das Ticket, prüft das Problem und eskaliert gegebenenfalls. Sie müssen sich nicht an das Supportteam beider Unternehmen wenden.

Bei Problemen empfehlen wir, in der Teams-Benutzeroberfläche auf **Hilfe > Problem melden** zu klicken. VDA-seitige Protokolle werden automatisch zwischen Citrix und Microsoft geteilt, um technische Probleme schneller zu beheben.

Sammeln von Protokollen

Die HDX Media Engine-Protokolle sind auf der Benutzermaschine (nicht auf dem VDA). Bei Problemen fügen Sie die Protokolle Ihrem Supportfall bei.

Windows-Protokolle:

Windows-Protokolle finden Sie auf der Benutzermaschine unter %TEMP% im Ordner **HDXTeams** (AppData/Local/Temp/HDXTeams oder AppData/Local/Temp/HdxRtcEngine). Suchen Sie die TXT-Datei webrpc_Day_Month_timestamp_Year.txt. Wenn Sie eine neuere Citrix Workspace-App-Version verwenden, z. B. Citrix Workspace-App 2009.5, speichern Sie die Protokolle in AppData\Local\Temp\HdxRtcEngine.

Für jede Sitzung wird ein eigener Protokollordner erstellt.

Mac-Protokolle:

1. VDWEBRTC-Protokoll - zeichnet die Ausführung des virtuellen Kanals auf.

   Speicherort: /Users/<User Name>/Library/Logs/Citrix Workspace/CitrixViewer_<Y_M_D_H_M_S>.txt

2. HdxRtcEngine log - zeichnet die Ausführung der Prozesse auf HdxRtcEngine auf.

   Speicherort: $TMPDIR/hdxrtcengine/<W_M_D_H_M_S_Y>/hdxrtcengine.log

   HdxRtcEngine-Protokollierung ist standardmäßig aktiviert.

Linux-Protokolle:

Die Linux-Protokolle sind im Verzeichnis /tmp/webrpc/<current date>/ and /tmp/hdxrtcengine/<current date>/.

Beim Einrichten eines Anrufs sind folgende vier ICE-Phasen erforderlich:

- Sammeln der Kandidaten
- Austausch der Kandidaten
- Konnektivitätsprüfungen (STUN-Bind-Anforderungen)
- Einstufung der Kandidaten

In den Protokollen für HdxTeams.exe sind die folgenden Einträge für ICE (Interactive Connectivity Establishment) relevant: Diese Einträge müssen vorhanden sein, damit ein Anruf erfolgreich eingerichtet wird (siehe Beispielausschnitt für Sammelphase):

```
RPCStubs Info: -> device id = \\?\display#int3470#4&1835d135&0&uid13424
   #{
 65e8773d-8f56-11d0-a3b9-00a0c9223196 }
 {
 bf89b5a5-61f7-4127-a279-e187013d7caf }
  label = Microsoft Camera Front groupId =

webrtcapi.RTCPeerConnection Info: createOffer. audio = 1 video = 1
webrtcapi.RTCPeerConnection Info: setLocalDescription.
>>> begin:sdp
[...]

webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
   HaveLocalOffer

webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state =
   Gathering

[...]
>>> begin:sdp
candidate:840548147 1 udp 2122194687 10.108.124.215 56927 typ host
   generation 0 ufrag oVk6 network-id 1
<<< end:sdp
[...]
>>> begin:sdp
candidate:1938109490 1 udp 24911871 52.114.xxx.xxx 52786 typ relay
   raddr 73.205.xxx.x rport 25651 generation 0 ufrag dDML network-id 1
   network-cost 10
<<< end:sdp
[...]
```



```
>>> begin:sdp
candidate:4271145120 1 udp 1685987071 66.xxx.xxx.xxx 55839 typ srflx
    raddr 10.108.124.215 rport 55839 generation 0 ufrag uAVH network-id
    1
<<< end:sdp
[...]

webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state =
    Complete webrtcapi.RTCPeerConnection Info: setRemoteDescription.
>>> begin:sdp
[...]

webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
    HaveRemotelOffer

<!--NeedCopy-->
```

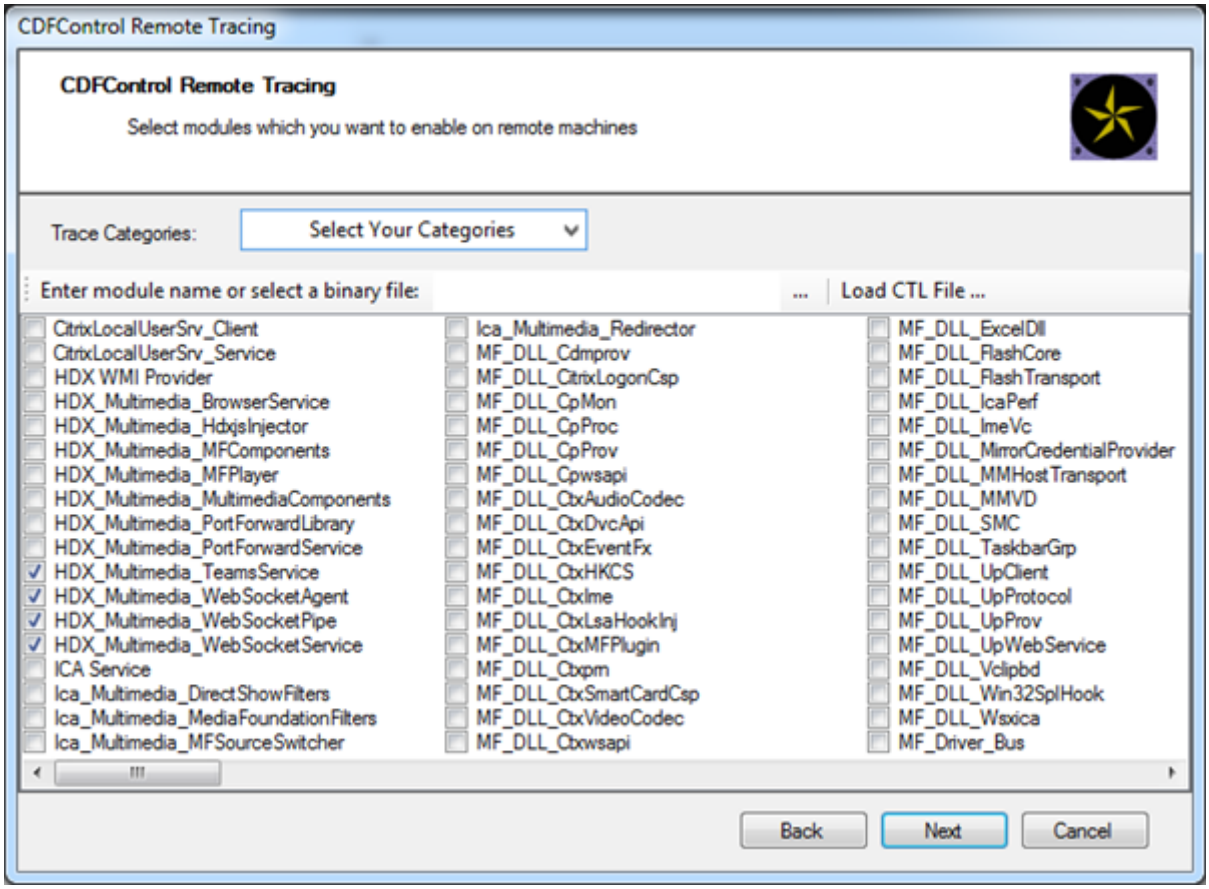
Wenn mehrere ICE-Kandidaten vorhanden sind, lautet die Reihenfolge der Präferenz:

1. Host
2. Peer reflexiv
3. Server reflexiv
4. Transport-Relay

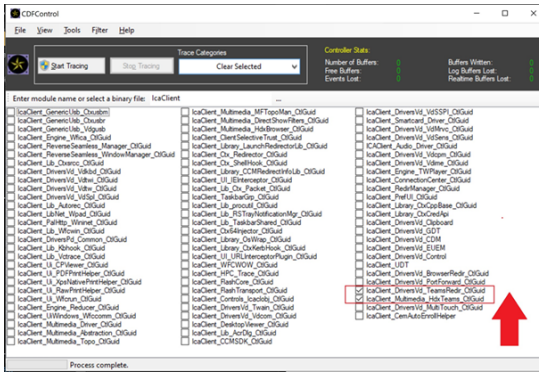
Wenn ein Problem auftritt und Sie es reproduzieren können, empfehlen wir, in Teams auf **Hilfe > Problem melden** zu klicken. Protokolle werden zwischen Citrix und Microsoft geteilt, um technische Probleme zu beheben, wenn Sie einen Supportfall bei Microsoft öffnen.
Das Aufzeichnen von CDF-Traces vor der Kontaktaufnahme mit dem Citrix Support ist ebenfalls von Vorteil. Weitere Informationen finden Sie im Knowledge Center-Artikel CDFcontrol.

Empfehlungen zur Erzeugung von CDF-Tracingberichten finden Sie im Knowledge Center-Artikel Recommendations for Collecting the CDF Traces.

VDA-seitige CDF-Tracingberichte –aktivieren Sie die folgenden CDF-Trace-Anbieter:



Workspace-App-seitige CDF-Tracingberichte –aktivieren Sie die folgenden CDF-Trace-Anbieter:



Windows Media-Umleitung

September 21, 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 Citrix Scout einen CDF-Trace (Citrix Diagnostics Facility) von HostMMTransport.dll durchführen, um zu ermitteln, welche Methode verwendet wird. Weitere Informationen finden Sie unter Citrix Scout.

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".

Einschränkung:

Wenn Sie Windows Media Player mit aktivierten Remote-Audio und Video Erweiterungen (RAVE) in einer Sitzung verwenden wird ggf. ein schwarzer Bildschirm angezeigt. Der schwarze Bildschirm kann angezeigt werden, wenn Sie mit der rechten Maustaste auf den Videoinhalt klicken und **Aktuelle Wiedergabe immer oben anzeigen** wählen.

Allgemeine Inhaltsumleitung

February 6, 2020

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. In der Regel sind andere Formen der Inhaltsumleitung besser. Diese Umleitungsart wird nur auf VDAs für Multisitzungs-OS und nicht auf VDAs für Einzelsitzungs-OS unterstützt.

Lokaler App-Zugriff und URL-Umleitung

Durch lokalen App-Zugriff werden lokal installierte Windows-Anwendungen problemlos in eine gehostete Desktopumgebung integriert. Es ist kein Wechsel zwischen Desktops erforderlich.

HDX-Technologie bietet **generische USB-Umleitung** für Spezialgeräte ohne optimierte Unterstützung oder wenn diese ungeeignet ist.

Clientordnerumleitung

February 6, 2020

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 werden als UNC-Links in Sitzungen angezeigt. Es ist nicht das komplette Dateisystem auf dem Benutzergerät abgebildet. Wenn Sie UNC-Links durch die Registrierung deaktivieren, werden Clientordner als zugeordnete Laufwerke in der Sitzung angezeigt.

Die Clientordnerumleitung wird nur auf Maschinen mit Windows-Einzelsitzungs-OS 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 der Citrix Workspace-App enthalten.

Anforderungen:

Server:

- Windows Server 2019, Standard und Datacenter Edition
- Windows Server 2016, Standard und Datacenter Edition
- Windows Server 2012 R2, Standard und Datacenter Edition

Clients:

- Windows 10, 32-Bit- und 64-Bit-Editionen (Mindestversion 1607)
- Windows 8.1, 32-Bit- und 64-Bit-Editionen (inkl. Embedded Edition)
- Windows 7, 32-Bit- und 64-Bit-Editionen (inkl. Embedded Edition)

> **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. 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 der Citrix Workspace-App installiert ist.
    b) Starten Sie vom Installationsverzeichnis der Citrix Workspace-App 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

March 15, 2022

Mit der Host-zu-Client-Umleitung können URLs, die als Hyperlink in einer Citrix Sitzung ausgeführten Anwendungen eingebettet sind, mit der zugehörigen Anwendung auf Benutzergeräten geöffnet werden. Häufige Anwendungsfälle für die Host-zu-Client-Umleitung sind:

- Umleitung von Websites, wenn der Citrix Server keinen Internet- oder Netzwerkzugriff auf die Quelle hat.
- Umleitung von Websites, wenn das Ausführen eines Webbrowsers in Citrix Sitzungen aus Sicherheits-, Leistungs-, Kompatibilitäts- oder Skalierbarkeitsgründen nicht erwünscht ist.
- Umleitung spezifischer URL-Typen für Anwendungen, die nicht auf dem Citrix Server installiert sind.

Die Host-zu-Client-Umleitung ist nicht für URLs vorgesehen, auf die über eine Webseite zugegriffen wird oder die in die Adressleiste des in der Citrix Sitzung ausgeführten Webbrowsers eingegeben werden. Informationen zur URL-Umleitung in Webbrowsern finden Sie unter Bidirektionale URL-Umleitung und Browserinhaltsumleitung.

Systemanforderungen

- Multisitzungs-OS-VDA
- Unterstützte Clients:
  - Citrix Workspace-App für Windows
  - Citrix Workspace-App für Mac
  - Citrix Workspace-App für Linux
  - Citrix Workspace-App für HTML5
  - Citrix Workspace-App für Chrome

Auf dem Clientgerät muss eine Anwendung zur Verarbeitung der Umleitung der URL-Typen installiert und konfiguriert sein.

Konfiguration

Verwenden Sie die Citrix Richtlinie Host-zu-Client-Umleitung, um diese Funktionalität zu aktivieren. Die **Host-zu-Client-Umleitung** ist standardmäßig deaktiviert. Nachdem Sie die Richtlinie "Host-zu-Client-Umleitung"aktiviert haben, registriert sich Citrix Launcher beim Windows-Server, damit es URLs abfangen und an das Clientgerät senden kann.

Sie müssen dann die Windows-Gruppenrichtlinie so konfigurieren, dass Citrix Launcher als Standardanwendung für die gewünschten URL-Typen verwendet wird. Erstellen Sie auf dem Citrix Server-VDA die Datei ServerFTAdefaultPolicy.xml und fügen Sie den folgenden XML-Code ein.

```
<?xml version="1.0" encoding="UTF-8"?>

<DefaultAssociations>

<Association Identifier="http" ProgId="ServerFTAHTML" ApplicationName="
    ServerFTA" />

<Association Identifier="https" ProgId="ServerFTAHTML" ApplicationName=
    "ServerFTA" />

</DefaultAssociations>
<!--NeedCopy-->
```

Gehen Sie in der Gruppenrichtlinien-Verwaltungskonsole zu **Computerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Datei-Explorer > Konfigurationsdatei für Standardzuordnungen festlegen** und speichern Sie die Datei ServerFTAdefaultPolicy.xml.

> **Hinweis:**
>
> Wenn ein Citrix Server keine Gruppenrichtlinieneinstellungen hat, werden die Benutzer von Windows aufgefordert, eine Anwendung zum Öffnen von URLs auszuwählen.

Standardmäßig unterstützen wir die Umleitung der folgenden URL-Typen:

- HTTP
- HTTPS
- RTSP
- RTSPU
- PNM
- MMS

Um weitere standardmäßige oder benutzerdefinierte URL-Typen in die Liste für die Umleitung aufzunehmen, erstellen Sie eine neue **Association Identifier**-Zeile in der o. g. Datei ServerFTAdefaultPolicy.xml. Beispiel:

```
<Association Identifier="ftp"ProgId="ServerFTAHTML"ApplicationName="
ServerFTA"/>

<Association Identifier="mailto"ProgId="ServerFTAHTML"ApplicationName
="ServerFTA"/>

<Association Identifier="customtype1"ProgId="ServerFTAHTML"ApplicationName
="ServerFTA"/>
```



```
<Association Identifier="customtype2"ProgId="ServerFTAHTML"ApplicationName
="ServerFTA"/>
```

Das Hinzufügen von URL-Typen zur Liste erfordert außerdem eine Clientkonfiguration. Erstellen Sie den folgenden Registrierungsschlüssel mit den folgenden Werten auf dem Windows-Client.

> **Hinweis:**
>
> 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.

- Schlüssel: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Citrix\ICA Client\SFTA
- Wertname: ExtraURLProtocols
- Werttyp: REG_SZ
- Wertdaten: URL-Typen, durch Semikolon getrennt. Geben Sie alles vor dem authority-Teil der URL ein. Beispiel:
  `ftp://;mailto:;customtype1://;custometype2://`

Sie können URL-Typen nur für Windows-Clients hinzufügen. Clients ohne die obigen Registrierungseinstellungen lehnen die Umleitung zurück an die Citrix Sitzung ab. Auf dem Client muss eine Anwendung installiert und konfiguriert sein, die die angegebenen URL-Typen verarbeiten kann.

Um URL-Typen aus der Standardumleitungsliste zu entfernen, erstellen Sie den folgenden Registrierungsschlüssel mit den folgenden Werten auf dem Server-VDA.

- Schlüssel: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- Wertname: DisableServerFTA
- Werttyp: DWORD
- Wertdaten: 1
- Wertname: NoRedirectClasses
- Werttyp: REG_MULTI_SZ
- Wertdaten: eine beliebige Kombination der Werte –`httphttps`, `rtsp`, `rtspu`, `pnm` oder `mms`. Geben Sie mehrere Werte auf separaten Zeilen an. Beispiel:

```
http

https

rtsp
```


Zum Aktivieren der Host-zu-Client-Umleitung für spezifische Websites erstellen Sie einen Registrierungsschlüssel mit Werten auf dem Server-VDA.

- Schlüssel: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- Wertname: ValidSites
- Werttyp: REG_MULTI_SZ
- Wertdaten: eine beliebige Kombination vollständig qualifizierter Domänennamen (FQDN). Geben Sie mehrere FQDNs auf separaten Zeilen an. Geben Sie nur den FQDN ohne Protokoll (`http://` oder `https://`) ein. Ein FQDN darf nur an der Stelle ganz links ein Sternchen (`*`) als Platzhalter enthalten. Der Platzhalter entspricht einer Domänenebene und somit den Vorgaben von RFC 6125. Beispiel:

`www.exmaple.com`

`*.example.com`

> **Hinweis:**
>
> Sie können den Schlüssel **ValidSites** nicht in Kombination mit den Schlüsseln **DisableServerFTA** und **NoRedirectClasses** verwenden.

Standardbrowserkonfiguration auf dem Server-VDA

Die hier beschriebene Aktivierung der Host-zu-Client-Umleitung ersetzt jede bestehende Standardbrowserkonfiguration auf dem Server-VDA. Wenn eine Web-URL nicht umgeleitet wird, übergibt Citrix Launcher die URL an den im Registrierungsschlüssel `command_backup` konfigurierten Browser. Der Schlüssel verweist standardmäßig auf Internet Explorer, Sie können jedoch den Pfad eines anderen Browsers angeben. Weitere Informationen finden Sie unter Standardbrowserkonfiguration auf dem Server-VDA in der Liste der über die Registrierung verwalteten Features.

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

- Einzelsitzungs- oder Multisitzungs-OS-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

November 2, 2022

Einführung

Durch lokalen App-Zugriff werden lokal installierte Windows-Anwendungen problemlos in eine gehostete Desktopumgebung integriert, ohne dass ein Wechsel zwischen Desktops 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. Hierfür platzieren Sie eine Verknüpfung mit der veröffentlichten Anwendung auf das Windows-Gerät des Benutzers.
- 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. Beispiel hierfür sind DVD-Brenner und TV-Tuner.

In Citrix Virtual Apps and Desktops 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 wieder in der Desktopsitzung 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 den 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 Citrix Virtual Apps and Desktops-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 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 der VDA beispielsweise von einem Datencenter in Großbritannien bereitgestellt wird und der Client eine Verbindung aus Indien herstellt, würde der Benutzer erwarten, dass die Website in.msn.com erscheint. Stattdessen wird uk.msn.com angezeigt.
- Multimedia-Inhalt: Websites mit Rich-Media-Inhalten, die auf dem Clientgerät wiedergegeben werden, ermöglichen die gewohnte Benutzererfahrung und das Einsparen von Bandbreite während die Funktionalität auch in Netzwerken mit hoher Latenz gewährleistet ist. Dieses Feature leitet Websites mit anderen Medientypen wie Silverlight um. 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 für die gültigen Betriebssystemen für VDAs für Windows-Multisitzungs-OS und Windows-Einzelsitzungs-OS unterstützt. Der lokale App-Zugriff erfordert mindestens Version 4.1 der Citrix Workspace-App für Windows. 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

Citrix Viewer muss auch auf dem VDA aktiviert sein.

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 Sie lokalen App-Zugriff auf einem virtuellen Desktop verwenden, der im Fenstermodus bzw. nicht auf allen Monitoren ausgeführt wird.
  - Bei Verwendung mehrerer Monitore: Der maximierte Monitor ist der Standarddesktop für alle Anwendungen, die in der Sitzung gestartet werden. Dies gilt auch dann, wenn nachfolgende Anwendungen normalerweise auf einem anderen Monitor starten würden.
  - Das Feature unterstützt einen VDA. Es ist keine Integration mit mehreren VDAs gleichzeitig 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/64-Bit-Systeme mit clientgehosteten Anwendungen und VDA-Anwendungen unterstützt. Lokale 32-Bit-Anwendungen können also nicht mit 64-Bit-VDA-Anwendungen gruppiert werden.
  - Anwendungen können nicht mit 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 Dateien zu erstellen.
- Mehrere Instanzen einer lokal ausgeführten Anwendung verhalten sich entsprechend den Taskleisteneinstellungen für den virtuellen Desktop. Verknüpfungen mit 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.

- Wenn Sie die Richtlinieneinstellung **Lokalen App-Zugriff zulassen** auf **Aktiviert** festlegen, wird die Browserinhaltsumleitung nicht unterstützt.

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 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 die 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 zudem URL-Positivlisten- und Sperrlisten-Richtlinieneinstellungen 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.
> - 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. Dies gilt selbst dann, wenn sie auf der Sperrliste steht.

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.

Generische USB-Umleitung und Clientlaufwerke

April 19, 2024

HDX-Technologie bietet **optimierte Unterstützung** für die gebräuchlichsten USB-Geräte. 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.
- 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 die Citrix Workspace-App für Android haben.
- Die Version der Citrix Workspace-App 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.

> **Wichtig:**
>
> - 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.
> - Die Citrix Richtlinieneinstellung Regeln für die USB-Clientgeräteoptimierung ist eine spezifische Einstellung für die generische USB-Umleitung für ein bestimmtes USB-Gerät. Es gilt nicht für die hier beschriebene optimierte Unterstützung.
> - Bei Vermittlung einer Sitzung mit Citrix Software an eine virtuelle Azure-Maschine bietet Citrix bestmögliche Unterstützung für die USB-Umleitung an die virtuelle Azure-Maschine. Wir bieten Support bei Problemen der Citrix Software, jedoch nicht für die zugrunde liegende virtuelle Azure-Maschine.

Überlegungen zur Leistung für USB-Geräte

Bei Verwendung 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). Kann die Bandbreite nicht erhöht werden, können Sie evtl. die Bandbreitennutzung anderer Komponenten über die Einstellung der Bandbreitenrichtlinie anpassen. 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 der Citrix Workspace-App und von Citrix Virtual Apps and Desktops 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 verwenden, die von einer vertrauenswürdigen Quelle stammen.
> - USB-Geräte in zugänglichen Umgebungen (z. B. Internetcafé) nicht unbeaufsichtigt lassen.
> - Erläutern Sie die Risiken der Verwendung eines USB-Geräts 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 Workspace-App-Versionen unterstützen die generische USB-Umleitung:

- Citrix Workspace-App für Windows, siehe Konfigurieren der Anwendungsbereitstellung
- Citrix Workspace-App für Mac, siehe Konfigurieren von Citrix Workspace-App für Mac
- Citrix Workspace-App für Linux, siehe Optimieren
- Citrix Workspace-App für Chrome, siehe Citrix Workspace-App für Chrome

Informationen zu den Citrix Workspace-App-Versionen finden Sie unter Citrix Workspace-App-Featurematrix.

Wenn Sie eine ältere Version der Citrix Workspace-App verwenden, prüfen Sie in der zugehörigen Dokumentation, ob die generische USB-Umleitung unterstützt wird. Die Dokumentation zur Citrix Workspace-App enthält Informationen zu allen Einschränkungen für unterstützte USB-Gerätetypen.

Die generische USB-Umleitung unterstützt Desktopsitzungen mit VDAs für Einzelsitzungs-OS ab Version 7.6 bis zur aktuellen Version.

Die generische USB-Umleitung unterstützt Desktopsitzungen mit VDAs für Multisitzungs-OS ab Version 7.6 bis zur aktuellen Version, mit folgenden Einschränkungen:

- Der VDA muss unter Windows Server 2012 R2 oder Windows Server 2016 ausgeführt werden.
- Der USB-Gerätetreiber muss mit dem Remotedesktop-Sitzungshost für das Betriebssystem des VDAs (Windows 2012 R2) einschließlich voller Virtualisierung 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 Citrix Ready Marketplace. 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, und sie separat für die einzelnen Gerätetypen konfigurieren.

- Auf dem VDA mit Citrix Richtlinieneinstellungen. Weitere Informationen finden Sie unter Umleitung von Clientlaufwerken und Benutzergeräten und Einstellungen der Richtlinie "USB-Geräte".
- In der Citrix Workspace-App über Citrix Workspace-App-abhängige Mechanismen. Beispielsweise können durch eine administrative Vorlage Registrierungseinstellungen zur Konfiguration der Citrix Workspace-App für Windows gesteuert werden. Standardmäßig ist die USB-Umleitung für bestimmte Klassen von USB-Geräten zulässig bzw. nicht zulässig. Weitere Informationen finden Sie unter Konfigurieren in der Dokumentation der Citrix Workspace-App für Windows.

Diese separate Konfiguration ist flexibler. Beispiel:

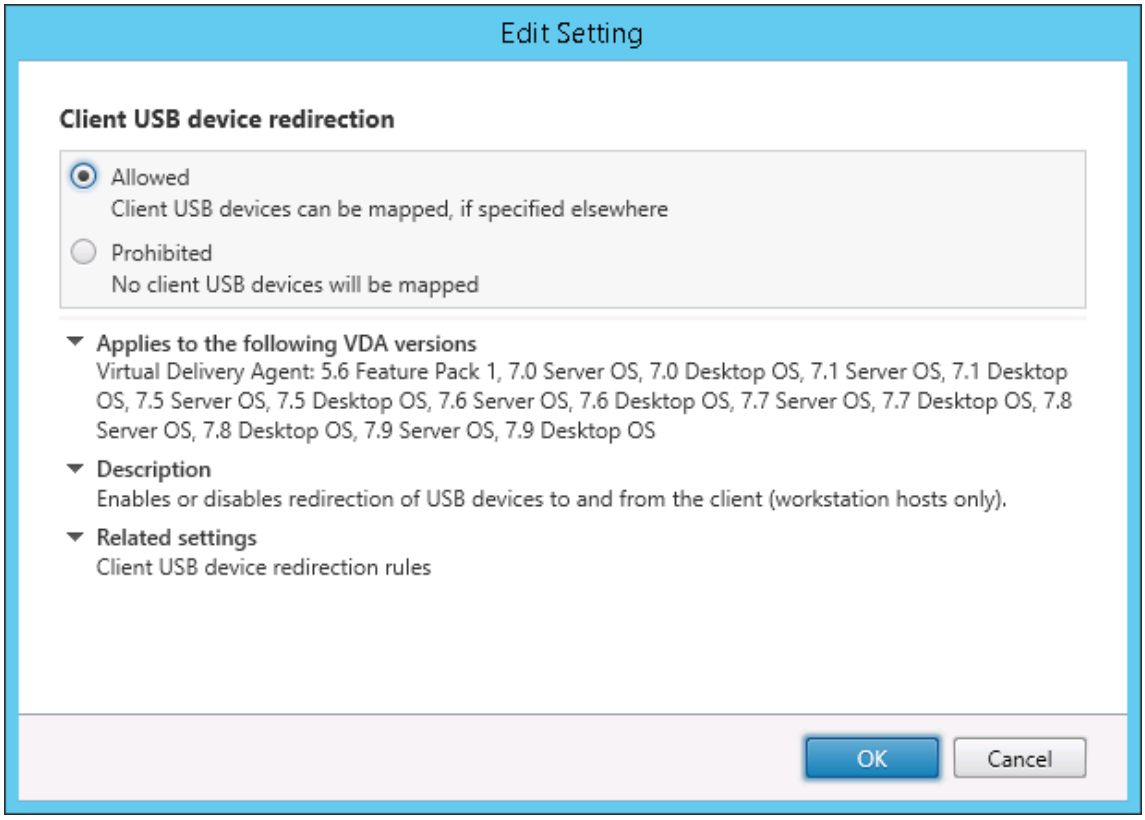
- Wenn zwei verschiedene Abteilungen für die Citrix Workspace-App und den VDA verantwortlich sind, können sie eigene Vorgaben festlegen. Diese Konfiguration gilt dann, wenn ein Benutzer in einer Abteilung auf eine Anwendung in einer anderen Abteilung zugreift.
- Citrix Richtlinieneinstellungen steuern USB-Geräte, die nur für bestimmte Benutzer oder nur für Benutzer, die eine Verbindung über das LAN anstelle von Citrix Gateway herstellen, zugelassen werden sollen.

Aktivieren der generischen USB-Umleitung

Um die generische USB-Umleitung zu aktivieren (= keine manuelle Umleitung durch den Benutzer erforderlich), konfigurieren Sie Citrix Richtlinieneinstellungen und die Verbindungseinstellungen der Citrix Workspace App.

Führen Sie in den Citrix Richtlinieneinstellungen folgende Schritte aus:

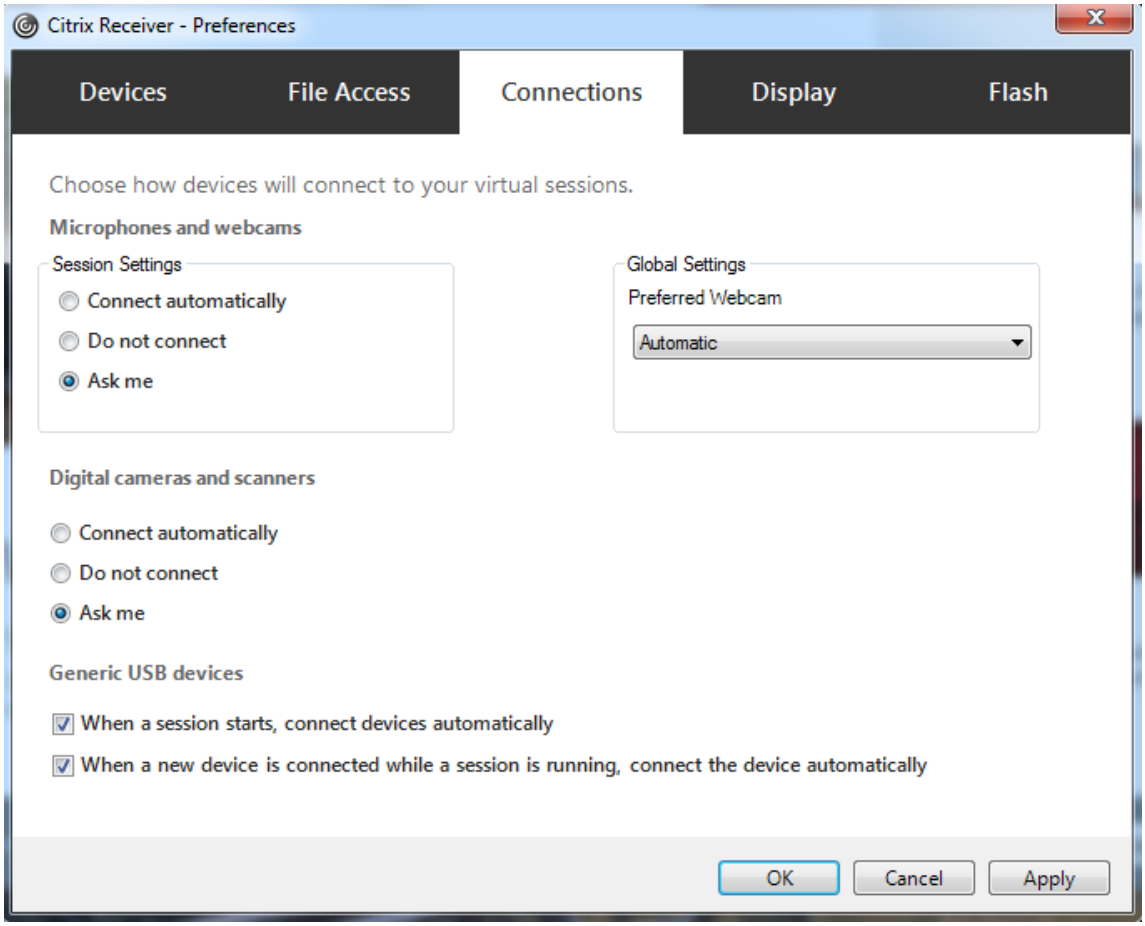
1. Fügen Sie die Client-USB-Geräteumleitung einer Richtlinie hinzu und stellen Sie den Wert auf **Zugelassen** ein.



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 der Citrix Workspace-App folgendermaßen vor:

3. Geben Sie an, dass Geräte automatisch, ohne manuelle Umleitung verbunden werden. Sie können eine administrative Vorlage verwenden oder die Einstellung unter "Citrix Workspace-App für Windows > Einstellungen > Verbindungen"festlegen.



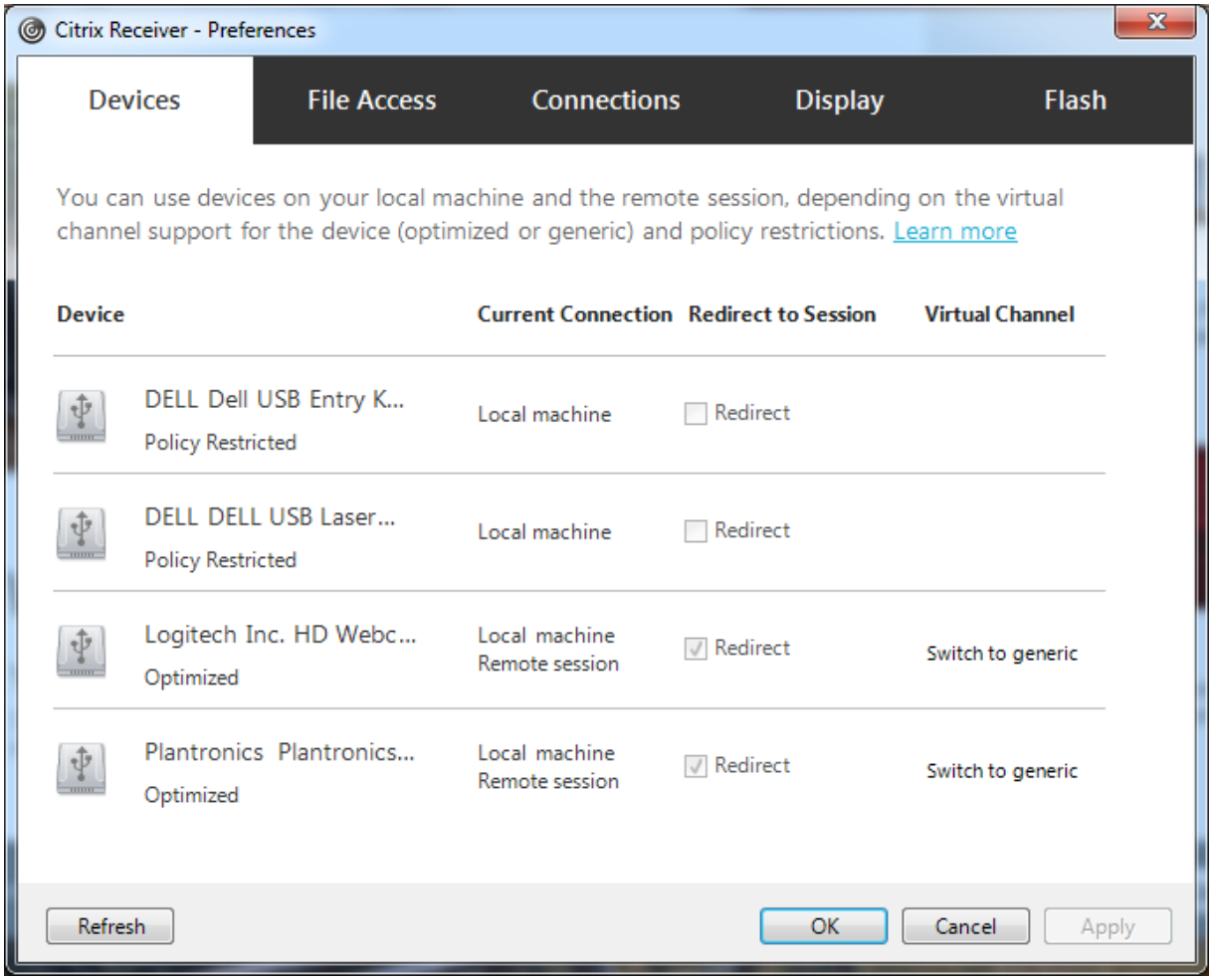
Wenn Sie im vorigen Schritt die USB-Richtlinienregeln für den VDA festgelegt haben, geben Sie nun die gleichen Richtlinienregeln für die Citrix Workspace-App ein.

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 der Verbindungsbalken nicht angezeigt wird.

Die Benutzer können Geräte, die nicht automatisch umgeleitet werden, explizit umleiten, indem sie sie aus der USB-Geräteliste auswählen. Weitere Informationen finden Sie unter Anzeigen von Geräten in Desktop Viewer in der Hilfe zur Citrix Workspace-App für Windows.



Verwendung der generischen USB-Umleitung anstelle der optimierten Unterstützung:

- Wählen Sie in der Citrix Workspace-App 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 Configure automatic redirection of USB devices.

> **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 die Citrix Workspace-App und den VDA spezifische Regeln festlegen.

Für die generische USB-Umleitung benötigen Sie mindestens die USB-Geräteklasse und die Unterklasse. 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 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 die Citrix Workspace-App fest, welche die USB-Standardrichtlinienregeln außer Kraft setzen.

VDA:

- Bearbeiten Sie die Administrator-Überschreibungsregeln für Maschinen mit Multisitzungs-OS 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 Workspace-App 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 (siehe Erläuterungen weiter unten). 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 http://www.usb.org/.
SubClass	Unterklasse vom Gerätedeskriptor oder ein Schnittstellendeskriptor
Prot	Protokoll vom Gerätedeskriptor oder ein Schnittstellendeskriptor

Wenn Sie Richtlinienregeln erstellen, beachten Sie Folgendes:

- Bei Regeln wird die Groß- und Kleinschreibung nicht berücksichtigt.
- Einer Regel kann optional ein Kommentar folgen, 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
```

- 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
```

Verwenden und Entfernen von USB-Geräten

Benutzer können ein USB-Gerät vor oder nach dem Starten einer virtuellen Sitzung anschließen.

Wenn Sie mit der Citrix Workspace-App 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. Die Unterstützung ist Teil der Citrix Virtual Apps and Desktops-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. Verwenden Sie die Einstellung **Clientwechseldatenträger**, um die Clientlaufwerkzuordnung zu konfigurieren. Diese Einstellung befindet sich im Bereich Dateiumleitung der ICA-Richtlinieneinstellungen.

Für USB-Massenspeichergeräte können Sie die Clientlaufwerkzuordnung, die generische USB-Umleitung oder beides verwenden. Die Steuerung erfolgt über Citrix Richtlinien. Die Hauptunterschiede sind folgende:

Feature	Clientlaufwerkzuordnung	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	Ja
BitLocker To Go-Geräte	Nein	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 und ein Massenspeichergerät vor oder nach dem Sitzungsstart angeschlossen wird, wird es mit der generischen USB-Umleitung umgeleitet. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX123015.

> **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

March 9, 2022

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 Multisitzungs-OS-Maschine 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.

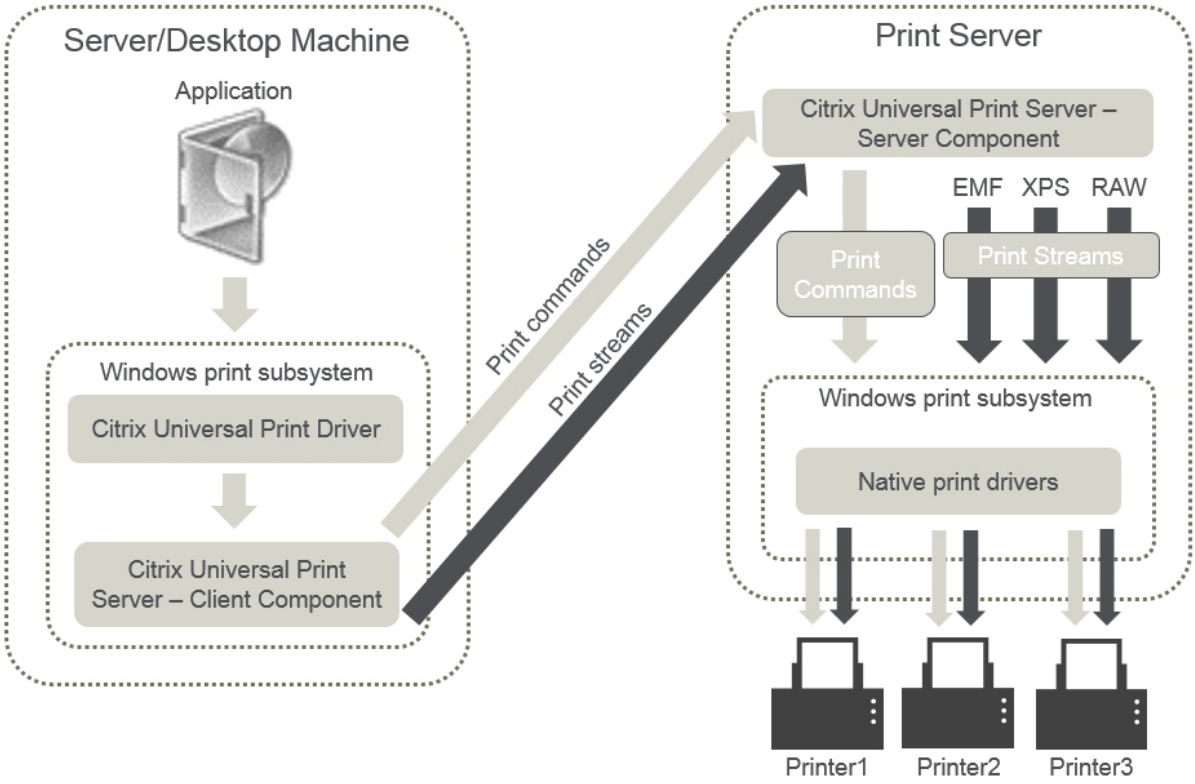
Der universelle Druckserver umfasst als Feature die folgenden Komponenten:

Eine Clientkomponente, **UPClient** - Aktivieren Sie UPClient auf jeder Multisitzungs-OS-Maschine, 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 Multisitzungs-OS-Maschinen 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 Multisitzungs-OS-Maschinen über die Richtlinieneinstellung "Druckertreiberzuordnung und -kompatibilität"

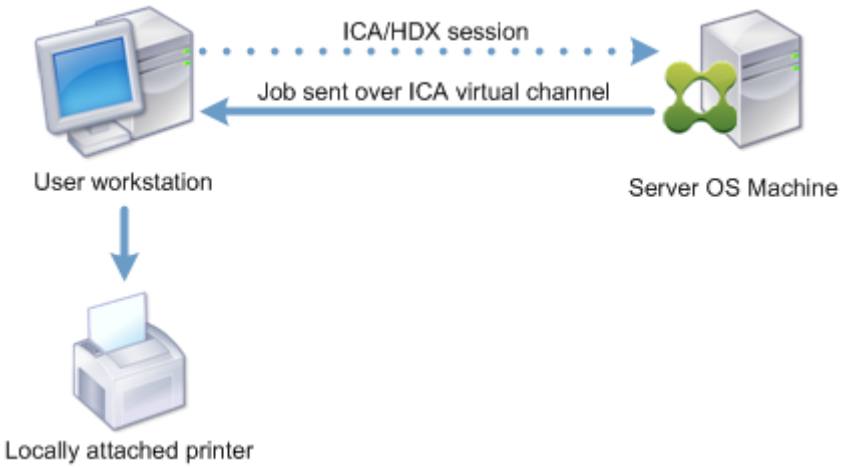
Weiterleiten von Druckaufträgen

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 Multisitzungs-OS-Maschine 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.



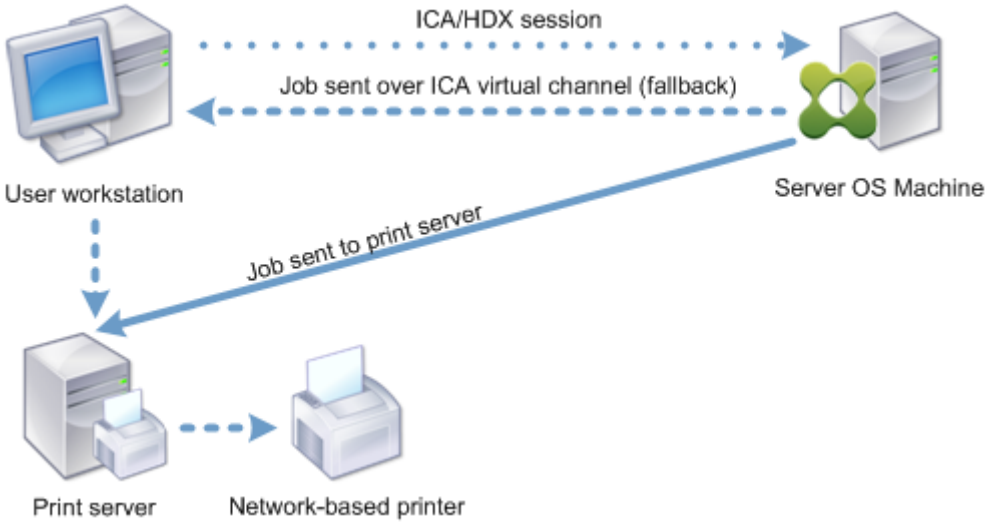
Netzwerkbasierte Drucker

Standardmäßig werden alle für Netzwerkdrucker bestimmten Druckaufträge von der Multisitzungs-OS-Maschine 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 Multisitzungs-OS-Maschine 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 von Citrix Virtual Apps and Desktops 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

Die Option zum Steuern der Installation des PDF-Druckertreibers für den universellen Druckserver wurde aus den VDA-Installationsprogrammen entfernt. Der PDF-Druckertreiber wird jetzt immer automatisch installiert. Bei einem Upgrade auf den VDA 7.17 (oder eine spätere unterstützte Version) wird ein zuvor installierter Citrix PDF-Druckertreiber automatisch entfernt und durch die neueste Version ersetzt.

Wenn ein Druckauftrag initiiert wird, sendet der Treiber die Ausgabe der Anwendung ohne Änderung an das Endpunktgerät.

Clientkomponente. Der Citrix UPD wird als Teil der Citrix Workspace-App installiert. Er ruft den eingehenden Druckdatenstrom der Citrix Virtual Apps and Desktops-Sitzung ab. Er leitet diesen dann an das lokale Drucksubsystem weiter, wo der Druckauftrag mit den gerätespezifischen Druckertreibern verarbeitet wird.

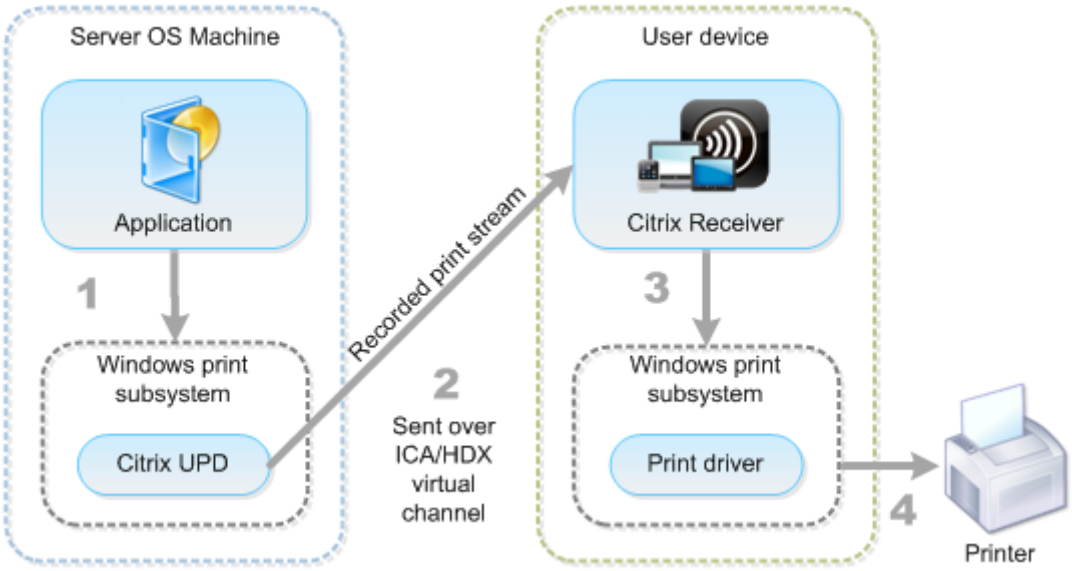
Der Citrix UPD unterstützt die folgenden Druckformate:

- 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.

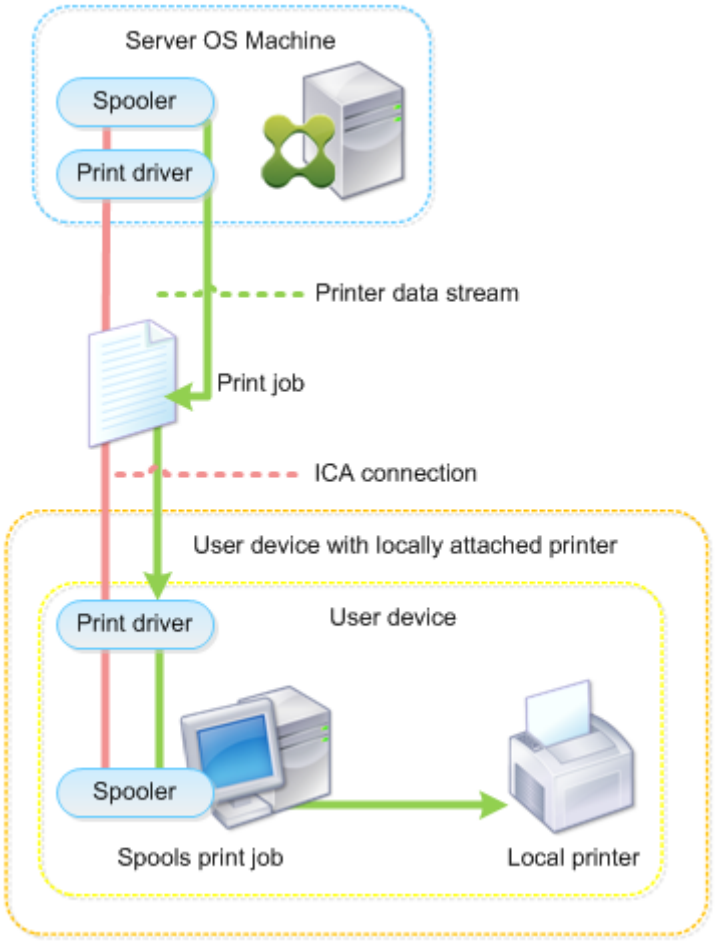


Legen Sie bei der Planung der Strategie zur Treiberverwaltung fest, ob Sie gerätespezifische Treiber,

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 Multisitzungs-OS-Maschine 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 Multisitzungs-OS-Maschine 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 Multisitzungs-OS-Maschinen nicht vorhanden)
- Erstellen der Treiberkompatibilitätslisten

Verwandter Inhalt

- Druckkonfigurationsbeispiele
- Bewährte Methoden, Überlegungen zur Sicherheit und Standardvorgänge
- Druckrichtlinien und Einstellungen
- Druckerprovisioning
- Pflegen der Druckumgebung

Druckkonfigurationsbeispiele

March 9, 2022

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.

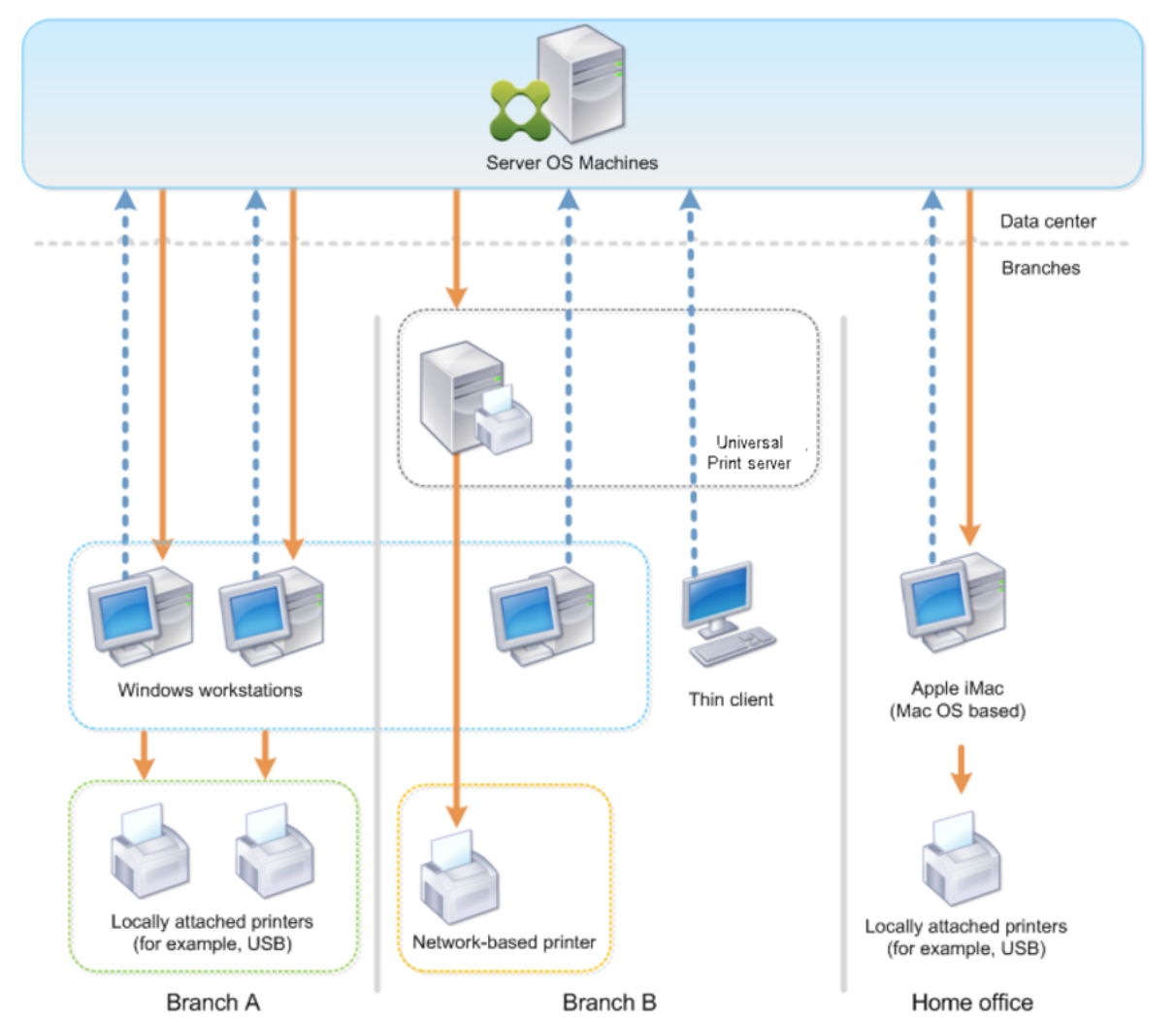
Achten Sie beim Entwerfen der Druckkonfiguration darauf, den Benutzern die gleiche Erfahrung in einer Sitzung zu bieten, wie sie es beim Drucken von lokalen Benutzergeräten aus gewohnt sind.

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 Multisitzungs-OS-Maschinen 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. Multisitzungs-OS-Maschinen 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

September 21, 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.
- Minimieren Sie die Anzahl der installierten Druckertreiber auf Multisitzungs-OS-Maschinen.
- 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 Multisitzungs-OS-Maschinen. 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 Multisitzungs-OS-Maschine 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.
- In VDAs ab Version 7.16 hat die Citrix Richtlinieneinstellung "Automatische Installation von mitgelieferten Druckertreibern"keine Auswirkungen auf Windows-Betriebssystemversionen ab Windows 8, da die mitgelieferten V3-Druckertreiber nicht im Betriebssystem enthalten sind.
- In VDAs bis Version 7.16 verwendet das System die Windows-Version des Druckertreibers, falls sie auf der Multisitzungs-OS-Maschine 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

September 21, 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 die Citrix Workspace-App 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 Multisitzungs-OS-Maschine 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 Multisitzungs-OS-Maschine, vorgenommen wurden.
- **Auf der Multisitzungs-OS-Maschine:** 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 Geräteeinstellun-

gen 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 Multisitzungs-OS-Maschine gespeicherten Standarddruckereinstellungen mit allen beibehaltenen Einstellungen oder Clientdruckereinstellungen 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 Multisitzungs-OS-Maschine 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

March 9, 2022

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 Multisitzungs-OS-Maschine, 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 Citrix Virtual Apps and Desktops Virtual Delivery Agent (VDA) für Windows-Einzelsitzungs-OS oder Windows-Multisitzungs-OS 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**.

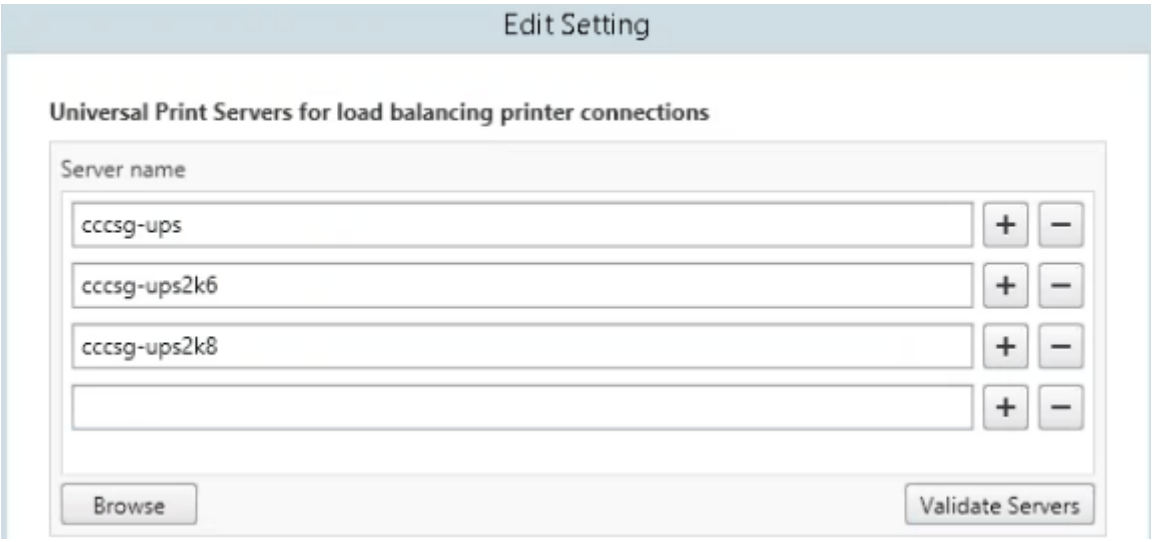
Zum Ändern des HTTP-Standardports 8080 für die Kommunikation zwischen universellem Druckserver und Citrix Virtual Apps and Desktops-VDAs müssen Sie außerdem auf Computern mit dem

universeller Druckserver den folgenden Registrierungsschlüssel erstellen und die Portnummer ändern:

HKEY_LOCAL_MACHINE\\SOFTWARE\\Policies\\Citrix\\PrintingPolicies
“UpsHttpPort”=DWORD:<portnumber>

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

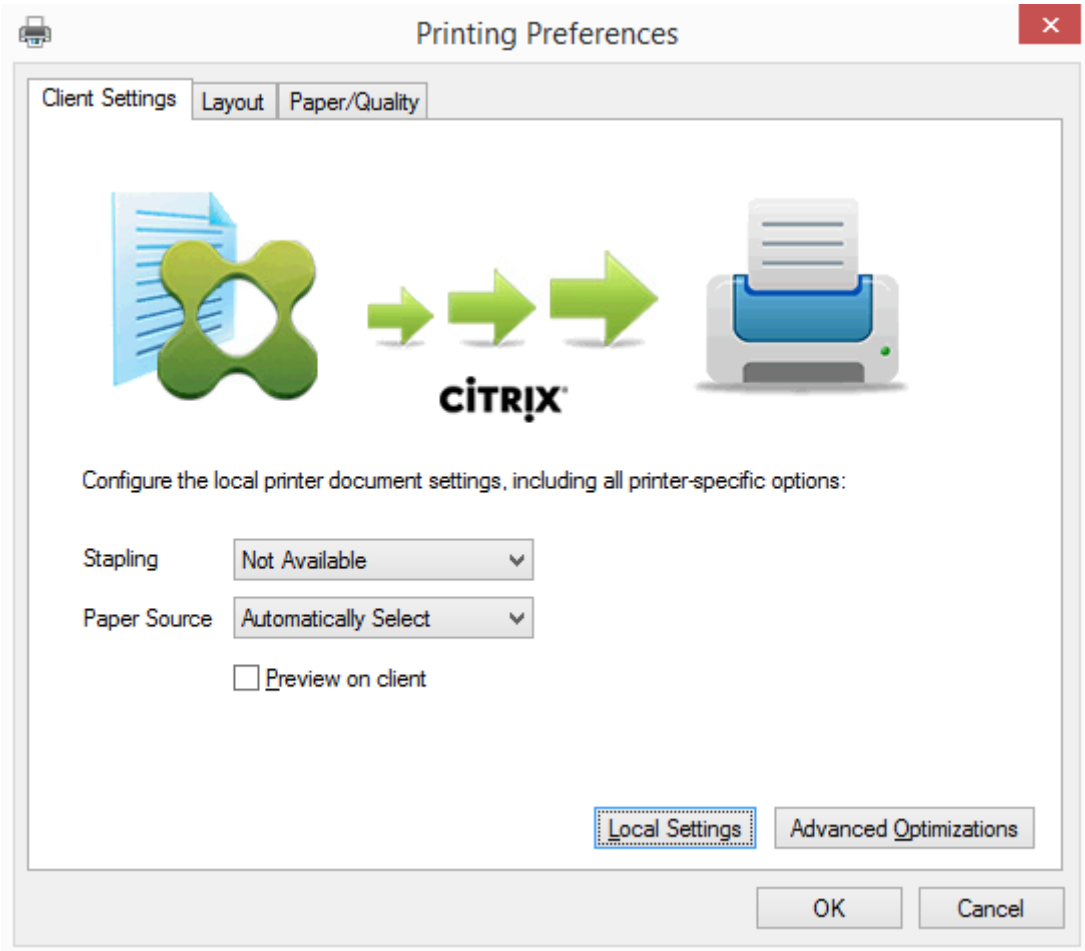
aktiviert, die Komponenten des universellen Druckservers sind installiert und die Richtlinieneinstellungen werden angewendet.

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 Workspace-Apps 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 die Citrix Workspace-App 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

September 21, 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 Multisitzungs-OS-Maschinen mithilfe 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 Multisitzungs-OS-Maschinen 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 Multisitzungs-OS-Maschine 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 Multisitzungs-OS-Maschinen 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 Multisitzungs-OS-Maschine 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 Multisitzungs-OS-Maschine hinzugefügt werden)	Netzwerkdruckmodell	UAC aktiviert: Druckserver > Systemsteuerung; UAC deaktiviert: Druckserver > Systemsteuerung

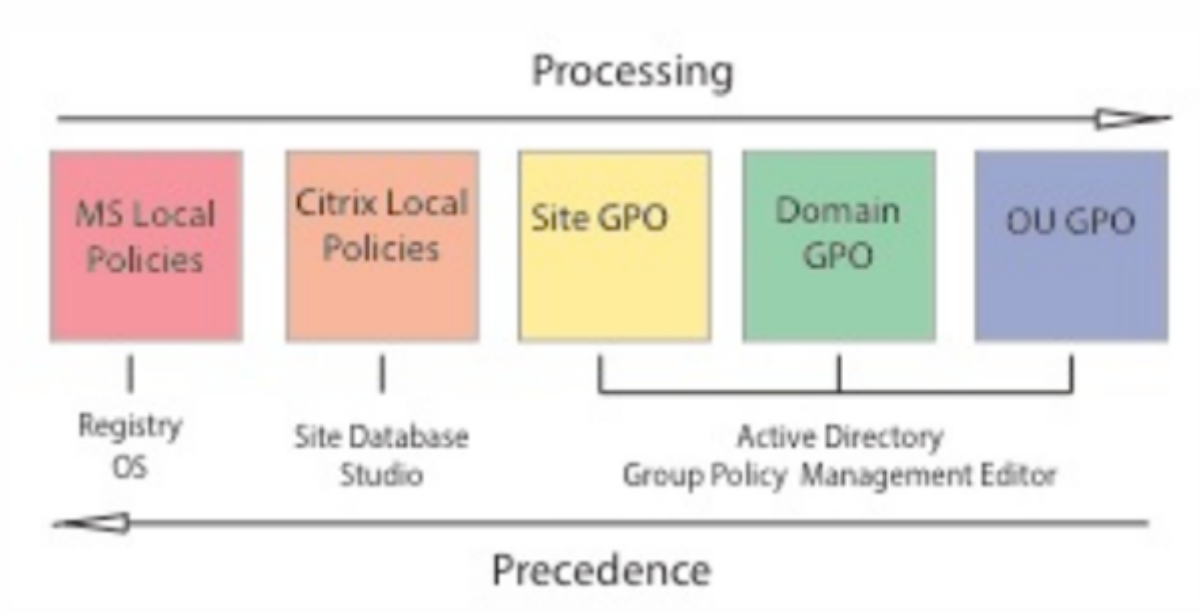
> **Hinweis:**
>
> Druckwarteschlangen für Netzwerkdrucker, die das Netzwerkdruckmodell verwenden, sind privat und können nicht über das System verwaltet werden.

Richtlinien

September 21, 2021

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 außer Kraft setzen.

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 der Citrix Workspace-App 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

March 15, 2022

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.

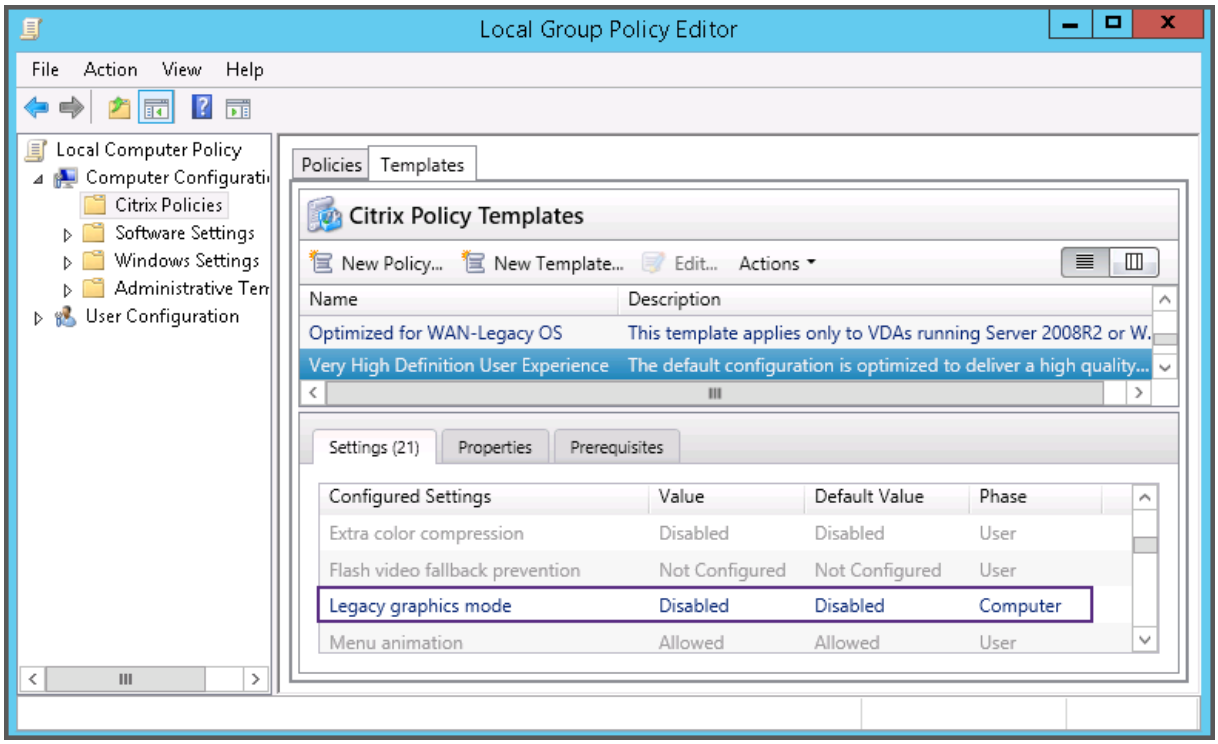
Sie können die Suche verfeinern, indem Sie eine bestimmte Produktversion oder Kategorie auswählen. Für eine ungefilterte Suche wählen Sie Alle Einstellungen.

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

April 19, 2024

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.
- Als Referenz zum leichteren Vergleich von 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.

Überlegungen zur Erstellung von Richtlinien auf der Basis von Vorlagen finden Sie im Knowledge Center-Artikel CTX202330. Um das PDF herunterzuladen, melden Sie sich mit Ihren Zugangsdaten an.

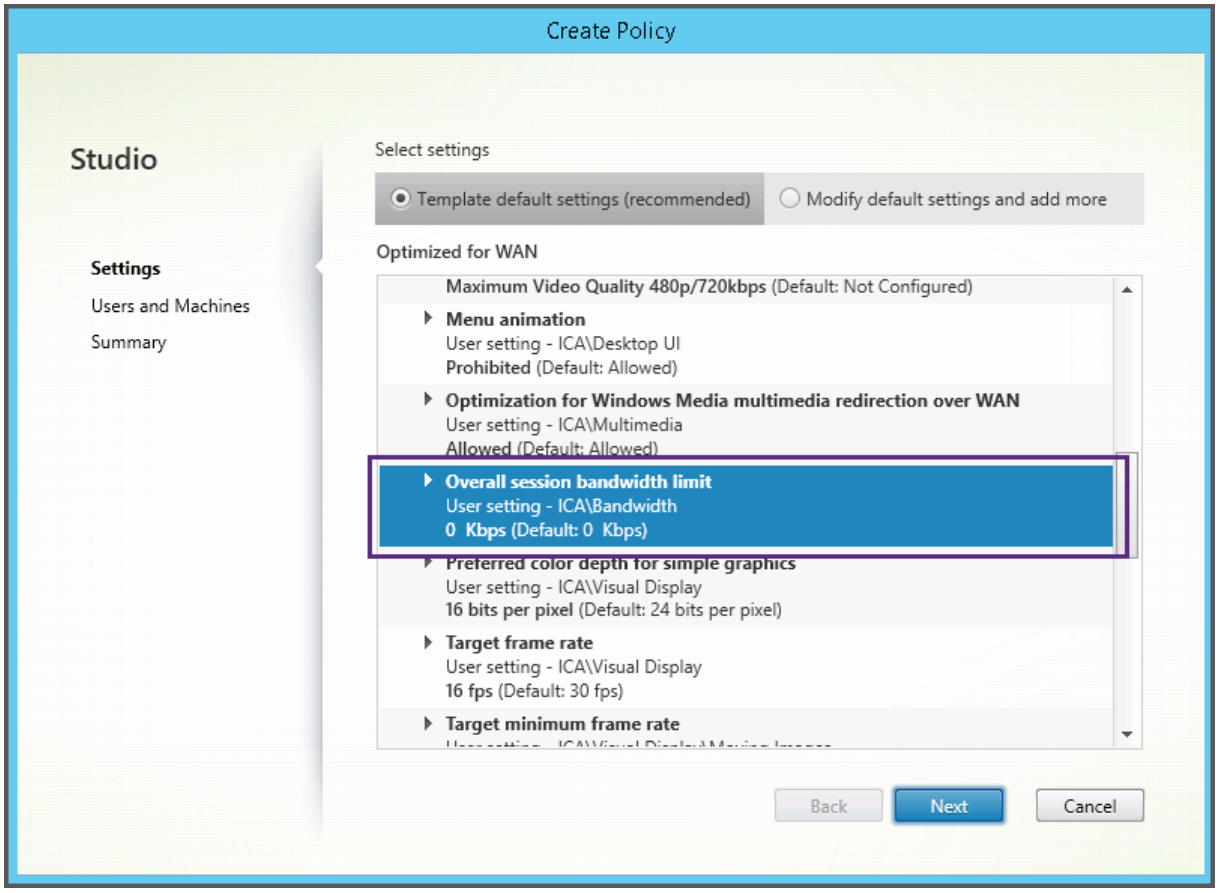
Integrierte Citrix Vorlagen

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 zum Komprimieren 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 Citrix Virtual Desktops 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 Citrix Virtual Apps and Desktops standardmäßig aktivierten Features zu minimieren. Die in dieser Vorlage enthaltenen Einstellungen deaktivieren auf Benutzergeräten den Zugriff auf Drucker, Zwischenablage, Peripheriegeräte, Laufwerkzuordnung, Portumleitung und Flash-Beschleunigung. 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, für einige Einstellungen gibt es jedoch keinen empfohlenen Wert. Ein Beispiel ist 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, sind ggf. die Vorlagenversionen für ältere Betriebssysteme ("Legacy-OS") zu verwenden.

> **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 Vorlage basierend auf einer Vorlage:

1. Wählen Sie im Navigationsbereich von Studio die Option **Richtlinien**.
2. Wählen Sie die Registerkarte **Vorlagen** und dann die Vorlage, mit der Sie eine 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 alle Einstellungen, die nicht erforderlich sind. 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 Vorlage basierend auf einer Richtlinie:

1. Wählen Sie im Navigationsbereich von Studio die Option **Richtlinien**.
2. Wählen Sie die Registerkarte **Richtlinien** und dann die Richtlinie, mit der Sie die 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 alle Einstellungen, die nicht erforderlich sind. Geben Sie einen Namen und eine Beschreibung für die Vorlage ein und klicken Sie auf **Fertig stellen**.

Importieren einer Vorlage

1. Wählen Sie im Navigationsbereich von Studio die Option **Richtlinien**.
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 Navigationsbereich von Studio die Option **Richtlinien**.
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

Gehen 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**.

Aufgabe	Anweisung
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 Citrix Virtual Apps and Desktops-Sitedatenbank. Richtlinienvorlagen werden daher über Windows-Administratorrechte und nicht über die Rollen und Geltungsbereiche der delegierten Site-Administration gesteuert.

Ein Administrator mit Lesezugriff für die Site kann so zum Beispiel Vorlagen erstellen. 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

September 21, 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"auswählen. 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.
NetScaler SD-WAN	Gibt an, ob eine Benutzersitzung über Netscaler SD-WAN gestartet wird. Hinweis: Sie können einer Richtlinie nur eine Netscaler SD-WAN-Zuweisung hinzufügen.
Client-IP-Adresse	IP-Adresse des Benutzergeräts, das für die Verbindung mit 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 **Hinweis:** Die Filteroptionen “Privater Desktop” und “Freigegebener Desktop”sind nur für Citrix Virtual Apps and Desktops 7.x verfügbar. Weitere Informationen finden Sie unter CTX219153.
Organisationseinheit	Organisationseinheit
Tag	Tags **Hinweis:** Wenden Sie diese Richtlinie auf alle getaggten Maschinen an. Beachten Sie, dass Anwendungstags nicht enthalten sind.
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 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

Gehen 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.

Aufgabe	Anweisung
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. Wenn Sie einer Richtlinie mehr als einen Filter hinzufügen, müssen alle Filterbedingungen erfüllt sein, damit die Richtlinie angewendet werden kann.
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

January 8, 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 VDA für Einzelsitzungs-OS eine Verbindung mit einem VDA für Multisitzungs-OS herstellt, ist die Wirkung der Citrix Richtlinien auf den VDA für Einzelsitzungs-OS die gleiche wie bei einem 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 Maschine mit dem VDA für Einzelsitzungs-OS 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

September 21, 2021

Die folgenden Tabellen enthalten Richtlinieneinstellungen, die Standardeinstellungen und die VDA-Versionen, für die sie gelten.

ICA

Name	Standardeinstellung	VDA
Adaptiver Transport	Aus; Verwenden, wenn bevorzugt	VDA 7.13 –7.15; VDA 7.16 bis aktuelle Version
Clientzwischenablagenumleitung	Zugelassen	Alle VDA-Versionen
Desktop starten	Nicht zugelassen	VDA für Multisitzungs-OS 7 bis aktuelle Version
ICA-Listenerportnummer	1494	Alle VDA-Versionen
Starten nicht-veröffentlichter Programme bei Clientverbindung	Nicht zugelassen	VDA für Multisitzungs-OS 7 bis aktuelle Version
Zum Schreiben in Clientzwischenablage zugelassene Formate	Keine Formate angegeben	VDA 7.6 bis aktuelle Version
Rendezvousprotokoll	Deaktiviert	Gilt nur für HDX-Sitzungen, die über Citrix Cloud erstellt wurden.
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

Name	Standardeinstellung	VDA
Tabletmodus ein/aus	Aktiviert	VDA 7.16 bis aktuelle Version; bei VDA 7.14 und 7.15 LTSR müssen Sie diese Einstellung in der Registrierung konfigurieren.
Positivliste virtueller Kanäle	Deaktiviert	VDA 1912

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 Multisitzungs-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
Audio über UDP - Real-time Transport	Zugelassen	Alle VDA-Versionen
Automatische Wiederverbindung von Clients	Zugelassen	Alle VDA-Versionen

Name	Standardeinstellung	VDA
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
Timeout beim automatischen Wiederverbinden von Clients	120 Sekunden	VDA 7.13 bis aktuelle Version
UI-Transparenzstufe während Wiederverbindung	80 %	VDA 7.13 bis aktuelle Version

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 Multisitzungs-OS 7 bis aktuelle Version, VDA für Einzelsitzungs-OS 7 bis aktuelle Version
Bandbreitenlimit für Client-USB-Geräteumleitung (Prozent)	0	VDA 5.5, 5.6 FP1, VDA für Multisitzungs-OS 7 bis aktuelle Version, VDA für Einzelsitzungs-OS 7 bis aktuelle Version
Bandbreitenlimit für Zwischenablagenumleitung	0 KBit/s	Alle VDA-Versionen
Bandbreitenlimit für Zwischenablagenumleitung (Prozent)	0	Alle VDA-Versionen

Name	Standardeinstellung	VDA
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.
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 Multisitzungs-OS 7 und VDA für Einzelsitzungs-OS 7 bis aktuelle Version, VDA für Multisitzungs-OS und VDA für Einzelsitzungs-OS
Bandbreitenlimit für HDX MediaStream-Multimediabeschleunigung (Prozent)	0	VDA 5.5, 5.6 FP1, VDA für Multisitzungs-OS 7 bis aktuelle Version, VDA für Einzelsitzungs-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

Name	Standardeinstellung	VDA
Bandbreitenlimit für TWAIN-Geräteumleitung	0 KBit/s	VDA 5.5, 5.6 FP1, VDA für Multisitzungs-OS 7 bis aktuelle Version, VDA für Einzelsitzungs-OS 7 bis aktuelle Version
Bandbreitenlimit für TWAIN-Geräteumleitung (Prozent)	0	VDA 5.5, 5.6 FP1, VDA für Multisitzungs-OS 7 bis aktuelle Version, VDA für Einzelsitzungs-OS 7 bis aktuelle Version

ICA/bidirektionale Inhaltsumleitung

Name	Standardeinstellung	VDA
Bidirektionale Inhaltsumleitung zulassen	Nicht zugelassen	VDA 7.13 bis aktuelle Version
Für Umleitung an Client zulässige URLs	Leer	VDA 7.13 bis aktuelle Version
Für Umleitung an VDA zulässige URLs	Leer	VDA 7.13 bis aktuelle Version
Bidirektionale Inhaltsumleitung von Client zu Host (VDA) und von Client zu Client		Verwenden der administrativen Gruppenrichtlinienobjektvorlage der Citrix Workspace-App

ICA/Browserinhaltsumleitung

Name	Standardeinstellung	VDA
Browserinhaltsumleitung	Zugelassen	VDA 7.16 bis aktuelle Version
ACL-Konfiguration für die Browserinhaltsumleitung	`https://www.youtube.com/*`	VDA 7.16 bis aktuelle Version
Proxykonfiguration für die Browserinhaltsumleitung	Leer	VDA 7.16 bis aktuelle Version

ICA/Clientsensoren

Name	Standardeinstellung	VDA
Anwendungen können den physischen Standort des Clientgeräts verwenden	Nicht zugelassen	VDA 5.6 FP1, VDA für Multisitzungs-OS 7 bis aktuelle Version, VDA für Einzelsitzungs-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 Einzelsitzungs-OS 7 bis 7.15
Grafikqualität Desktopgestaltung	Mittel	VDA 5.6, VDA für Einzelsitzungs-OS 7 bis 7.15
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
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 Multisitzungs-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 Multisitzungs-OS 7 bis aktuelle Version
Clientlaufwerksbuchstaben erhalten	Deaktiviert	VDA 5, 5.5, 5.6 FP1, VDA für Single-Session OS 7 bis aktuelle Version
Schreibgeschützter Zugriff auf Clientlaufwerke	Deaktiviert	VDA 5.5, 5.6 FP1, VDA für Multisitzungs-OS 7 bis aktuelle Version, VDA für Einzelsitzungs-OS 7 bis aktuelle Version
Umleitung spezieller Ordner	Zugelassen	Nur Webinterface-Bereitstellungen; VDA für Multisitzungs-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 Single-Session 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 Multisitzungs-OS 7 bis aktuelle Version, VDA für Einzelsitzungs-OS 7 bis aktuelle Version
Bildzwischenspeicherung	Aktiviert	VDA 5.5, 5.6 FP1, VDA für Multisitzungs-OS 7 bis aktuelle Version, VDA für Einzelsitzungs-OS 7 bis aktuelle Version
Legacygrafikmodus	Deaktiviert	VDA für Multisitzungs-OS 7 bis aktuelle Version, VDA für Einzelsitzungs-OS 7 bis aktuelle Version
Maximal zugelassene Farbtiefe	32 Bit pro Pixel	Alle VDA-Versionen
Benutzer beim Herabsetzen des Anzeigemodus benachrichtigen	Deaktiviert	VDA für Multisitzungs-OS 7 bis aktuelle Version
Optimierung für 3D-Grafikworkload	Deaktiviert	VDA 7.17 bis aktuelle Version
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 Kbit/s	VDA für Multisitzungs-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 Multisitzungs-OS 7 bis aktuelle Version, VDA für Einzelsitzungs-OS 7 bis aktuelle Version
URL-Umleitungssperrliste	Keine Sites angegeben	VDA für Multisitzungs-OS 7 bis aktuelle Version, VDA für Einzelsitzungs-OS 7 bis aktuelle Version

Name	Standardeinstellung	VDA
URL-Umleitungspositivliste	Keine Sites angegeben	VDA für Multisitzungs-OS 7 bis aktuelle Version, VDA für Einzelsitzungs-OS 7 bis aktuelle Version

ICA/Mobilerfahrung

Name	Standardeinstellung	VDA
Automatische Anzeige der Tastatur	Nicht zugelassen	VDA 5.6 FP1, VDA für Multisitzungs-OS 7 bis aktuelle Version, VDA für Einzelsitzungs-OS 7 bis aktuelle Version
Für Fingereingabe optimierten Desktop starten	Zugelassen	VDA 5.6 FP1, VDA für Multisitzungs-OS 7 bis aktuelle Version, VDA für Einzelsitzungs-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 Multisitzungs-OS 7 bis aktuelle Version, VDA für Einzelsitzungs-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 Multisitzungs-OS 7 bis aktuelle Version, VDA für Einzelsitzungs-OS 7 bis aktuelle Version
Microsoft Teams-Umleitung	Zugelassen	VDA für Multisitzungs-OS 1906 bis aktuelle Version, VDA für Einzelsitzungs-OS 1906 bis aktuelle Version
Multimediakonferenzen	Zugelassen	Alle VDA-Versionen
Optimierung von Windows Media-Multimediaumleitung über WAN	Zugelassen	VDA für Multisitzungs-OS 7 bis aktuelle Version, VDA für Einzelsitzungs-OS 7 bis aktuelle Version
GPU für die Optimierung von Windows Media-Multimediaumleitung über WAN verwenden	Nicht zugelassen	VDA für Multisitzungs-OS 7 bis aktuelle Version, VDA für Einzelsitzungs-OS 7 bis aktuelle Version
Verhindern von Fallback auf Windows Media	Nicht konfiguriert	VDA 7.6 FP3 bis aktuelle Version
Clientseitiger Abruf von Windows Media-Inhalten	Zugelassen	VDA für Multisitzungs-OS 7 bis aktuelle Version, VDA für Einzelsitzungs-OS 7 bis aktuelle Version
Windows Media-Umleitung	Zugelassen	Alle VDA-Versionen
Windows Media-Umleitungspuffergröße	5 Sekunden	VDA 5, 5.5, 5.6 FP1 bis aktuelle Version
Verwendung von Windows Media-Umleitungspuffergröße	Deaktiviert	VDA 5, 5.5, 5.6 FP1 bis aktuelle Version

ICA/Multistreamverbindungen

Name	Standardeinstellung	VDA
Audio über UDP	Zugelassen	VDA für Multisitzungs-OS 7 bis aktuelle Version

Name	Standardeinstellung	VDA
Audio-UDP-Portbereich	16500, 16509	VDA 5.5, 5.6 FP1, VDA für Multisitzungs-OS 7 bis aktuelle Version, VDA für Einzelsitzungs-OS 7 bis aktuelle Version
Multiportrichtlinie	Primärer Port (2598) hat hohe Priorität	VDA 5.5, 5.6 FP1, VDA für Multisitzungs-OS 7 bis aktuelle Version, VDA für Einzelsitzungs-OS 7 bis aktuelle Version
Multistreamcomputereinstellung	Deaktiviert	VDA 5.5, 5.6 FP1, VDA für Multisitzungs-OS 7 bis aktuelle Version, VDA für Einzelsitzungs-OS 7 bis aktuelle Version
Multistreambenutzereinstellung	Deaktiviert	VDA 5.5, 5.6 FP1, VDA für Multisitzungs-OS 7 bis aktuelle Version, VDA für Einzelsitzungs-OS 7 bis aktuelle Version
Einstellung für die Zuweisung virtueller Multistreamkanäle	Informationen zur Streamzuweisung finden Sie unter Einstellungen für die Zuweisung virtueller Multistreamkanäle.	VDA 1912

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.

Name	Standardeinstellung	VDA
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
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	VDA 5.6
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

Name	Standardeinstellung	VDA
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
Universelles Drucken - Bildkomprimierungslimit	Optimale Qualität (verlustfreie Komprimierung)	Alle VDA-Versionen
Universelles Drucken - Optimierungsstandards	Bildkomprimierung: Gewünschte Bildqualität = Standardqualität, Heavyweight-Komprimierung aktivieren = Falsch; Bild- und Schriftartcaching: Zwischenspeichern eingebetteter Bilder zulassen = Wahr; Nicht-Administratoren können diese Einstellungen ändern = Falsch;	Alle VDA-Versionen
Universelles Drucken - Vorschaueinstellung	Druckvorschau für automatisch erstellte oder generische universelle Drucker nicht verwenden	Alle VDA-Versionen

Name	Standardeinstellung	VDA
Universelles Drucken - Druckqualitätslimit	Kein Limit	Alle VDA-Versionen

ICA/Sicherheit

Name	Standardeinstellung	VDA
SecureICA-Mindestverschlüsselungsgrad	Standard	VDA für Multisitzungs-OS 7 bis aktuelle Version

ICA/Serverlimits

Name	Standardeinstellung	VDA
Serverleerlauf-Zeitintervall	0 Millisekunden	VDA für Multisitzungs-OS 7 bis aktuelle Version

ICA/Sitzungslimits

Name	Standardeinstellung	VDA
Timer für getrennte Sitzung	Deaktiviert	VDA 5, 5.5, 5.6 FP1, VDA für Single-Session OS 7 bis aktuelle Version
Getrennte Sitzungen - Timerintervall	1440 Minuten	VDA 5, 5.5, 5.6 FP1, VDA für Single-Session OS 7 bis aktuelle Version
Sitzungsverbindungstimer	Deaktiviert	VDA 5, 5.5, 5.6 FP1, VDA für Single-Session OS 7 bis aktuelle Version
Sitzungsverbindung - Timerintervall	1440 Minuten	VDA 5, 5.5, 5.6 FP1, VDA für Single-Session OS 7 bis aktuelle Version

Name	Standardeinstellung	VDA
Sitzungsleerlauftimer	Aktiviert	VDA 5, 5.5, 5.6 FP1, VDA für Single-Session OS 7 bis aktuelle Version
Sitzungsleerlauf - Timerintervall	1440 Minuten	VDA 5, 5.5, 5.6 FP1, VDA für Single-Session 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 Multisitzungs-OS 7 bis aktuelle Version
Wiederherstellen der Zeitzone für Einzelsitzungs-OS beim Trennen oder Abmelden der Sitzung	Aktiviert	Aktuelle VDA-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 Multisitzungs-OS 7 bis aktuelle Version, VDA für Einzelsitzungs-OS 7 bis aktuelle Version
TWAIN-Komprimierungsgrad	Mittel	VDA 5.5, 5.6 FP1, VDA für Multisitzungs-OS 7 bis aktuelle Version, VDA für Einzelsitzungs-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); standardmäßig 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 Multisitzungs-OS 7 bis aktuelle Version, VDA für Einzelsitzungs-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

Name	Standardeinstellung	VDA
Bildqualität	Mittel	VDA für Multisitzungs-OS 7 bis aktuelle Version, VDA für Einzelsitzungs-OS 7 bis aktuelle Version

ICA/Visuelle Anzeige/Bewegtbilder

Name	Standardeinstellung	VDA
Mindestbildqualität	Normal	VDA 5.5, 5.6 FP1, VDA für Multisitzungs-OS 7 bis aktuelle Version, VDA für Einzelsitzungs-OS 7 bis aktuelle Version
Bewegtbildkomprimierung	Aktiviert	VDA 5.5, 5.6 FP1, VDA für Multisitzungs-OS 7 bis aktuelle Version, VDA für Einzelsitzungs-OS 7 bis aktuelle Version
Grad der progressiven Komprimierung	–	VDA 5.5, 5.6 FP1, VDA für Multisitzungs-OS 7 bis aktuelle Version, VDA für Einzelsitzungs-OS 7 bis aktuelle Version
Schwellenwert für progressive Komprimierung	2147483647 Kbit/s	VDA 5.5, 5.6 FP1, VDA für Multisitzungs-OS 7 bis aktuelle Version, VDA für Einzelsitzungs-OS 7 bis aktuelle Version
Mindestframeratesollwert	10 f/s	VDA 5.5, 5.6 FP1, VDA für Multisitzungs-OS 7 bis aktuelle Version, VDA für Einzelsitzungs-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 Multisitzungs-OS 7 bis aktuelle Version, VDA für Einzelsitzungs-OS 7 bis aktuelle Version
WebSockets-Portnummer	8008	VDA für Multisitzungs-OS 7 bis aktuelle Version, VDA für Einzelsitzungs-OS 7 bis aktuelle Version
Vertrauenswürdige WebSockets-Ursprungsserverliste	Bei Verwendung des Platzhalters * wird allen Receiver für Web-URLs vertraut.	VDA für Multisitzungs-OS 7 bis aktuelle Version, VDA für Einzelsitzungs-OS 7 bis aktuelle Version

Lastverwaltung

Name	Standardeinstellung	VDA
Toleranzwert für gleichzeitige Anmeldungen	2	VDA für Multisitzungs-OS 7 bis aktuelle Version
CPU-Nutzung	Deaktiviert	VDA für Multisitzungs-OS 7 bis aktuelle Version

Name	Standardeinstellung	VDA
CPU-Nutzung ausschließlich Prozesspriorität	Unter normal oder niedrig	VDA für Multisitzungs-OS 7 bis aktuelle Version
Datenträgernutzung	Deaktiviert	VDA für Multisitzungs-OS 7 bis aktuelle Version
Sitzungshöchstanzahl	250	VDA für Multisitzungs-OS 7 bis aktuelle Version
Speichernutzung	Deaktiviert	VDA für Multisitzungs-OS 7 bis aktuelle Version
Speichernutzung - Ausgangslast	Nulllast: 768 MB	VDA für Multisitzungs-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

Name	Standardeinstellung	VDA
Pfad zu Benutzerspeicher	Windows	Alle VDA-Versionen
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

Name	Standardeinstellung	VDA
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

Name	Standardeinstellung	VDA
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

Name	Standardeinstellung	VDA
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
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
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

Name	Standardeinstellung	VDA
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
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 Multisitzungs-OS 7 bis aktuelle Version, VDA für Einzelsitzungs-OS 7 bis aktuelle Version

Benutzerpersonalisierungslayer

Name	Standardeinstellung	VDA
Repositorypfad für Benutzerlayer	Deaktiviert. Kein Pfad angegeben.	VDA 19.12 und höher
Größe von Benutzerlayer in GB	0 GB (Mindestgröße 10 GB als Standardwert)	VDA 19.12 oder höher

Virtual Delivery Agent

Name	Standardeinstellung	VDA
IPv6-Netzwerkmaske für Controllerregistrierung	Keine Netzwerkmaske angegeben.	VDA für Multisitzungs-OS 7 bis aktuelle Version, VDA für Einzelsitzungs-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 Multisitzungs-OS 7 bis aktuelle Version, VDA für Einzelsitzungs-OS 7 bis aktuelle Version
Nur IPv6-Controllerregistrierung verwenden	Deaktiviert	VDA für Multisitzungs-OS 7 bis aktuelle Version, VDA für Einzelsitzungs-OS 7 bis aktuelle Version
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

February 19, 2020

Richtlinien enthalten Einstellungen, die gelten, wenn die Richtlinie angewendet wird. In diesem Abschnitt wird auch angegeben, 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.

Eine vollständige Liste aller Richtlinieneinstellungen ist im CHM-Format (Compiled HTML) und im CSV-Format verfügbar. Diese Dateien sind im Ordner `\program files\citrix\grouppolicy` auf dem Server, auf dem der Broker (Delivery Controller) installiert ist. Sie können die aktuelle Version der Richtlinieneinstellungen auch hier herunterladen.

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)
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)

Beschränken der Bandbreite	Richtlinieneinstellung
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
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; TWAIN-Umleitung
Steuern, ob die USB-Geräte in einer Sitzung verfügbar sind	Client-USB-Geräteumleitung und Regeln für die Client-USB-Geräteumleitung

Aufgabe	Richtlinieneinstellung
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

> **Wichtig:**
>
> Die Flash-Richtlinie bleibt nur bestehen, damit Kunden mit älteren VDAs, die neuere Controller verwenden (z. B. Controller der Version 1912), Flash weiterhin einsetzen können. Diese VDA-Version unterstützt Flash nicht.

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

Aufgabe	Richtlinieneinstellung
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
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

Aufgabe	Richtlinieneinstellung
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"

June 26, 2023

Adaptiver Transport

Diese Einstellung steuert den Datentransport über EDT als primäre Methode mit Fallback auf TCP.

Standardmäßig ist der adaptive Transport aktiviert (**Bevorzugt**) und EDT wird, sofern möglich, mit Fallback auf TCP verwendet. Wenn er deaktiviert wurde und Sie ihn aktivieren möchten, gehen Sie folgendermaßen vor.

1. Aktivieren Sie in Studio die Richtlinieneinstellung "Adaptiver HDX-Transport". 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 Sie diese Einstellung auf “Zugelassen”festgelegt haben, konfigurieren Sie die maximal zulässige Bandbreite, die die Zwischenablage bei einer Clientverbindung belegen darf. Verwenden Sie die Einstellung **Bandbreitenlimit für Zwischenablageumleitung** 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 sowie Citrix Virtual Apps and Desktops vordefiniert:

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8
- CFX_FILE

Das HTML-Format ist standardmäßig deaktiviert. Aktivieren des Features

- Stellen Sie sicher, dass **Clientzwischenablagenumleitung** auf **Zugelassen** festgelegt ist.
- Stellen Sie sicher, dass **Schreiben in Clientzwischenablage einschränken** auf **Aktiviert** festgelegt ist.
- Fügen Sie **Zum Schreiben in Clientzwischenablage zugelassene Formate** einen Eintrag für **CF_HTML** (sowie alle anderen Formate, die unterstützt werden sollen) hinzu.

Sie können weitere benutzerdefinierte Formate hinzufügen. 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.

> **Hinweis**
>
> Durch das Aktivieren der Unterstützung für das HTML-Zwischenablagenkopieren (CF_HTML) werden alle Skripts 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.

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 sowie Citrix Virtual Apps and Desktops vordefiniert:

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8

Das HTML-Format ist standardmäßig deaktiviert. Aktivieren des Features

- Stellen Sie sicher, dass **Clientzwischenablagenumleitung** auf **Zugelassen** festgelegt ist.
- Stellen Sie sicher, dass **Schreiben in Sitzungszwischenablage einschränken** auf **Aktiviert** festgelegt ist.
- Fügen Sie **Zum Schreiben in Sitzungszwischenablage zugelassene Formate** einen Eintrag für **CF_HTML** (sowie alle anderen Formate, die unterstützt werden sollen) hinzu.

Sie können weitere benutzerdefinierte Formate hinzufügen. 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.

> **Hinweis**
>
> Durch das Aktivieren der Unterstützung für das HTML-Zwischenablagenkopieren (CF_HTML) werden alle Skripts 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 aus-

führen.

Desktopstarts

Mit dieser Einstellung legen Sie fest, ob Benutzer ohne Administratorrechte in der Gruppe der Benutzer mit direktem Zugriff eines VDAs 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.

Die 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

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 jeder Citrix Workspace-App-Instanz und jedem Plug-In ändern, die bzw. das eine Verbindung zu diesem Server herstellt.

Tastatur und Eingabemethoden-Editor (IME)

> **Hinweis:**
>
> Diese Richtlinie gilt nur ab 1912 LTSR CU2.

Diese Einstellung aktiviert und deaktiviert die dynamische Tastaturlayoutsynchronisierung, den Eingabemethoden-Editor (IME) sowie die Unicode-Tastaturlayoutzuordnung und blendet die Benachrichtigung beim Tastaturlayoutwechsel ein und aus.

1. Wählen Sie in Studio **Tastatur und IME**.
2. Wählen Sie **Client-Tastaturlayoutsynchronisierung und Verbesserung des IME**, um die dynamische Tastaturlayoutsynchronisierung und den generischen IME im VDA zu steuern. Sie können Folgendes konfigurieren:

   Deaktiviert: Deaktiviert die dynamische Tastaturlayoutsynchronisierung und den generischen Client-Eingabemethoden-Editor (IME).

   Dynamische Client-Tastaturlayoutsynchronisierung unterstützen: Aktiviert die dynamische Tastaturlayoutsynchronisierung.

   Client-Tastaturlayoutsynchronisierung und Verbesserung des IME: Aktiviert die dynamische Tastaturlayoutsynchronisierung und den generischen IME.
3. Wählen Sie **Unicode-Tastaturlayoutzuordnung aktivieren**, um die Unicode-Tastaturlayoutzuordnung zu aktivieren oder zu deaktivieren.
4. Wählen Sie **Meldungsfeld für Tastaturlayoutwechsel ausblenden**, um die Anzeige der Meldung über die Synchronisierung des Tastaturlayouts beim Wechsel des Clienttastaturlayouts durch den Benutzer zu steuern.

Standardeinstellungen

- **Client-Tastaturlayoutsynchronisierung und Verbesserung des IME**
  - Unter Windows Server 2016 und Windows Server 2019 deaktiviert.
  - Unterstützt die dynamische Synchronisierung des Clienttastaturlayouts und die IME-Verbesserung in Windows Server 2012 und Windows 2010.
- **Unicode-Tastaturlayoutzuordnung deaktivieren**
- **Meldungsfeld für Tastaturlayoutwechsel anzeigen**

Diese Richtlinie ersetzt die im Abschnitt **Beschreibung** der Richtlinieneinstellungen aufgeführten Registrierungseinstellungen.

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 Tren-

nen von Clientsitzungen abgewartet wird.

Durch diese Einstellung wird auch die Zeitdauer der Benutzerabmeldung vom Server erhöht.

Rendezvousprotokoll

Mit dieser Einstellung wird die Proxyvergabe für HDX-Sitzungen bei Verwendung von Citrix Gateway Service geändert. Ist die Option aktiviert, wird der HDX-Datenverkehr nicht mehr über den Citrix Cloud Connector geleitet. Stattdessen stellt der VDA eine ausgehende Verbindung direkt mit Citrix Gateway Service her (wodurch die Cloud Connector-Skalierbarkeit verbessert wird).

> **Wichtig:**
>
> Dieses Feature wird durch eine Option in Citrix Cloud und eine HDX-Richtlinieneinstellung gesteuert. In Citrix Cloud ist es standardmäßig aktiviert und in der HDX-Einstellung standardmäßig deaktiviert. Die HDX-Einstellung wirkt sich nur auf HDX-Sitzungen aus, die über Citrix Gateway Service eingerichtet wurden. Sitzungen, die direkt zwischen Client und VDA oder über ein On-Premises Citrix Gateway eingerichtet wurden, sind von dieser Einstellung nicht betroffen.

Weitere Informationen finden Sie unter Rendezvous-Protokoll.

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.

Einstellungen der Richtlinie “Tabletmodus-Umschaltung”

Die Tabletmodus-Umschaltung optimiert das Aussehen und Verhalten von Store-Apps, Win32-Apps und der Windows-Shell auf dem VDA. Dazu wird der virtuelle Desktop automatisch in den Tabletmodus umgeschaltet, wenn Verbindungen von kleinformatigen Geräten (Smartphones und Tablets o. Ä.) oder anderen Geräten mit Touchscreen hergestellt werden.

Wenn diese Richtlinie deaktiviert ist, verbleibt der VDA unabhängig vom Clienttyp in dem vom Benutzer festgelegten Modus.

Einstellungen der Richtlinie "Automatische Wiederverbindung von Clients"

February 6, 2020

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 bzw. ab Citrix Workspace-App 1808 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 ändern 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 Workspace-App-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. Die Citrix Workspace-App versucht, die Verbindung mit der Sitzung wiederherzustellen, bis die Wiederverbindung erfolgreich war oder der Benutzer die Wiederverbindung abbricht.

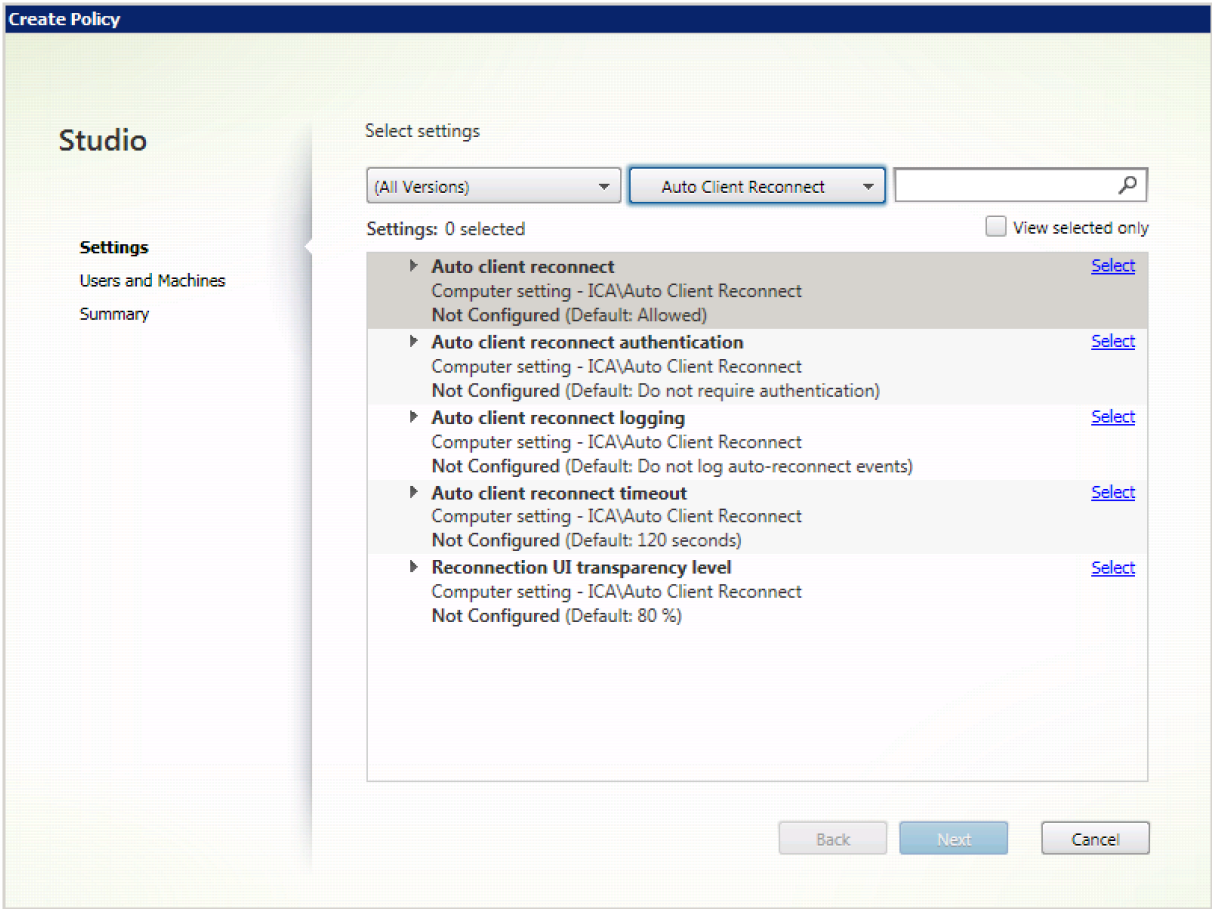
Wenn die automatische Wiederverbindung zugelassen ist, versucht die Citrix Workspace-App bei Benutzersitzungen eine festgelegte Zeit lang, die Verbindung mit der Sitzung wiederherzustellen, bis

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 die Citrix Workspace-App gesendet. Wenn diese Einstellung konfiguriert ist, werden keine Cookies

verwendet. Stattdessen wird ein Dialogfeld mit der Aufforderung zur Eingabe der Anmeldeinformationen angezeigt, wenn die Citrix Workspace-App 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. Wählen Sie **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. Wählen Sie **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. Wählen Sie **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. Wählen Sie **OK**.

Einstellungen der Richtlinie "Audio"

February 6, 2020

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 Maschinen mit Windows-Multisitzungs-OS.

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.

  An das Benutzergerät gesendete Audiodaten werden bis auf 64 KBit/s komprimiert. Die 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 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 Maschinen mit Windows-Multisitzungs-OS 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. Die Benutzer können die Warnung in der Citrix Workspace-App deaktivieren.

Auf Maschinen mit Windows-Multisitzungs-OS 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”

March 15, 2022

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 Richtlinieneinstellungen Multistream 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 (niedrigerer Wert) 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 (niedrigerer Wert) 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 (niedrigerer Wert) 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 (niedrigerer Wert) 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 (niedrigerer Wert) 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 (niedrigerer Wert) 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 (niedrigerer Wert) 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 (niedrigerer Wert) 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 und für die Einstellung Bandbreitenlimit für Dateiumleitung (Prozent) einen Wert angeben, wird die restriktivere Einstellung (niedrigerer 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 (niedrigerer Wert) 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 und für die Einstellung Bandbreitenlimit für HDX MediaStream-Multimediabeschleunigung (Prozent) einen Wert angeben, wird die restriktivere Einstellung (niedrigerer Wert) 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 (niedrigerer Wert) 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 (niedrigerer Wert) 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 Reg-

istrierung).

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 (niedrigerer Wert) 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 (niedrigerer Wert) 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 (niedrigerer Wert) 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 (niedrigerer Wert) 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

April 19, 2024

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.

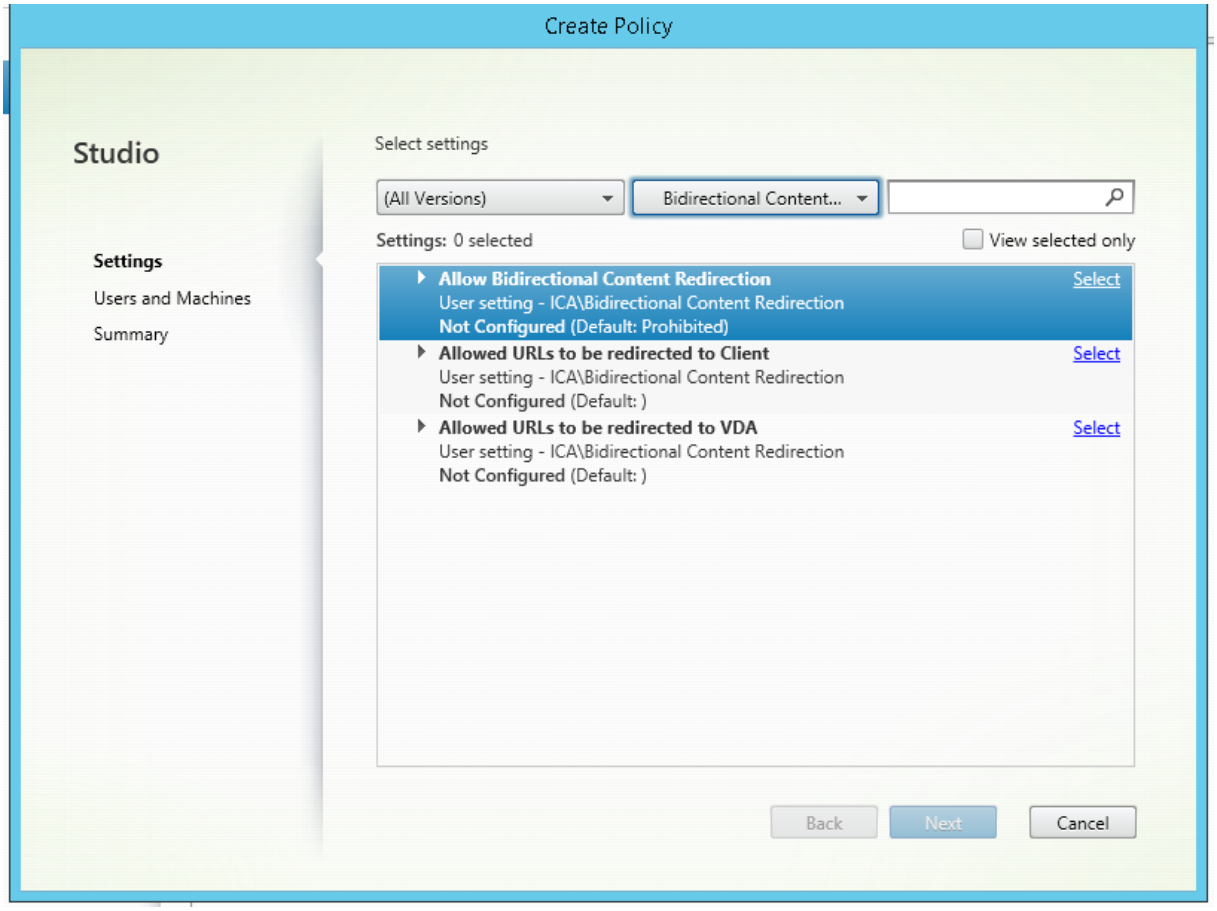
Ein Semikolon (;) ist das Trennzeichen. Ein Sternchen (*) kann als Platzhalter verwendet werden. Beispiel:

Aktivieren der bidirektionalen Inhaltsumleitung

Wenn Sie URLs einschließen, können Sie eine URL angeben oder eine durch Semikolon getrennte Liste von URLs. Sie können ein Sternchen (*) als Platzhalter im Domänennamen verwenden. Beispiel:

http://*.citrix.com; http://www.google.com

1. Starten Sie Citrix Studio.
2. Öffnen Sie die Richtlinie **Bidirektionale Inhaltsumleitung**.
3. Wählen Sie **Bidirektionale Inhaltsumleitung zulassen** und anschließend **Zugelassen** gefolgt von **OK**. Wenn Sie die Option nicht zulassen, können Sie diesen Vorgang nicht abschließen.
4. Wählen Sie **Für Umleitung an Client zulässige URLs** und geben Sie eine URL oder eine URL-Liste an oder übernehmen Sie den Standardwert.
5. Wählen Sie **Für Umleitung an VDA zulässige URLs** und geben Sie eine URL oder eine URL-Liste an oder übernehmen Sie den Standardwert.



Informationen zur Konfiguration der clientseitigen bidirektionalen Inhaltsumleitung in der Citrix Workspace-App finden Sie unter Bidirektionale Inhaltsumleitung in der Dokumentation zur Citrix Workspace-App für Windows.

Kopieren und Einfügen zwischen Sitzung und Client

Zum Konfigurieren der Funktion zum Kopieren und Einfügen zwischen Sitzung und Client legen Sie die folgenden Richtlinien fest:

- "Clientzwischenablagenumleitung"auf "Zugelassen".
- "Schreiben in Clientzwischenablage einschränken", um das Einfügen aller Formate aus der Zwischenablage in den Client einzuschränken.
- "Zum Schreiben in Clientzwischenablage zugelassene Formate", um eine Ausnahme für das Einfügen von Dateien aus der Zwischenablage in den Client festzulegen (verwenden Sie das Format CFX_FILE, um das Feature zuzulassen).
- "Schreiben in Sitzungszwischenablage einschränken", um das Einfügen aller Formate aus der Zwischenablage in die VDA-Sitzung einzuschränken.
- "Zum Schreiben in Sitzungszwischenablage zugelassene Formate", um eine Ausnahme für das

Einfügen von Dateien aus der Zwischenablage in den VDA festzulegen (verwenden Sie das Format CFX_FILE, um das Feature zuzulassen).

Registrieren von Browser-Add-Ons

Für die bidirektionale Inhaltsumleitung ist das Internet Explorer-Browser-Add-On erforderlich.

Sie können das Internet Explorer-Add-On mit den folgenden Befehlen registrieren bzw. seine Registrierung aufheben:

- Registrieren des Internet Explorer-Add-Ons auf einem Clientgerät: <clientinstallationsordner>\redirector.exe /regIE
- Aufheben der Registrierung des Internet Explorer-Add-Ons auf einem Clientgerät: <clientinstallationsordner>\redirector.exe /unregIE
- Registrieren des Internet Explorer-Add-Ons auf einem VDA: <VDAinstallationsordner>\VDARedirector.exe /regIE
- Aufheben der Registrierung des Internet Explorer-Add-Ons auf einem VDA: <VDAinstallationsordner>\VDARedirector.exe /unregIE

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 wird das Internet Explorer-Add-On auf einem VDA für Windows-Multisitzungs-OS registriert.

C:\Programme (x86)\Citrix\System32\VDARedirector.exe /regIE

Richtlinieneinstellungen für die Browserinhaltsumleitung

March 9, 2022

Der Bereich "Webbrowser-Inhaltsumleitung"enthält Richtlinieneinstellungen zum Konfigurieren dieses Features.

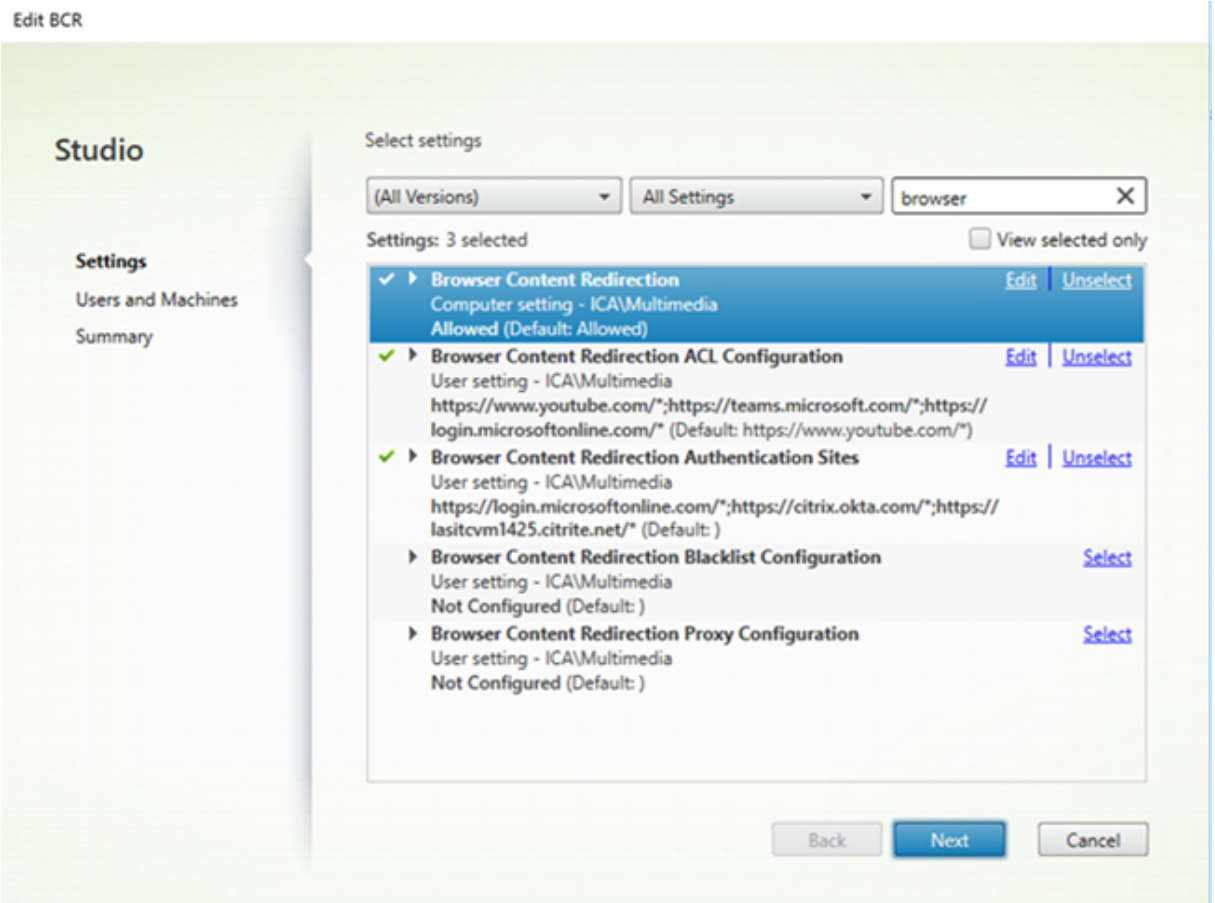
Die Browserinhaltsumleitung steuert und optimiert die Bereitstellung von Browserinhalt (z. B. HTML5) durch Citrix Virtual Apps and Desktops an Benutzer. Es wird nur der sichtbare Browserbereich, in dem Inhalt angezeigt wird, umgeleitet.

Die HTML5-Videoumleitung und die Browserinhaltsumleitung sind unabhängige Features. Die HTML5-Videoumleitungsrichtlinien werden für das Funktionieren des Features nicht benötigt, doch

der Citrix HDX-HTML5-Videoumleitungsdienst wird für die Browserinhaltsumleitung verwendet. Weitere Informationen finden Sie unter Umleitung des Browserinhalts.

Richtlinieneinstellungen:

Die folgenden Richtlinieneinstellungen sind für die Browserinhaltsumleitung in Citrix Studio verfügbar. Diese Richtlinien können mit Registrierungsschlüsseln auf dem VDA außer Kraft gesetzt werden. Registrierungsschlüssel sind allerdings optional.



TLS und Browserinhaltsumleitung

Sie können mit der Browserinhaltsumleitung HTTPS-Websites umleiten. 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.

Umleitung des Browserinhalts

Die Citrix Workspace-App versucht standardmäßig den clientseitigen Abruf und die clientseitige Wiedergabe. Wenn Abruf und Wiedergabe clientseitig fehlschlagen, wird die serverseitige Wiedergabe versucht. Wenn Sie außerdem die Richtlinie "Proxykonfiguration für die Webbrowser-Inhaltsumleitung"aktivieren, versucht die Citrix Workspace-App nur den serverseitigen Abruf und die clientseitige Wiedergabe.

Standardmäßig ist diese Einstellung auf Zugelassen festgelegt.

Einstellung für Webproxyauthentifizierung für die Browserinhaltsumleitung mit serverseitigem Abruf

> **Hinweis:**
>
> Diese Richtlinie ist nur ab Version 1912 CU3 verfügbar.

Mit dieser Einstellung wird der von einem Overlay-Netz kommende HTTP-Datenverkehr über einen downstream platzierten Webproxy geleitet. Dieser Downstreamwebproxy autorisiert und authentifiziert den HTTP-Datenverkehr mit den Domänenanmeldeinformationen des VDA-Benutzers über das Aushandlungsauthentifizierungsschema.

Sie müssen die Browserinhaltsumleitung für den serverseitigen Abruf in der PAC-Datei konfigurieren. Verwenden Sie hierfür die Proxykonfigurationsrichtlinie für die Browserinhaltsumleitung. Geben Sie im PAC-Skript Anweisungen zum Weiterleiten des Overlay-Datenverkehrs über einen Downstreamwebproxy ein. Konfigurieren Sie dann im Downstreamwebproxy das Authentifizieren der VDA-Benutzer über das Aushandlungsauthentifizierungsschema.

Wenn dieser Wert auf **Zugelassen** festgelegt ist, antwortet der Webproxy mit dem Statuscode 407 und einer Aushandlungsauthentifizierungsaufforderung, die den Header **Proxy-Authenticate: Negotiate** enthält. Die Browserinhaltsumleitung verwendet die Domänenanmeldeinformationen des VDA-Benutzers, um ein Kerberos-Dienstticket zu empfangen, das dann in nachfolgenden Anforderungen an den Webproxy enthalten ist.

Wenn dieser Wert auf **Nicht zugelassen** festgelegt ist, leitet die Browserinhaltsumleitung den gesamten TCP-Datenverkehr ungehindert zwischen Overlay-Netz und Webproxy weiter. Das Overlay-Netz authentifiziert sich beim Webproxy über Standardauthentifizierungsangaben oder andere verfügbare Anmeldeinformationen.

Die Standardeinstellung ist "Nicht zugelassen".

Einstellungen der Richtlinie ACL-Konfiguration für die Webbrowser-Inhaltsumleitung

Mit dieser Einstellung können Sie eine Zugriffssteuerungsliste (ACL) mit URLs konfigurieren und festlegen, ob diese die Webbrowser-Inhaltsumleitung verwenden können oder nicht.

Autorisierte URLs sind URLs, deren Inhalt an den Client weitergeleitet wird.

Der Platzhalter * ist zulässig, jedoch nicht im Protokoll- oder Domänenadressteil der URL.

Zulässig: `http://www.xyz.com/index.html`, `https://www.xyz.com/*`, `http://www.xyz.com/*videos*`

Nicht zulässig: `http://*.xyz.com/`

Sie können eine bessere Granularität erzielen, indem Sie Pfade in der URL angeben. Wenn Sie beispielsweise `https://www.xyz.com/sports/index.html` angeben, wird nur die Seite "index.html"umgeleitet.

Standardmäßig ist diese Einstellung folgendermaßen eingestellt: `https://www.youtube.com/*`

Weitere Informationen finden Sie im Knowledge Center-Artikel CTX238236.

Authentifizierungssites für Browserinhaltsumleitung

Verwenden Sie diese Einstellung, um eine Liste von URLs zu konfigurieren. Für über die Browserinhaltsumleitung umgeleitete Websites wird die Liste zum Authentifizieren von Benutzern verwendet. Die Einstellung gibt die URLs an, bei denen die Browserinhaltsumleitung aktiv bleibt, wenn ein Benutzer von einer URL auf der Positivliste wegnavigiert.

Ein typisches Szenario sind Websites, bei denen zur Authentifizierung ein Identitätsanbieter (IdP) verwendet wird. Beispiel: Website `www.xyz.com` muss an den Endpunkt umgeleitet werden aber ein IDP eines Drittanbieters wie z. B. Okta (`www.xyz.okta.com`) erledigt die Authentifizierung. Der Administrator setzt mithilfe der ACL-Konfigurationsrichtlinie für die Browserinhaltsumleitung `www.xyz.com` auf die Positivliste und verwendet dann Authentifizierungswebsites für die Browserinhaltsumleitung, um `www.xyz.okta.com` auf die Positivliste zu setzen.

Weitere Informationen finden Sie im Knowledge Center-Artikel CTX238236.

Sperrlistenkonfiguration für die Browserinhaltsumleitung

Diese Einstellung funktioniert zusammen mit der Einstellung "ACL-Konfiguration für die Browserinhaltsumleitung". Wenn für die Einstellung "ACL-Konfiguration für die Browserinhaltsumleitung"und "Sperrlistenkonfiguration für die Browserinhaltsumleitung"URLs festgelegt wurden, hat die Sperrlistenkonfiguration Vorrang und der Browserinhalt der URL wird nicht umgeleitet.

Nicht berechtigte URLs: URLs auf der Sperrliste, deren Browserinhalt nicht an den Client weitergeleitet, sondern auf dem Server wiedergegeben wird.

Der Platzhalter * ist zulässig, jedoch nicht im Protokoll- oder Domänenadressteil der URL.

Zulässig: `http://www.xyz.com/index.html`, `https://www.xyz.com/*`, `http://www.xyz.com/*videos*`

Nicht zulässig: `http://*.xyz.com/`

Sie können eine bessere Granularität erzielen, indem Sie Pfade in der URL angeben. Wenn Sie beispielsweise `https://www.xyz.com/sports/index.html` angeben, wird nur die Seite "index.html"auf die Sperrliste gesetzt.

Proxyeinstellung beim Umleiten des Browserinhalts

> **Wichtig:**
>
> Die folgenden Einstellungen gelten nur für 1912 LTSR CU1 oder höher.

Diese Einstellung bietet Proxykonfigurationsoptionen auf dem VDA für die Browserinhaltsumleitung. Wenn mit einer gültigen Proxyadresse und Portnummer, PAC/WPAD-URL oder Direkt/Transparent-Einstellung aktiviert, versucht die Citrix Workspace-App nur den serverseitigen Abruf und die clientseitige Wiedergabe.

Ist die Einstellung deaktiviert oder nicht konfiguriert und es wird ein Standardwert verwendet, versucht die Citrix Workspace-App den clientseitigen Abruf und die clientseitige Wiedergabe.

Die Standardeinstellung ist "Nicht zugelassen".

Zulässiges Muster für einen expliziten Proxy:

`http://\<hostname/ip address\>:\<port\>`

Beispiel:

`http://proxy.example.citrix.com:80`
`http://10.10.10.10:8080`

Zulässige Muster für PAC/WPAD-Dateien:

`http://<hostname/ip address>:<port>/<path>/<Proxy.pac>`

Beispiel: `http://wpad.myproxy.com:30/configuration/pac/Proxy.pac`

`https://<hostname/ip address>:<port>/<path>/<wpad.dat>`

Beispiel: `http://10.10.10.10/configuration/pac/wpad.dat`

Zulässige Muster für direkte oder transparente Proxys:

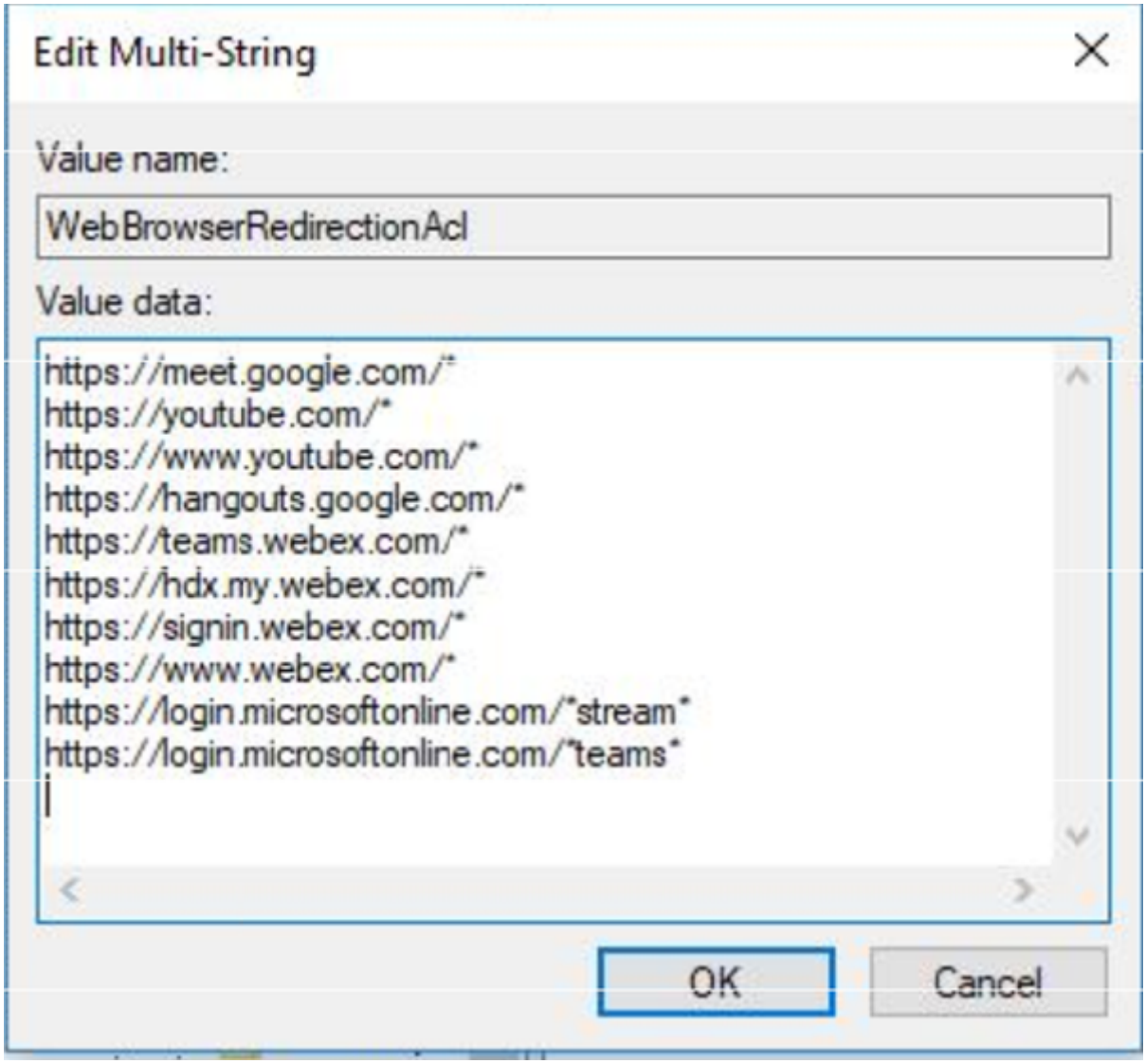
Geben Sie im Richtlinientextfeld das Wort **DIRECT** ein.

Außerkraftsetzung von Registrierungsschlüsseln für die Browserinhaltsumleitung

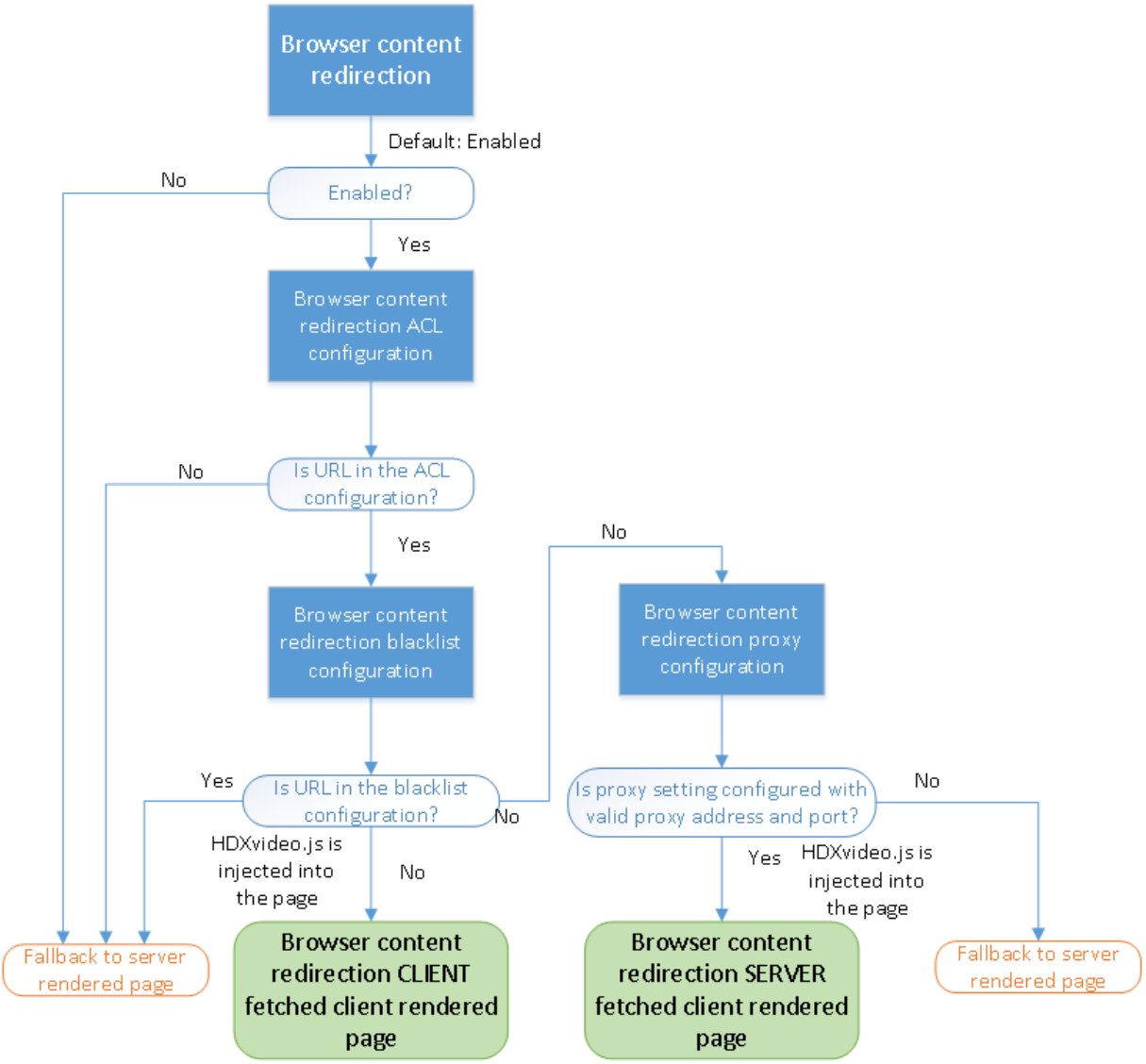
> **Warnung**
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.
>
> Außerkraftsetzungsoptionen der Registrierung für Richtlinieneinstellungen:

`\HKLM \SOFTWARE\Wow6432Node\Citrix\HdxMediastream`

Name	Typ	Wert
WebBrowserRedirection	DWORD	1 = zugelassen, 0 = nicht zugelassen
WebBrowserRedirectionAcl	REG_MULTI_SZ	
WebBrowserRedirectionAuthenticationSites	REG_MULTI_SZ	
WebBrowserRedirectionProxyAddress	REG_SZ	`http://myproxy.citrix.com:8080` oder `http://10.10.10.10:8888`
WebBrowserRedirectionBlacklist	REG_MULTI_SZ	



HDXVideo.js-Einfügung für Browserinhaltsumleitung



HdxVideo.js wird unter Einsatz der Chrome-Erweiterung für die Browserinhaltsumleitung bzw. des Browserhilfsobjekts (BHO) für Internet Explorer auf der Webseite eingefügt. Das BHO ist ein Plug-In-Modell für Internet Explorer. Es bietet Hooks für Browser-APIs und ermöglicht dem Plug-In den Zugriff auf das Document Object Model (DOM) der Seite, um die Navigation zu steuern.

Das BHO entscheidet, ob HdxVideo.js auf einer bestimmten Seite eingefügt werden soll. Die Entscheidung erfolgt gemäß den im Flussdiagramm oben dargestellten Verwaltungsrichtlinien.

Wenn JavaScript eingefügt und der Browserinhalt an den Client umgeleitet wurde, wird die betreffende Webseite im Internet Explorer auf dem VDA leer dargestellt. Durch Festlegen von **document.body.innerHTML** auf “empty”wird der gesamte Webseitenhauptteil auf dem VDA entfernt. Die Seite kann dann zur Anzeige im Overlaybrowser (Hdxbrowser.exe) des Clients an diesen gesendet

werden.

Einstellungen der Richtlinie "Clientsensoren"

February 6, 2020

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 Workspace-App-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:

- Stellen Sie sicher, dass eine standortaktivierte Anwendung sich nicht darauf verlässt, dass Standortinformationen verfügbar sind. Gründe:
  - 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. (Die Citrix Workspace-App 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 muss eine sichere Verbindung (zum Beispiel mit TLS oder einem VPN) erzwungen werden. Die Citrix Workspace-App muss eine Verbindung mit vertrauenswürdigen Servern herstellen.
- Sie sollten eine Rechtsberatung hinsichtlich der Verwendung von Standortdiensten erwägen.

Einstellungen der Richtlinie "Desktopbenutzeroberfläche"

February 6, 2020

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.

> **Wichtig**
>
> In diesem Release werden der Legacygrafikmodus und die Desktopgestaltungsumleitung nicht unterstützt. Diese Richtlinie ist nur zum Zweck der Abwärtskompatibilität im Fall einer Verwendung von XenApp 7.15 LTSR, XenDesktop 7.15 LTSR und früheren VDA-Releases mit Windows 7 und Windows 2008 R2 enthalten.

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 zu deaktivieren 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.

Der Standardwert 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 zu deaktivieren 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. Wenn die Desktopeinstellungen so festgelegt sind, dass am Desktop vorgenommene Änderungen nach dem Beenden der Sitzung verworfen werden, steht Benutzern, die Menüanimation in einer Sitzung aktiviert haben, in späteren Sitzungen auf dem Desktop keine Menüanimation zur Verfügung. 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"

February 6, 2020

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

February 6, 2020

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"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"

February 19, 2020

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.

> **Hinweis:**
>
> Richtlinieneinstellungen für die Clientlaufwerkumleitung gelten nicht für Laufwerke, die Sitzungen mit generischer USB-Umleitung zugeordnet sind.

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 der Citrix Workspace-App und des 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 und der Citrix Workspace-App 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 eine relativ hohe Bandbreite und eine hohe Latenz aufweisen, 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 "Grafiken"

March 15, 2022

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.

Grafikstatusanzeige

Durch diese Einstellung wird das Ausführen der Grafikstatusanzeige in der Benutzersitzung konfiguriert. Hier kann der Benutzer Details zum verwendeten Grafikmodus anzeigen, einschließlich Grafikanbieter, Encoder, Hardwarecodierung, Bildqualität, Status der progressiven Anzeige und verlustfreier Text.

Standardmäßig ist Grafikstatusanzeige deaktiviert. Diese Einstellung ersetzt die Qualitätsanzeige. In früheren Versionen von Citrix Virtual Apps and Desktops wird stattdessen die Qualitätsanzeige aktiviert.

Einschränkung aufgrund von Microsoft-Ruhezeit:

Nach dem Aktivieren der Grafikstatusanzeige kann ein Problem auftreten, wenn sich ein Benutzer zum **ersten** Mal bei Citrix Virtual Apps and Desktops anmeldet. Vier Stunden vergehen, bevor das Statusindikatorsymbol im Infobereich angezeigt wird.

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) x (vertikale Auflösung in Pixel) x (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) x (600) x (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

Diese Einstellung aktiviert oder deaktiviert die Anzeige von nahtlosen Fenstern in:

- Flip-
- Flip-3D
- Symbolleistenvorschau
- Fenstervorschau

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. Sie steuert nicht, ob Bilder zwischengespeichert werden. Wenn die Einstellung “Legacygrafikmodus”aktiviert ist, werden Bilder zwischengespeichert.

Legacygrafikmodus –nicht unterstützt. Nur für Rückwärtskompatibilität

> **Wichtig:**
>
> In diesem Release werden der Legacygrafikmodus und die Desktopgestaltungsumleitung nicht unterstützt. Diese Richtlinie ist nur zum Zweck der Abwärtskompatibilität im Fall einer Verwendung von XenApp 7.15 LTSR, XenDesktop 7.15 LTSR und früheren VDA-Releases mit Windows 7 und Windows 2008 R2 enthalten.

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 höher finden Sie unter 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 VDAs für Einzelsitzungs-OS mit einem WDDM-Treiber als primären Anzeigetreiber, z. B. Windows 8, hat diese Einstellung keine Auswirkung. Bei VDAs mit Windows-Multisitzungs-OS und 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.

Optimierung für 3D-Grafikworkload

Mit dieser Einstellung werden die am besten für grafikintensive Workloads geeigneten Standardeinstellungen konfiguriert. Aktivieren Sie diese Einstellung für Benutzer die vorwiegend mit grafikintensiven Anwendungen arbeiten. Wenden Sie diese Richtlinie nur an, wenn eine GPU für die Sitzung verfügbar ist. Alle anderen Einstellungen, die die von dieser Richtlinie festgelegten Standardeinstellungen explizit außer Kraft setzen, haben Vorrang.

Standardmäßig ist die Optimierung für 3D-Grafik-Workloads deaktiviert.

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.

Sie 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 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 **Verwenden, wenn bevorzugt** 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 **Verwenden, wenn bevorzugt**, 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 bei wenigen auf dem Server wiedergegebenen Videos oder anderen grafisch intensiven Anwendungen.

Der Standardwert ist **Verwenden, wenn bevorzugt**.

Verwenden der Hardwarecodierung für Video

Diese Einstellung ermöglicht die Verwendung von Grafikhardware (falls verfügbar) zum Komprimieren von Bildschirmelementen mit dem Videocodec. 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 Workspace-App-Versionen, die Videodecodierung unterstützen, können mit Hardwarecodierung verwendet werden.

NVIDIA

Für NVIDIA GRID-GPUs wird die Hardwarecodierung von VDAs für Einzel- und Multisitzungs-OS 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 ist mit der NVENC-Hardwarecodierung nicht kompatibel. Wird er aktiviert, hat verlustfreier Text Vorrang vor der NVENC-Hardwarecodierung.

Die selektive Verwendung des H.264-Hardwarecodecs für aktiv veränderliche Bereiche wird unterstützt.

Visuell verlustfreie Komprimierung (4:4:4) wird unterstützt. Die visuell verlustfreie Komprimierung (Grafikrichtlinieneinstellung Visuell verlustfreie Komprimierung zulassen) erfordert Citrix Workspace-App 1808 oder höher oder Citrix Receiver für Windows 4.5 oder höher.

Intel

Bei Intel Iris Pro-Grafikprozessoren wird die Hardwarecodierung von VDAs für Einzel- und Multisitzungs-OS 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 nur unterstützt, wenn die Videocodec-Richtlinie auf den gesamten Bildschirm festgelegt ist und die **Optimierung für 3D-Grafikworkload** deaktiviert ist.

Visuell verlustfrei (YUV 4:4:4) wird nicht unterstützt.

Die Intel-Codierung bietet 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.

AMD

Für AMD wird die Hardwarecodierung von VDAs für Einzelsitzungs-OS unterstützt.

AMD-GPUs müssen das RapidFire-SDK unterstützen. Beispiele: AMD Radeon Pro oder FirePro.

Damit die Codierung funktioniert, installieren Sie die neuesten AMD-Treiber. Sie können diese Treiber von https://www.amd.com/en/support herunterladen.

Verlustfreier Text ist mit der AMD-Hardwarecodierung nicht kompatibel. Wird er aktiviert, hat verlustfreier Text Vorrang vor der AMD-Hardwarecodierung.

Die selektive Verwendung des H.264-Hardwarecodecs für aktiv veränderliche Bereiche wird unterstützt.

Einstellungen der Richtlinie “Zwischenspeichern”

February 6, 2020

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

September 21, 2021

> **Wichtig:**
>
> Ab Citrix Virtual Apps and Desktops 7 1903 wird Framehawk nicht mehr unterstützt. Verwenden Sie stattdessen Thinwire mit aktiviertem adaptivem Transport.

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"

February 6, 2020

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"

March 2, 2021

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.

Wenn Sie die Richtlinieneinstellung **Lokalen App-Zugriff zulassen** auf **Aktiviert** festlegen, wird die Browserinhaltsumleitung nicht unterstützt.

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"

February 6, 2020

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 Workspace-App-Benutzeroberfläche, indem sie eine für Tablet-Geräte ausgelegte touchoptimierte Benutzeroberfläche zulässt oder verweigert.

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 der Citrix Workspace-App für iOS ändern und das Windows-Kombinationsfeld verwenden.

Standardmäßig wird die Funktion zum Remoten von Kombinationsfeldern verweigert.

Multimedia - Richtlinieneinstellungen

June 27, 2024

Der Abschnitt "Multimedia"enthält Richtlinieneinstellungen, mit denen Sie das Streaming von HTML5- und Windows-Audio- und Videoinhalten in Benutzersitzungen verwalten.

> **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. Erstellen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

Multimediarichtlinien

Standardmäßig werden alle auf dem Delivery Controller festgelegten Multimediarichtlinien in folgenden Registrierungseinträgen gespeichert:

Maschinenrichtlinien:

```
HKEY_LOCAL_MACHINE\Software\Policies\Citrix\MultimediaPolicies
```

Benutzerrichtlinien:

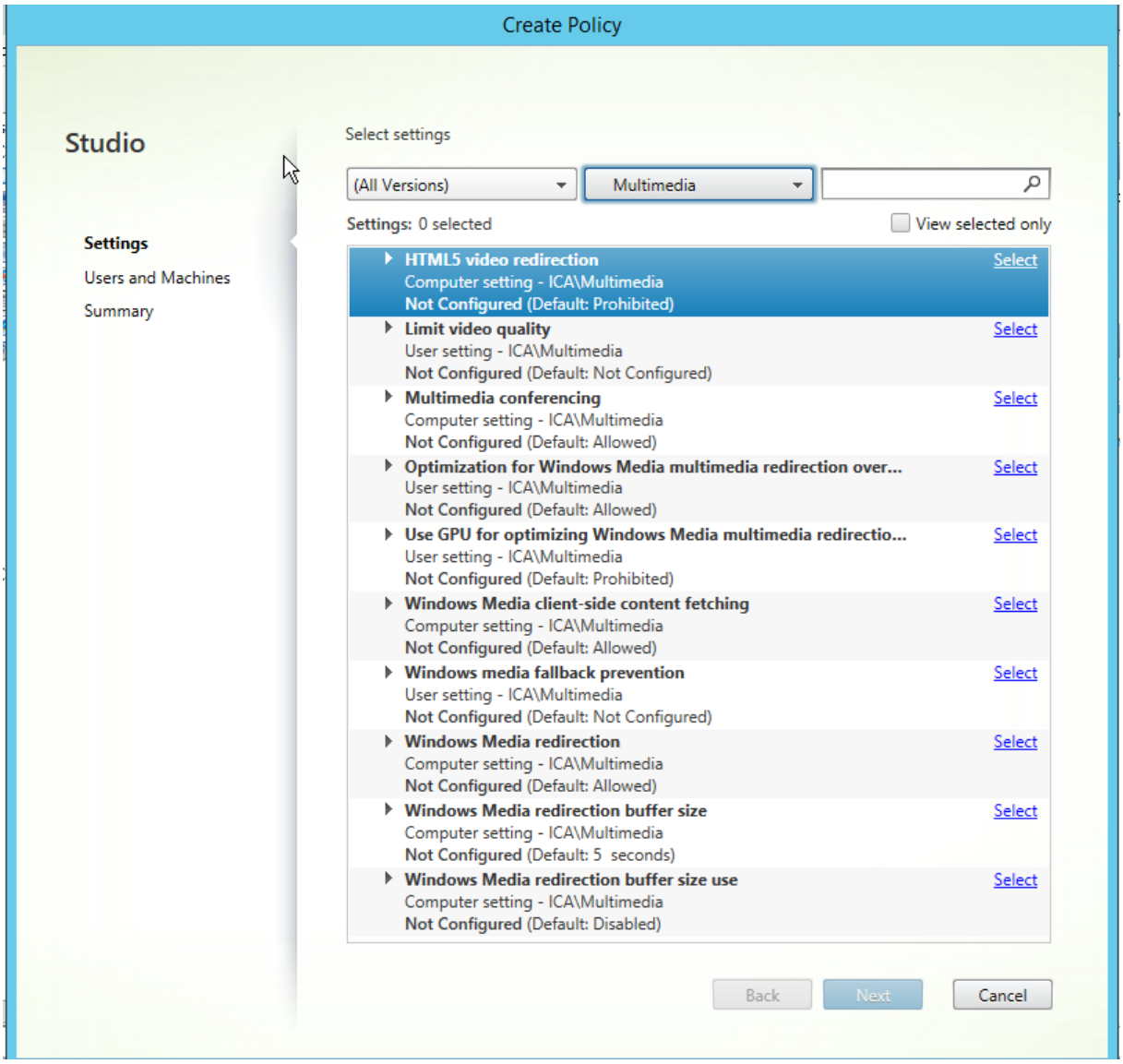
```
HKEY_LOCAL_MACHINE\Software\Policies\Citrix{ User Session ID } \User\
MultimediaPolicies
```

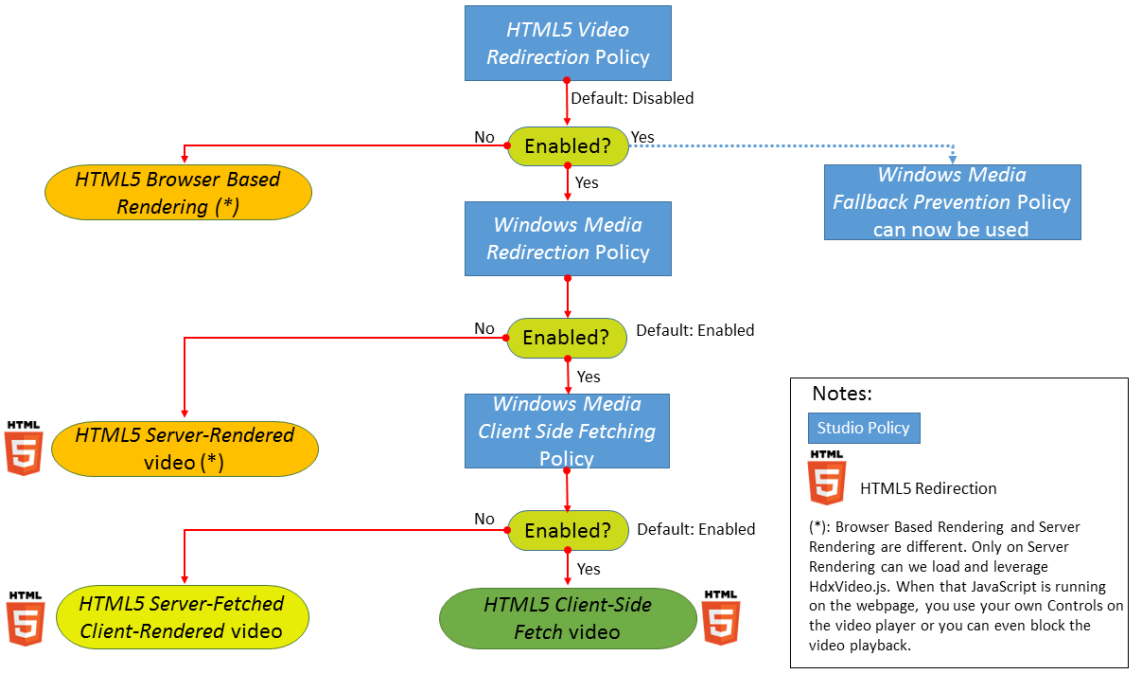
Zum Abfragen der ID der aktuellen Benutzersitzung geben Sie den Befehl **qwinsta** in der Windows-Eingabeaufforderung ein.

HTML5-Videoumleitung

Steuert und optimiert die Bereitstellung von HTML5-Multimediawebinhalten durch Citrix Virtual Apps and Desktops-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 Citrix Virtual Apps and Desktops 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
- Anhalten
- Suchen
- Wiederholen
- Audio
- Vollbild

Unter https://www.citrix.com/solutions/html5-redirect.html finden Sie eine HTML5-Videoumleitungstestseite.

TLS- und HTML5-Videoumleitung und Browserinhaltsumleitung

Mit der HTML5-Videoumleitung können Sie Videos von HTTPS-Websites umleiten. Mit der Browserinhaltsumleitung können Sie die gesamte Website umleiten. 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 als ein lokales Systemkonto ausgeführt und dient der SSL-Beendigung und Benutzersitzungszuordnung.

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.

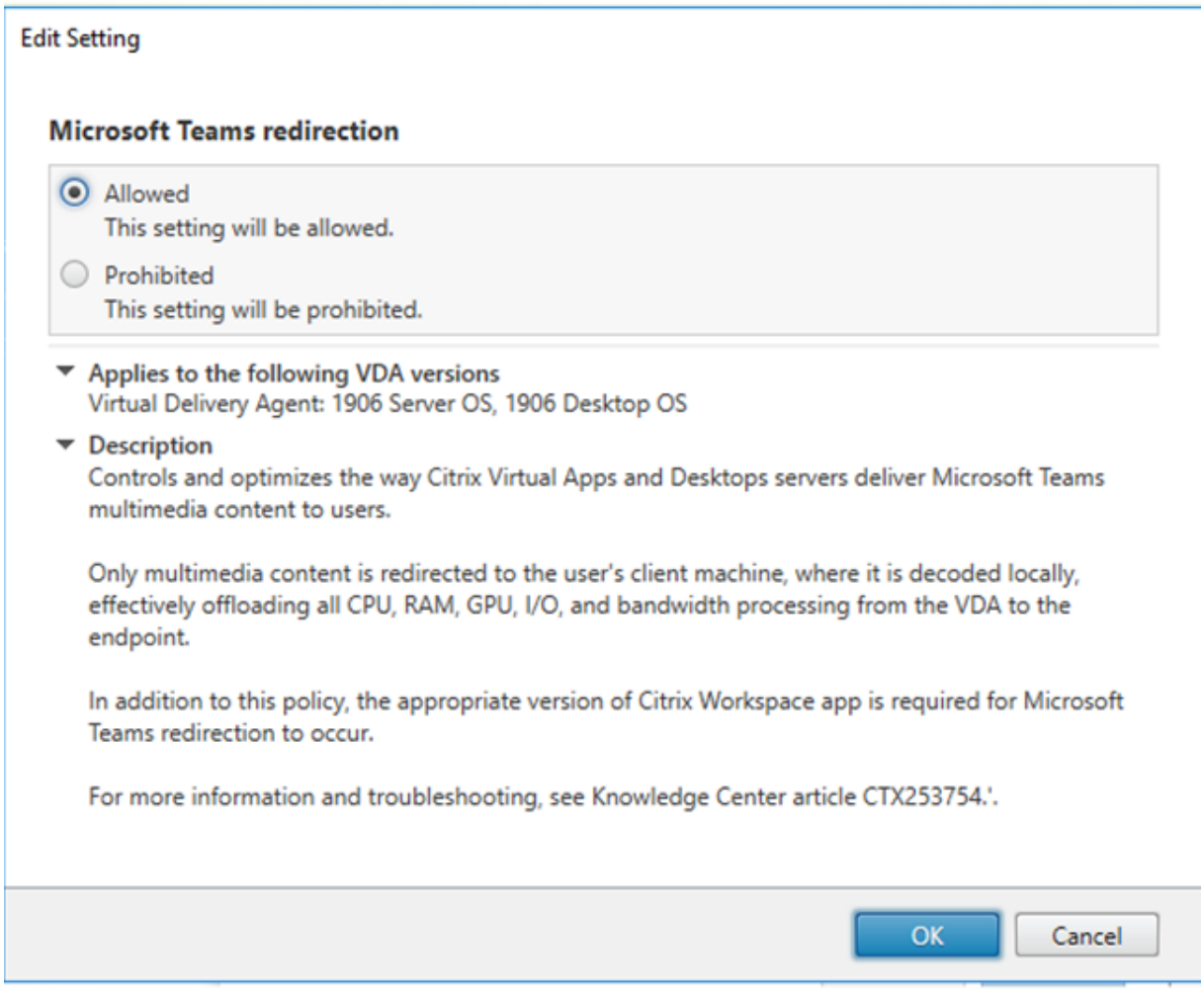
Zum Festlegen der maximalen Qualität wählen Sie eine der folgenden Optionen:

- 1080 p/8,5 MBit/s
- 720 p/4,0 MBit/s
- 480 p/720 KB/s
- 380 p/400 KB/s
- 240 p/200 KB/s

Die gleichzeitige Wiedergabe mehrerer Videos auf einem Server verbraucht viele Ressourcen und kann die Skalierbarkeit des Servers beeinträchtigen.

Microsoft Teams-Umleitung

Mit dieser Einstellung kann Microsoft Teams mithilfe der HDX-Technologie optimiert werden.



Wenn diese Richtlinie aktiviert ist und Sie eine unterstützte Version der Citrix Workspace-App verwenden, wird dieser Registrierungsschlüssel auf dem VDA auf **1** festgelegt. Microsoft Teams liest den Schlüssel zum Laden im VDI-Modus.
Beachten Sie, dass der Registrierungsschlüssel nicht manuell festgelegt werden muss.

HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream

Name: MSTeamsRedirSupport

Wert: DWORD (1 - ein, 0 - aus)

> **Hinweis:**
>
> Wenn Sie VDAs der Version 1906.2 oder höher mit älteren Controller-Versionen (z. B. Version 7.15) verwenden, für die die Richtlinie in Studio nicht verfügbar ist, ist die HDX-Optimierung standardmäßig im VDA aktiviert. Ab Workspace-App-Version 1907 startet Teams im optimierten Modus.
>
> Um das Feature in dieser Situation für bestimmte Benutzer zu deaktivieren, können Sie die Reg-

> istrierungseinstellung über eine Gruppenrichtlinie zur Anwendung eines Anmeldeskripts auf die Organisationseinheit des Benutzers außer Kraft setzen.

In der Standardeinstellung ist die Microsoft Teams-Umleitung aktiviert.

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 die Browserinhaltsumleitung, HTML5 und Windows Media. Damit sie für HTML5 funktioniert, legen Sie die Richtlinie **HTML5-Videoumleitung** auf **Zugelassen** fest.

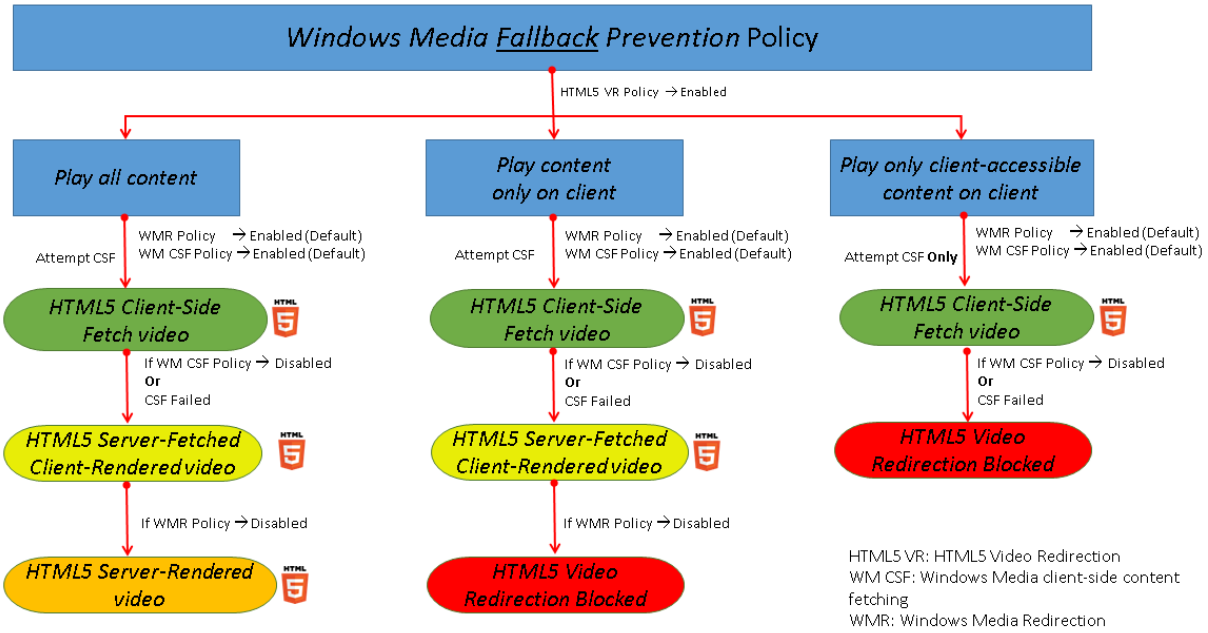
Administratoren können über die Einstellung der Richtlinie "Verhinderung von Fallback auf Windows Media"die Methoden für die Übertragung gestreamter Inhalte an Benutzer steuern.

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.

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 Inhaltsabruf von Windows Media

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.

Audio ist in der Citrix Workspace-App standardmäßig deaktiviert. Wenn Benutzer Multimedia-Anwendungen in ICA-Sitzungen ausführen können, aktivieren Sie Audio oder geben Sie den Benutzern in der Citrix Workspace-App-Benutzeroberfläche 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"

January 8, 2021

Im Abschnitt "Multistreamverbindungen"finden Sie Richtlinieneinstellungen zum Verwalten der Quality-of-Service-Priorität 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 (niedrigste Portnummer,höchste Portnummer), die vom 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 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. Konfigurieren Sie die Multistream-Computerrichtlinieneinstellung, wenn Sie Citrix SD-WAN oder Router von Drittanbietern verwenden, um die gewünschte Quality of Service zu erreichen.

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, 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.

Multistreambenutzereinstellung

Mit dieser Einstellung aktivieren oder deaktivieren Sie Multistream auf dem Benutzergerät.

Standardmäßig ist Multistream für alle Benutzer deaktiviert. Konfigurieren Sie die Multistream-Benutzereinstellung, wenn Sie Citrix SD-WAN oder Router von Drittanbietern verwenden, um die gewünschte Quality of Service zu erreichen.

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 für die Zuweisung virtueller Multistreamkanäle

> **Wichtig:**
>
> Die folgenden Einstellungen gelten nur für 1912 LTSR CU1 oder höher.

Diese Einstellungen geben den ICA-Stream an, dem die virtuellen Kanäle bei Verwendung von Multistream zugewiesen werden.

Wenn Sie diese Einstellungen nicht konfigurieren, verbleiben virtuelle Kanäle in ihrem Standardstream. Um einem ICA-Stream einen virtuellen Kanal zuzuweisen, wählen Sie die gewünschte Streamnummer (0, 1, 2, 3) aus der Liste **Streamnummer** neben dem Namen des virtuellen Kanals aus.

Wird in der Umgebung ein benutzerdefinierter virtueller Kanal verwendet, klicken Sie auf **Hinzufügen**, geben Sie den Namen des virtuellen Kanals im Textfeld unter **Virtuelle Kanäle** ein und wählen Sie die gewünschte Streamnummer aus der Liste **Streamnummer** daneben aus. Sie müssen den tatsächlichen Namen des virtuellen Kanals und nicht den Anzeigenamen eingeben. Beispielsweise "CTXSBR" und nicht "Citrix Browserbeschleunigung".

Diese Einstellungen werden nur wirksam, wenn Sie "Multistreamcomputereinstellung"aktiviert haben.

Die Standardzuweisung virtueller Kanäle und ihrer Streams ist wie folgt:

- Audio: 0
- Browserinhaltsumleitung: 2
- Client-COM-Portzuordnung: 3
- Clientlaufwerkszuordnung: 2
- Clientdruckerzuordnung: 3
- Zwischenablage: 2

- CTXDND: 1
- DVC-Plug-Ins (statischer Name des virtuellen Kanals, der automatisch aus dem DVC-Plug-In-Anzeigenamen generiert oder vom Administrator zugewiesen wird): 2
- End User Experience Monitoring: 1
- Dateiübertragung (HTML5 Receiver): 2
- Generische Datenübertragung: 2
- ICA-Steuerung: 1
- Eingabemethoden-Editor: 1
- Legacy-Clientdruckerzuordnung (COM1): 1, 3
- Legacy-Clientdruckerzuordnung (COM2): 2, 3
- Legacy-Clientdruckerzuordnung (LPT1): 1, 3
- Legacy-Clientdruckerzuordnung (LPT2): 2, 3
- Lizenzverwaltung: 1
- Microsoft Teams-/WebRTC-Umleitung: 1
- Mobiler Receiver: 1
- MultiTouch: 1
- Portweiterleitung: 2
- Remote Audio- und Videoerweiterungen (RAVE): 2
- Seamless (Transparente Fensterintegration): 1
- Sensor und Position: 1
- Smartcard: 1
- Thinwire-Grafiken: 1
- Transparente UI-Integration/Anmeldestatus: 2
- TWAIN-Umleitung: 2
- USB: 2
- Schriftart und Tastatur ohne Latenz: 2
- Datenkanal ohne Latenz: 2

Weitere Informationen zu Zuweisung und Priorität virtueller Kanäle finden Sie im Knowledge Center unter CTX131001.

Einstellungen der Richtlinie “Portumleitung”

March 15, 2022

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"

September 21, 2021

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. Der Citrix-Druckmanagerdienst (Cpsvc.exe) erstellt in der ICA/HDX-Sitzung bei der Sitzungsanmeldung eine Netzwerkdruckerverbindung für jeden in der Richtlinieneinstellung **Sitzungsdrucker** definierten Netzwerkdrucker. Beim Abmelden von der Sitzung werden die Drucker wieder gelöscht. In der Standardeinstellung sind keine Drucker angegeben.

In der Richtlinieneinstellung **Sitzungsdrucker** können sich die Netzwerkdrucker auf einem Windows-Druckserver oder einem universellen Citrix-Druckserver befinden.

- **Windows-Druckserver:** Freigabe eines oder mehrerer Netzwerkdrucker. Die für die Verwendung der Netzwerkdrucker erforderlichen systemeigenen Druckertreiber sind vorhanden.
- **Universeller Druckserver:** Ein Windows-Druckserver, auf dem die Software für den universellen Citrix-Druckserver installiert wurde.

Bei Verwendung eines Windows-Druckservers werden die Netzwerkdruckerverbindungen vom Citrix-Druckmanagerdienst über systemeigene Druckertreiber hergestellt. Die systemeigenen Druckertreiber müssen auf dem Citrix Virtual Apps-Server installiert sein.

Bei Verwendung eines universellen Citrix-Druckservers werden die Netzwerkdruckerverbindungen vom Citrix-Druckmanagerdienst über systemeigene Druckertreiber, den universellen Citrix-Druckertreiber oder den universellen Citrix XPS-Druckertreiber hergestellt. Der verwendete Treiber wird durch die gewählte Einstellung der Richtlinie "Verwendung universeller Druckertreiber" gesteuert.

Alle Windows-Druckertreiber gehören aktuell zur Treiberversion v3 oder v4. Weitere Informationen finden Sie unter Support for the Microsoft V3 and V4 Printer Driver Architectures.

Gehen Sie folgendermaßen vor, um Sitzungsdrucker hinzuzufügen und um sicherzustellen, dass sie in den Sitzungen angezeigt werden:

1. Navigieren Sie in Citrix Studio zur Registerkarte **Richtlinien**.
2. Aktivieren Sie im Dialogfeld **Richtlinie bearbeiten** die Sitzungsdruckrichtlinie.
3. Fügen Sie in der Richtlinie den Sitzungsdrucker hinzu. 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. Der Sitzungsdrucker muss in der Liste angezeigt werden.

4. Nachdem die Richtlinie festgelegt wurde, zeigt die veröffentlichte Anwendung möglicherweise keine Sitzungsdrucker an. Dieses Problem kann auftreten, wenn der Druckertreiber auf dem Citrix Virtual Apps-Server fehlt oder wenn die Richtlinie zwar erstellt, aber nicht aktiviert wurde.

   > Hinweis:
   >
   > Wenn der Druckertreiber nicht auf dem Citrix Virtual Apps-Server installiert ist, wurde dies möglicherweise vom Administrator vergessen (der wohl häufigste Fehler bei Sitzungsdruckern).

5. Starten Sie den veröffentlichten Desktop und fügen Sie den Sitzungsdrucker unter **Geräte und Drucker > Systemsteuerung** manuell hinzu.
6. Wenn dies fehlschlägt, überprüfen Sie die Kommunikation zwischen dem Citrix Virtual Apps-Server und dem Druckserver. Führen Sie gegebenenfalls einen Test mit RDP aus.

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”

September 21, 2021

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

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 werden generische universelle Drucker nicht automatisch erstellt.

Die folgenden Richtlinieneinstellungen hängen zusammen:

- Verwendung universeller Druckertreiber
- Priorität universeller Treiber

Universellen PDF-Drucker automatisch erstellen

Diese Einstellung aktiviert bzw. deaktiviert die automatische Erstellung des Citrix PDF-Druckers für Sitzungen mit der Citrix Workspace-App für Windows (ab VDA-Version 7.19), der Citrix Workspace-App für HTML5 oder der Citrix Workspace-App für Chrome.

Standardmäßig wird der Citrix PDF-Drucker nicht automatisch erstellt.

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 Citrix Virtual Apps einen gespeicherten Drucker wiederherstellt, 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.

Universeller PDF-Druckertreiber von Citrix

Der universelle PDF-Druckertreiber von Citrix ermöglicht das Drucken von Dokumenten aus gehosteten Anwendungen und aus Anwendungen, die auf mit Citrix Virtual Apps and Desktops bereitgestellten virtuellen Desktops ausgeführt werden. Wenn ein Benutzer die Option Citrix PDF-Drucker auswählt, wird die Datei vom Treiber in PDF konvertiert und auf das lokale Gerät übertragen. Die PDF-Datei wird dann zur Ansicht geöffnet und kann auf einem lokal angeschlossenen Drucker ausgedruckt werden. PDF ist neben EMF und XPS eines der von Citrix Universal Printing unterstützten Formate.
Der PDF-Drucker kann mithilfe der Citrix Richtlinie aktiviert, konfiguriert und als Standard festgelegt werden. Die Option "Citrix PDF-Drucker"steht in der Citrix Workspace-App für Windows, Chrome und HTML5 zur Verfügung.

> **Hinweis:**
>
> Bei Windows-Endpunkten ist ein PDF-Viewer erforderlich. Der Client muss über eine Anwendung mit in Windows registrierter Dateitypzuordnung verfügen, damit PDF-Dateien geöffnet werden können.

Einstellungen der Richtlinie "Treiber"

September 21, 2021

Der Abschnitt "Treiber"enthält Richtlinieneinstellungen für Druckertreiber.

Automatische Installation von mitgelieferten Druckertreibern

> **Hinweis**
>
> Diese Richtlinie unterstützt keine VDAs in diesem Release.

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"

January 8, 2021

Der Abschnitt "Universeller Druckserver" enthält Richtlinieneinstellungen für die Behandlung des universellen Druckservers.

SSL-Verschlüsselungssammlung

Diese Einstellung legt die SSL/TLS-Verschlüsselungssammlung fest, die vom universellen Druckclient für verschlüsselte Datenstromverbindungen (CGP) verwendet werden sollen.

Informationen zur Steuerung der vom universellen Druckclient für Webdienstverbindungen (HTTPS/-SOAP) verwendeten Verschlüsselungssammlungen finden Sie unter [SCHANNEL].

Standardwert: ALLE

Die Einstellung hat folgende Werte: ALLE, COM und GOV.

Den Werten entsprechen folgende Verschlüsselungssammlungen:

ALL:

TLS_ECDHE_RSA_AES256_GCM_SHA384

TLS_ECDHE_RSA_AES256_CBC_SHA384

TLS_ECDHE_RSA_AES128_CBC_SHA

COM:

TLS_ECDHE_RSA_AES128_CBC_SHA

GOV:

TLS_ECDHE_RSA_AES256_GCM_SHA384

TLS_ECDHE_RSA_AES256_CBC_SHA384

SSL-Konformitätsmodus

Diese Einstellung legt die Stufe der Konformität mit "Special Publication 800-52" des US-amerikanischen National Institute of Standards and Technology für verschlüsselte Datenstromverbindungen (CGP) des universellen Druckclients fest.

Standardwert: Keine.

Diese Einstellung hat die folgenden Werte:

Keine.

Für verschlüsselte Datenstromverbindungen wird der Standardkonformitätsmodus verwendet.

SP800-52.

Für verschlüsselte Datenstromverbindungen wird der Kompatibilitätsmodus (NIST Special Publication 800-52) verwendet.

SSL aktiviert

Diese Einstellung legt fest, ob vom universellen Druckclient für verschlüsselte Datenstromverbindungen (CGP) und für Webdienstverbindungen (HTTP/SOAP) SSL/TLS verwendet werden soll.

Wenn Sie **Universellen Druckserver aktivieren** auf **Aktiviert mit Fallback auf systemeigenen Windows-Remotedruck** festlegen, werden vom Microsoft Windows-Netzwerkdruckanbieter Fallbackverbindungen hergestellt. Diese Einstellung wirkt sich nicht auf diese Fallbackverbindungen aus.

Standardwert: Deaktiviert

Diese Einstellung hat die folgenden Werte:

Aktiviert.

Der universelle Druckclient verwendet SSL/TLS, um eine Verbindung mit dem universellen Druckserver herzustellen.

Deaktiviert.

Der universelle Druckclient verwendet SSL/TLS, um eine Verbindung mit dem universellen Druckserver herzustellen.

SSL FIPS-Modus

Diese Einstellung legt fest, ob das vom universellen Druckclient für verschlüsselte Datenstromverbindungen (CGP) verwendete kryptografische Modul im FIPS-Modus ausgeführt werden soll.

Standardwert: Deaktiviert

Diese Einstellung hat die folgenden Werte:

Aktiviert.

FIPS-Modus ist aktiviert.

Deaktiviert.

FIPS-Modus ist deaktiviert.

SSL-Protokollversion

Diese Einstellung legt fest, welche SSL/TLS-Protokollversion vom universellen Druckclient verwendet werden soll.

Standardwert: ALLE

Diese Einstellung hat die folgenden Werte:

ALLE.

Es wird TLS-Version 1.0, 1.1 oder 1.2 verwendet.

TLSv1.

Es wird TLS-Version 1.0 verwendet.

TLSv1.1.

Es wird TLS Version 1.1 verwendet.

TLSv1.2.

Es wird TLS-Version 1.2 verwendet.

Port für SSL-verschlüsselten Druckdatenstrom (CGP) des universellen Druckservers

Diese Einstellung legt die Nummer des TCP-Ports für den verschlüsselten Druckdatenstrom (CGP) des universellen Druckservers fest. Der Port empfängt Daten für Druckaufträge.

Standardwert: 443

Port für SSL-verschlüsselten Webdienst des universellen Druckservers (HTTPS/SOAP)

Diese Einstellung legt die Nummer des TCP-Ports für den verschlüsselten Webdienst (HTTPS/SOAP) des universellen Druckservers fest. Dieser Port empfängt Daten für Druckbefehle.

Standardwert: 8443

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 Citrix Virtual Apps and Desktops-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. Diese Einstellung ändert den VDA in Citrix Virtual Apps and Desktops. 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"

February 6, 2020

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”

September 21, 2021

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 Citrix Virtual Apps and Desktops 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.

Die Schlüssel für die RC5-Blockverschlüsselung werden beim Erstellen einer Sitzung vereinbart. Die Vereinbarung erfolgt unter Einsatz des Diffie-Hellman-Algorithmus. Die Vereinbarung verwendet öffentliche Diffie-Hellman-Parameter, die bei der Installation des Virtual Delivery Agents in der Windows-Registrierung gespeichert werden. Öffentliche Parameter sind nicht geheim. Das Ergebnis der Diffie-Hellman-Vereinbarung ist ein geheimer Schlüssel, aus dem Sitzungsschlüssel für die RC5-Blockverschlüsselung abgeleitet werden. Separate Sitzungsschlüssel werden für die Benutzeranmeldung und für die Datenübertragung verwendet. Für den Datenverkehr zum und vom Virtual Delivery Agent werden ebenfalls separate Sitzungsschlüssel verwendet. Daher gibt es vier Sitzungsschlüssel für jede Sitzung. Die geheimen Schlüssel und die Sitzungsschlüssel werden nicht gespeichert. Die Initialisierungsvektoren für die RC5-Blockverschlüsselung werden ebenfalls aus dem geheimen Schlüssel abgeleitet.

Einstellungen der Richtlinie “Serverlimits”

September 21, 2021

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.

Um die Richtlinie anzuzeigen, wählen Sie **Mehrere Versionen**, deaktivieren Sie die Einzelsitzungs-OS-Versionen und wählen Sie dann **Serverlimits**.

> **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 Microsoft-Dialogfeldmeldung wird nicht von Citrix Richtlinieneinstellungen gesteuert.Weitere Informationen finden Sie unter http://support.citrix.com/article/CTX118618.

Einstellungen der Richtlinie “Sitzungslimits”

September 21, 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 nicht 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"

February 6, 2020

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 Sitzungszuverlässigkeit und die automatische Wiederverbindung von Clients ermöglichen Benutzern, nach einer Netzwerkunterbrechung automatisch wieder eine Verbindung mit ihren Citrix Workspace-App-Sitzungen herzustellen. Standardmäßig ist die Sitzungszuverlässigkeit zugelassen.

Ab Citrix Workspace-App 1808 und Citrix Receiver für Windows 4.7 werden die Einstellungen von Studio auf dem Client durchgesetzt. Citrix Receiver-Gruppenrichtlinienobjekt auf den Clients wird durch die Studio-Richtlinie überschrieben. 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 Version 4.7: Stellen Sie Richtlinien in Studio und in der Vorlage für das Citrix Receiver-Gruppenrichtlinienobjekt auf dem Client ein, 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.

Bei Verwendung der Sitzungszuverlässigkeit bleibt die Sitzung auf dem Server aktiv. Als Hinweis darauf, dass die Verbindung unterbrochen wird, wird die Anzeige opak. Die Sitzung friert während der Unterbrechung ggf. ein und der Benutzer kann mit der Anwendung weiterarbeiten, wenn die Netzwerkverbindung wiederhergestellt ist. Die Sitzungszuverlässigkeit verbindet Benutzer ohne Neuauthentifizierung wieder.

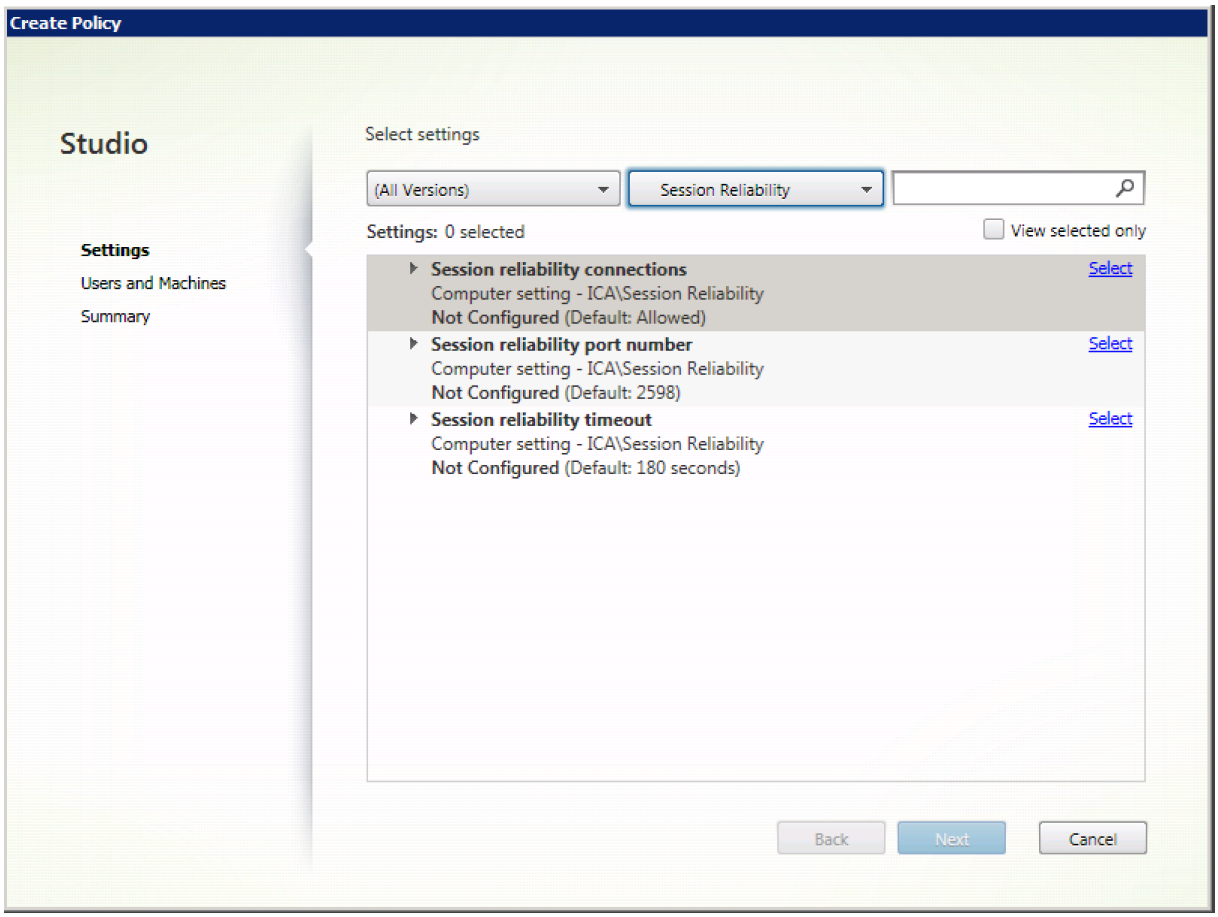
Wenn Sie sowohl Sitzungszuverlässigkeit als auch die Funktion zur automatischen Wiederverbindung verwenden, werden beide Funktionen nacheinander ausgeführt. Die Sitzungszuverlässigkeit beendet oder trennt die Benutzersitzung, nachdem der mit der Option Sitzungszuverlässigkeit - Timeout festgelegte Zeitraum abgelaufen ist. Anschließend werden die Richtlinieneinstellungen für die automa-

tische Wiederverbindung von Clients wirksam und es wird versucht, eine Verbindung mit der unterbrochenen Sitzung wiederherzustellen.

Standardmäßig ist die Sitzungszuverlässigkeit zugelassen.

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

Mit dieser Einstellung legen Sie fest, wie viele Sekunden der Sitzungszuverlässigkeitsproxy auf die Wiederverbindung der Sitzung wartet, bevor die Sitzung getrennt 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 “Sitzungswasserzeichen”

February 6, 2020

Der Bereich “Sitzungswasserzeichen”enthält Richtlinieneinstellungen zum Konfigurieren dieses Features.
Wenn Sie das Feature aktivieren, erhöhen sich der Verbrauch an Netzwerkbandbreite und die CPU-Auslastung durch die VDA-Maschine erheblich. Es wird empfohlen, Sitzungswasserzeichen für ausgewählte VDA-Maschinen auf Grundlage der verfügbaren Hardwareressourcen zu konfigurieren.

> **Wichtig**
>
> Aktivieren Sie die Option “Sitzungswasserzeichen”, damit die anderen Richtlinieneinstellungen für Wasserzeichen wirksam werden. Zur Erzielung einer besseren Benutzererfahrung aktivieren Sie maximal zwei Wasserzeichentexte.

Aktivieren von Sitzungswasserzeichen

Wenn Sie diese Einstellung aktivieren, werden Sitzungen mit einem undurchsichtigen Textwasserzeichen angezeigt, das sitzungsspezifische Informationen enthält. Die anderen Wasserzeicheneinstellungen hängen davon ab, dass dieses aktiviert ist.

Standardmäßig sind Sitzungswasserzeichen deaktiviert.

Client-IP-Adresse einschließen

Wenn Sie diese Einstellung aktivieren, wird in der Sitzung die aktuelle Client-IP-Adresse als Wasserzeichen angezeigt.

Standardmäßig ist die Option "Client-IP-Adresse einschließen"deaktiviert.

Verbindungszeit einschließen

Wenn Sie diese Einstellung aktivieren, wird im Sitzungswasserzeichen eine Verbindungszeit angezeigt. Das Format ist JJJJ/MM/TT hh:mm. Die angezeigte Zeit basiert auf der Systemuhr und der Zeitzone.

Standardmäßig ist die Option "Verbindungszeit einschließen"deaktiviert.

Anmeldenamen einschließen

Wenn Sie diese Einstellung aktivieren, wird in der Sitzung der aktuelle Anmeldename als Wasserzeichen angezeigt. Das Anzeigeformat ist BENUTZERNAME@DOMÄNENNAME. Es wird empfohlen, Benutzernamen auf maximal 20 Zeichen zu beschränken. Wenn ein Benutzernamen mehr als 20 Zeichen hat, werden die Zeichen evtl. zu klein angezeigt oder abgeschnitten und die Wirksamkeit des Wasserzeichens verringert.

Standardmäßig ist "Anmeldebenutzernamen einschließen"aktiviert.

VDA-Hostnamen einschließen

Wenn Sie diese Einstellung aktivieren, wird in der Sitzung der VDA-Hostname der aktuellen ICA-Sitzung als Wasserzeichen angezeigt.

Standardmäßig ist "VDA-Hostnamen einschließen"aktiviert.

VDA-IP-Adresse einschließen

Wenn Sie diese Einstellung aktivieren, wird in der Sitzung die VDA-IP-Adresse der aktuellen ICA-Sitzung als Wasserzeichen angezeigt.

Standardmäßig ist die Option "Client-IP-Adresse einschließen"deaktiviert.

Sitzungswasserzeichenstil

Diese Einstellung steuert, ob eine einzelne oder mehrere Wasserzeichenbeschriftungen angezeigt werden sollen. Wählen Sie in dem Dropdownmenü **Wert** die Option **Einzeln** oder **Mehrere**.

Bei Auswahl von **Mehrere** werden fünf Wasserzeichenbeschriftungen in der Sitzung angezeigt: eine in der Mitte und vier in den Ecken.

Bei Auswahl von **Einzeln** wird nur eine Wasserzeichenbeschriftung in der Mitte angezeigt.

Standardmäßig ist "Mehrere"ausgewählt.

Benutzerdefinierter Wasserzeichentext

Mit dieser Einstellung können Sie eine eigene Zeichenfolge (z. B. den Unternehmensnamen) zur Anzeige im Sitzungswasserzeichen angeben. Wenn Sie eine Zeichenfolge angeben, wird dieser Text in einer neuen Zeile nach den anderen Informationen im Wasserzeichen angezeigt.
Der benutzerdefinierte Text für Wasserzeichen darf maximal 25 Unicode-Zeichen enthalten. Wenn Sie eine längere Zeichenfolge konfigurieren, wird diese auf 25 Zeichen gekürzt.

Es gibt keinen Standardtext.

Wasserzeichentransparenz

Sie können eine Wasserzeichendeckkraft von 0–100 angeben. Je größer der Wert, desto deckender ist das Wasserzeichen.

Der Standardwert ist 17.

Einstellungen der Richtlinie "Zeitzonensteuerung"

September 21, 2021

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.

Wiederherstellen der Zeitzone des Desktopbetriebssystems beim Trennen oder Abmelden der Sitzung

Diese Einstellung legt fest, ob die Zeitzoneneinstellung des VDAs für Einzelsitzungs-OS auf die ursprüngliche Maschinenzeitzone zurückgesetzt wird, wenn der Benutzer die Verbindung trennt oder sich abmeldet. Wenn Sie die Einstellung aktivieren, stellt der VDA die ursprüngliche Zeitzone der Maschine wieder her, wenn der Benutzer die Verbindung trennt oder sich abmeldet. Damit diese Einstellung wirksam wird, legen Sie die **Lokale Zeit des Clients verwenden** auf **Clientzeitzone verwenden** fest.

Standardmäßig ist diese Einstellung aktiviert.

Lokale Zeit des Clients verwenden

Mit dieser Einstellung legen Sie die Zeitzoneneinstellung der Benutzersitzung fest. Zur Auswahl stehen die Zeitzone der Benutzersitzung (Serverzeitzone) oder die Zeitzone des Benutzergeräts (Clientzeitzone).

Standardmäßig wird die Zeitzone der Sitzung des Benutzers verwendet.

Damit diese Einstellung wirksam wird, aktivieren Sie die Einstellung **Zeitzonenumleitung zulassen** im Gruppenrichtlinien-Editor. Diese Einstellung ist unter **Benutzerkonfiguration** > **Computerkonfiguration** > **Administrative Vorlagen** > **Windows-Komponenten** > **Remotedesktopdienste** > **Remotedesktop-Sitzungshost** > **Geräte- und Ressourcenumleitung**.

Bei einem VDA für Einzelsitzungs-OS, der auf einem Multisitzungs-OS ausgeführt wird, konfigurieren Sie das lokale Benutzerrecht **Zeitzone ändern** zu **Jeder**. Dieses Benutzerrecht finden Sie unter **Lokale Computerrichtlinie** > **Computerkonfiguration** > **Windows-Einstellungen** > **Sicherheitseinstellungen** > **Lokale Richtlinien** > **Zuweisung von Benutzerrechten**.

> **Hinweis:**
>
> In einem Einzelsitzungs-OS sind **Benutzer** in der Benutzerrechtzuweisung **Zeitzone ändern** enthalten. Dies gilt jedoch nicht in einem Multisitzungs-OS. In einem Multisitzungs-OS wird die Zeitzone über die folgende Gruppenrichtlinie synchronisiert: Computerkonfiguration\ Administrative Vorlagen\ Windows-Komponenten\Remotedesktopdienste\Remotedesktop-Sitzungshost\Geräte- und Ressourcenumleitung\Zeitzonenumleitung zulassen. Diese Richtlinie gilt nicht, wenn der Server kein Remotedesktop-Sitzungshost im VDA für Multisitzungs-OS ist (mit dem Befehl `/ServerVDI` installiert). In einem Multisitzungs-OS haben Benutzer standardmäßig nicht das lokale Recht, die Zeitzone zu ändern.

Einstellungen der Richtlinie "TWAIN-Geräte"

September 21, 2021

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)

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"

January 8, 2021

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 Einstellungen für **USB-Richtlinie** 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. Beschreibungen der verfügbaren Modi finden Sie in der Tabelle in diesem Artikel.

Nützliche Info

- Für Wacom Signatur-Tablets empfiehlt es sich, den Bildschirmschoner zu deaktivieren. Anweisungen zum Deaktivieren des Bildschirmschoners finden Sie am Ende dieses Abschnitts.
- Unterstützung für die Optimierung von Wacom-Signatur-Tablets der STU-Reihe ist in der Installation von Richtlinien bei Citrix Virtual Apps and Desktops vorkonfiguriert.
- Signaturgeräte funktionieren uneingeschränkt in Citrix Virtual Apps and Desktops und erfordern zur Verwendung als Signaturgerät keine Treiber. Wacom bietet zusätzliche Software an, die zur weiteren Anpassung des Geräts installiert werden kann. Siehe http://www.wacom.com/.
- Grafiktablets: Bestimmte Grafik-Eingabegeräte werden als HID-Gerät an einem PCI/ACPI-Bus präsentiert und nicht unterstützt. Schließen Sie solche Geräte an einen USB-Hostcontroller auf dem Client an, damit sie innerhalb der Citrix Virtual Desktops-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. Wählen Sie **Change** und dann **Yes**, wenn das Fenster für die 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	Vendor-ID vom Gerätedeskriptor
PID	Produkt-ID vom Gerätedeskriptor
REL	Release-ID vom Gerätedeskriptor
Klasse	Klasse vom Gerätedeskriptor oder ein Schnittstellendeskriptor
SubClass	Unterklasse vom Gerätedeskriptor oder ein Schnittstellendeskriptor

Tagname	Beschreibung
Prot	Protokoll vom Gerätedeskriptor oder ein Schnittstellendeskriptor

Wenn Sie 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 # Weitere Branche, Weiteres Flash-Laufwerk
- 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.

Konfigurieren der automatischen Umleitung von USB-Geräten

USB-Geräte werden automatisch umgeleitet, wenn die USB-Unterstützung aktiviert ist und die USB-Einstellungen für eine automatische Verbindung der USB-Geräte konfiguriert wurden.

> Hinweis:
>
> In Receiver für Windows 4.2 werden USB-Geräte auch automatisch umgeleitet, wenn das Gerät im Modus “Desktop Appliance”ist und der Verbindungsbalken nicht angezeigt wird. In älteren Citrix Receiver für Windows-Versionen werden USB-Geräte automatisch umgeleitet, wenn sie im

> Desktopgerätemodus oder mit von einer virtuellen Maschine gehosteten Anwendungen ausgeführt werden.

Die Umleitung aller USB-Geräte ist nicht immer ideal. Benutzer können Geräte, die nicht automatisch umgeleitet werden, explizit umleiten, indem sie sie aus der USB-Geräteliste auswählen. Um zu verhindern, dass USB-Geräte aufgelistet oder umgeleitet werden, verwenden Sie auf dem Clientendpunkt oder dem Virtual Desktop Agent (VDA) DeviceRules. Weitere Informationen finden Sie in der Dokumentation zur Verwaltung.

> Achtung
>
> 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.

Benutzereinstellungen für die automatische Umleitung von USB-Geräten

Richtlinie:

1. Öffnen Sie den **Editor für lokale Gruppenrichtlinien** und gehen Sie zu **Administrative Vorlagen > Citrix Komponenten > Citrix Receiver > Remoting von Clientgeräten > Generisches USB-Remoting**.
2. Öffnen Sie **Neue USB-Geräte**, wählen Sie **Aktiviert** und klicken Sie auf **OK**.
3. Öffnen Sie **Vorhandene USB-Geräte**, wählen Sie **Aktiviert** und klicken Sie auf **OK**.

Citrix Receiver:

1. Gehen Sie zu **Citrix Receiver-Einstellungen> Verbindungen**.
2. Stellen Sie sicher, dass die folgenden Optionen ausgewählt sind:
   - Geräte beim Start einer Sitzung automatisch verbinden
   - Wenn ein neues Gerät angeschlossen wird, während eine Sitzung ausgeführt wird, wird das Gerät automatisch verbunden
3. Klicken Sie auf **OK**.

Alle Registrierungsschlüssel und die Richtlinienänderungen werden auf das Windows-Clientgerät angewendet.

Umleitung einfacher USB-Drucker

Die beste Lösung für einfache USB-Drucker ist die Verwendung des dedizierten universellen Druckertreibers und eines virtuellen Kanals zum Drucken. Standardmäßig werden einfache USB-Drucker nicht automatisch umgeleitet.

Einfache Drucker werden unter Einsatz von Heuristik erkannt. Es wird zugrunde gelegt, dass komplexere Drucker, beispielsweise solche mit Scanfunktion, zur Gewährleistung des vollständigen Funktionsumfangs evtl. mithilfe von USB-Unterstützung umgeleitet werden müssen.

Verwenden Sie folgenden Registrierungsschlüssel, um festzulegen, ob einfache Drucker automatisch umgeleitet werden sollen:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

Name: AutoRedirectPrinters

Typ: DWORD

Daten: 00000000

Der Standardwert ist 0 (keine automatische Umleitung). Wenn Sie einen Wert größer als Null festlegen, wird die USB-Unterstützung zur Umleitung einfacher USB-Drucker aktiviert.

Sie können auch Active Directory-Richtlinien für diesen Registrierungsschlüssel bereitstellen und den Nicht-Richtlinienwert bei Vorhandensein beider Werte außer Kraft setzen:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

Name: AutoRedirectAudio

Typ: DWORD

Daten: 00000000

Umleitung einfacher Audiogeräte

Wie bei einfachen Druckern wird beim Senden von Audiodaten von einfachen Audiogeräten die beste Benutzererfahrung mit dem dedizierten virtuellen Audiokanal von ICA erreicht. Möglicherweise ist jedoch für Spezialgeräte eine Umleitung mithilfe der USB-Unterstützung erforderlich. Die Bestimmung einfacher Audiogeräte erfolgt mithilfe von Heuristik.

Verwenden Sie folgenden Registrierungsschlüssel, um festzulegen, ob einfache Audiogeräte automatisch umgeleitet werden sollen:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

Name: AutoRedirectAudio

Typ: DWORD

Daten: 00000000

Der Standardwert ist 0 (keine automatisch Umleitung). Wenn Sie einen anderen Wert als Null festlegen, erfolgt die Umleitung einfacher USB-Audiogeräte per USB-Unterstützung.

Sie können Active Directory-Richtlinien zum Bereitstellen dieses Werts für den Registrierungsschlüssel verwenden und den Nicht-Richtlinienwert bei Vorhandensein beider Werte außer Kraft setzen:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

Name: AutoRedirectVideo

Typ: DWORD

Daten: 00000000

Umleitung einfacher Speichergeräte (Massenspeicher)

Bei einfachen Speichergeräten erzielen Sie mit dem dedizierten virtuellen Kanal, z. B. per Clientlaufwerkzuordnung, bei der außerdem eine Optimierung erfolgt, die beste Benutzererfahrung. Für spezielle Vorgänge neben dem einfachen Lesen und Schreiben von Dateien, etwa zum Brennen von DVDs oder für den Zugriff auf verschlüsselte Dateisysteme, müssen Geräte evtl. dennoch über die allgemeine USB-Unterstützung umgeleitet werden.

Die Bestimmung einfacher Speichergeräte erfolgt mithilfe von Heuristik. Verwenden Sie folgenden Registrierungsschlüssel, um festzulegen, ob einfache Speichergeräte automatisch umgeleitet werden sollen:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

Name: AutoRedirectStorage

Typ: DWORD

Daten: 00000000

Der Standardwert ist 0 (keine automatisch Umleitung). Wenn Sie einen anderen Wert als Null festlegen, erfolgt die Umleitung einfacher USB-Speichergeräte per USB-Unterstützung.

Sie können auch Active Directory-Richtlinien zum Bereitstellen dieses Werts für den folgenden Registrierungsschlüssel verwenden und den Nicht-Richtlinienwert bei Vorhandensein beider Werte außer Kraft setzen:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

Name: AutoRedirectStorage

Typ: DWORD

Daten: 00000000

> Hinweis:
>
> Der Lesezugriff auf einfache Speichergeräte ist bei Verwendung der generischen USB-Unterstützung nicht konfigurierbar. Bei Verwendung der Clientlaufwerkzuordnung ist er konfigurierbar.

Umleitung von USB-Speichersticks mit Hardwareverschlüsselung

USB-Speichersticks mit Hardwareverschlüsselung bestehen in der Regel aus einer verschlüsselten Speicherpartition und einer *Hilfsprogrammpartition*, die ein Hilfsprogramm zum Entsperren der verschlüsselten Partition enthält. Bei USB-Speichersticks erzielen Sie mit dem dedizierten virtuellen HDX-Kanal per Clientlaufwerkzuordnung/dynamischer Thumbdrive-Zuordnung, bei der außerdem eine Optimierung erfolgt, die beste Benutzererfahrung.

Die generische USB-Umleitung ist erforderlich für Nicht-Windows-Clients (z. B. Linux-Clients) und für Clients, bei denen der Benutzerzugriff auf lokale Clientfunktionen eingeschränkt wurden. Die generische USB-Umleitung kann jedes USB-Speichergerät ohne Hardwareverschlüsselung in VDA-Sitzungen mit Einzel- und Multisitzungs-OS umleiten.

Vor Citrix Virtual Apps and Desktop 7 1808 konnten USB-Speichersticks mit Hardwareverschlüsselung nicht vernünftig in VDA-Sitzungen mit Einzel- und Multisitzungs-OS umgeleitet werden. Eine neue Erweiterung in Citrix Virtual Apps and Desktop 7 1808 unterstützt die generische USB-Umleitung von USB-Speichersticks mit Hardwareverschlüsselung in VDA-Sitzungen mit Einzel- und Multisitzungs-OS.
Nachdem das Gerät umgeleitet wurde, wird keines seiner Laufwerke auf dem lokalen Client angezeigt. Muss ein Laufwerk entsperrt werden, tun Sie das daher in der Sitzung. Dieses Feature erfordert Windows-Update KB4074590.

Einfache Standbildgeräte (Scanner und Digitalkameras)

Bei einfachen Standbildgeräten erzielen Sie mit dem dedizierten virtuellen Kanal, (z. B. TWAIN), bei dem außerdem eine Optimierung erfolgt, die beste Benutzererfahrung. Die Geräte müssen Industriestandards einhalten. Ist ein Gerät nicht konform oder soll es nicht gemäß dem ursprünglichen Zweck verwendet werden, ist eine generische USB-Umleitung evtl. die einzige Möglichkeit, das Gerät zu verwenden. Die Bestimmung einfacher Standbildgeräte erfolgt mithilfe von Heuristik.

Verwenden Sie folgenden Registrierungsschlüssel, um festzulegen, ob einfache Standbildgeräte automatisch umgeleitet werden sollen:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

Name: AutoRedirectImage

Typ: DWORD

Daten: 00000000

Der Standardwert ist 0 (keine automatisch Umleitung). Wenn Sie einen anderen Wert als Null festlegen, erfolgt die Umleitung einfacher USB-Standbildgeräte per USB-Unterstützung.

Sie können auch Active Directory-Richtlinien zum Bereitstellen dieses Werts für den Registrierungsschlüssel verwenden und den Nicht-Richtlinienwert bei Vorhandensein beider Werte außer Kraft setzen:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

Name: AutoRedirectImage

Typ: DWORD

Daten: 00000000

Gerätespezifische Einstellungen

Die Heuristik zur Auswahl Citrix-optimierbarer Geräte (Drucker, Audio-, Video-, Speichergeräte usw.) entspricht nicht in jedem Fall Ihren Wünschen. In Einzelfällen ist ggf. die Steuerung der automatischen Umleitung von Geräten, die oben nicht aufgeführt sind, erwünscht. Sie können die automatische Umleitung gerätespezifisch steuern.

Beispiel: Der Barcodeleser DemoTech 2000 muss nicht unter Einsatz der USB-Unterstützung umgeleitet werden. Seine Hersteller-ID lautet "12AB", die Produkt-ID "5678". Diese Hexadezimalzahlen finden Sie in Device Manager.

Um die automatische Umleitung zu unterbinden, erstellen Sie folgenden gerätespezifischen Registrierungsschlüssel:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices\VID12AB PID5678

Name: AutoRedirect

Typ: DWORD

Daten: 00000000

Der Wert 0 verhindert, dass das Gerät automatisch umgeleitet wird. Ein Wert ungleich Null bedeutet, dass das Gerät für die automatische Umleitung in Betracht gezogen werden muss (abhängig von den Benutzereinstellungen). Zwischen den Hersteller- und Produkt-ID steht ein einzelnes Leerzeichen.

Sie können diesen Wert auch über Active Directory-Richtlinien für den Registrierungsschlüssel bereitstellen. Dabei wird der Nicht-Richtlinienwert bei Vorhandensein beider Werte außer Kraft gesetzt:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices\VID12AB PID5678

Name: AutoRedirect

Typ: DWORD

Daten: 00000000

Gerätespezifische AutoRedirect-Einstellungen haben Vorrang vor den allgemeineren AutoRedirectXXX-Werten, die oben erläutert wurden. Die Standardheuristik für Citrix optimierte Geräte kann ein Gerät als generisch interpretieren. Legen Sie daher den gerätespezifischen AutoRedirect-Wert auf 1 fest, um eine automatische Umleitung zu erzielen.

Einstellungen der Richtlinie "Visuelle Anzeige"

September 21, 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. Mit dieser Einstellung wird die Leistung bei Netzwerkverbindungen mit beschränkter Bandbreite verbessert.
- **Immer verlustfrei:** Wenn kein Qualitätsverlust akzeptabel ist, wählen Sie "Immer verlustfrei" , um sicherzustellen, dass keine verlustreichen Daten an das Benutzergerät gesendet werden. Ein Beispiel hierfür wären Röntgenbilder.

Einstellungen der Richtlinie "Bewegtbilder"

February 6, 2020

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 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”

February 6, 2020

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 der Citrix Workspace-App 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 Röntgenbildern, 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”

September 21, 2021

Der Abschnitt “WebSockets”enthält Richtlinieneinstellungen für den Zugriff auf virtuelle Desktops und gehostete Anwendungen mit der Citrix Workspace-App 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 die Citrix Workspace-App für Web, in Form von URLs. Der Server akzeptiert nur WebSockets-Verbindungen, die von einer dieser Adressen stammen.

Standardmäßig wird der Platzhalter * verwendet. Damit wird allen URLs der Citrix Workspace-App für Web vertraut.

Wenn Sie eine Adresse in die Liste eingeben möchten, verwenden Sie folgende Syntax:

<Protokoll>://<Vollqualifizierter Domänenname des Hosts>:[[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”

September 21, 2021

Der Abschnitt “Lastverwaltung”enthält Richtlinieneinstellungen für das Aktivieren und Konfigurieren des Lastausgleichs zwischen Servern, über die Maschinen mit Windows-Multisitzungs-OS 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”

March 15, 2022

Dieser Abschnitt 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

November 30, 2020

Anzahl Wiederholungen beim Zugriff auf gesperrte Dateien

Legt die Anzahl der Wiederholungen beim Zugriff auf gesperrte Dateien fest.

Wenn diese Richtlinie deaktiviert ist, werden standardmäßig fünf Wiederholungen unternommen. Wenn diese Richtlinie hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet. Wenn diese Richtlinie weder hier noch in der INI-Datei konfiguriert ist, wird der Standardwert verwendet.

Internet-Cookiedateien bei Abmeldung verarbeiten

In manchen Bereitstellungen werden zusätzliche Internet-Cookies zurückgelassen, auf die es keine Verweise in der Datei Index.dat gibt. Nach längerem Browsen im Internet können diese zusätzlichen Cookies das Profil aufblähen. Aktivieren Sie diese Richtlinie, um die Verarbeitung von Index.dat zu erzwingen und die zusätzlichen Cookies zu entfernen. Die Richtlinie verlängert die Abmeldezeiten. Aktivieren Sie sie daher nur, wenn dieses Problem bei Ihnen auftritt.

Wenn diese Richtlinie hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet. Wenn diese Richtlinie weder hier noch in der INI-Datei konfiguriert ist, wird Index.dat nicht verarbeitet.

Automatische Konfiguration deaktivieren

Die Profilverwaltung überprüft alle Citrix Virtual Desktops-Umgebungen beispielsweise auf das Vorhandensein von persönlichen vDisks und konfiguriert die Gruppenrichtlinie entsprechend. Nur Richtlinien der Profilverwaltung im Zustand Nicht konfiguriert werden angepasst, damit Ihre Anpassungen gespeichert bleiben. 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 Citrix Virtual Apps 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 Richtlinien für verschiedene Betriebssysteme:

	Multisitzungs-OS	Einzelsitzungs-OS
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.
Profilstreaming	Aktiviert	*Deaktiviert*, wenn Personal vDisk verwendet wird, sonst aktiviert.

Wenn jedoch die automatische Konfiguration deaktiviert ist, werden alle oben genannten Richtlinien standardmäßig **deaktiviert**.

Ab der Profilverwaltungsversion 1909 können Sie die Benutzerfreundlichkeit des Startmenüs unter Windows 10 (Version 1607 und höher) und Windows Server 2016 und höher verbessern. Diese Verbesserung wird durch die automatische Konfiguration der folgenden Richtlinien erreicht:

- Hinzufügen von "Appdata\Local\Microsoft\Windows\Caches"und "Appdata\Local\Packages" zu "Folders to Mirror"
- Hinzufügen von "Appdata\Local\Microsoft\Windows\UsrClass.Dat*"zu "Files to synchronize"

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung wieder hier noch in der INI-Datei konfiguriert ist, ist die automatische Konfiguration aktiviert. Die Einstellungen der Profilverwaltung können sich daher bei geänderter Umgebung ändern.

Benutzer bei Problem abmelden

Wenn diese Richtlinie deaktiviert oder nicht konfiguriert ist, erhalten Benutzer ein temporäres Profil, wenn ein Problem auftritt (Der Benutzerspeicher ist z. B. nicht verfügbar). Wenn sie aktiviert ist, wird eine Fehlermeldung angezeigt, und Benutzer werden abgemeldet. Dieses Setup kann die Problembehandlung vereinfachen.

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.

Programm zur Verbesserung der Benutzerfreundlichkeit

Das Programm zur Verbesserung der Benutzerfreundlichkeit ist standardmäßig aktiviert, damit die Qualität und Leistung von Citrix-Produkten verbessert werden kann, indem anonyme Statistiken und Nutzungsinformationen gesendet werden.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Suchindex-Roaming für Outlook aktivieren

Ermöglicht eine native Outlook-Suche, indem automatisch Roaming für Outlook-Suchdaten zusammen mit dem Benutzerprofil eingerichtet wird. Dies erfordert zusätzlichen Speicherplatz im Benutzerspeicher, um den Suchindex für Outlook zu speichern.

Sie müssen sich abmelden und dann neu anmelden, damit diese Richtlinie wirksam wird.

Outlook-Suchindexdatenbank - Backup und Wiederherstellen

Mit dieser Einstellung wird vorgegeben, was bei der Anmeldung geschieht, wenn das Suchindex-Roaming für Outlook aktiviert ist.

Wenn diese Einstellung aktiviert ist, speichert die Profilverwaltung jedes Mal ein Backup der Suchindexdatenbank, wenn diese bei der Anmeldung erfolgreich bereitgestellt wird. Die Profilverwaltung behandelt das Backup als fehlerfreie Kopie der Suchindexdatenbank. Wenn ein Versuch, die Suchindexdatenbank bereitzustellen, aufgrund einer Beschädigung der Datenbank fehlschlägt, wird diese automatisch auf die letzte als fehlerfrei bekannte Kopie zurückgesetzt.

Hinweis: Das zuvor gespeicherte Backup wird gelöscht, wenn ein neues erfolgreich gespeichert wurde. Das Backup verbraucht Speicherplatz der VHDX-Dateien.

Grundlegende Richtlinieneinstellungen

November 30, 2020

Dieser Abschnitt enthält Richtlinieneinstellungen für die grundlegende Konfiguration der Profilverwaltung.

Profilverwaltung aktivieren

Um die Bereitstellung zu erleichtern, verarbeitet die Profilverwaltung keine An- oder Abmeldungen. Aktivieren Sie die Profilverwaltung erst, nachdem Sie alle anderen Setupaufgaben ausgeführt haben und getestet haben, wie sich Citrix-Benutzerprofile in Ihrer Umgebung verhalten.

Wenn diese Richtlinie hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet. Wenn diese Richtlinie weder hier noch in der INI-Datei konfiguriert ist, verarbeitet die Profilverwaltung keine Windows-Benutzerprofile.

Verarbeitete Gruppen

Sie können Gruppen auf dem lokalen Computer und Domänengruppen (lokal, global und universal) verwenden. Domänengruppen müssen in folgendem Format angegeben werden: DOMÄNENNAME\GRUPPENNAME.

Wenn diese Richtlinie hier konfiguriert ist, verarbeitet die Profilverwaltung nur Mitglieder dieser Benutzergruppen. Wenn diese Richtlinie deaktiviert ist, verarbeitet die Profilverwaltung alle Benutzer. Wenn diese Richtlinie 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 Mitglieder aller Benutzergruppen verarbeitet.

Ausgeschlossene Gruppen

Sie können mit lokalen Computergruppen und Domänengruppen (lokal, global und universell) die Verarbeitung bestimmter Benutzerprofile verhindern. Geben Sie Domänengruppen im Format DOMÄNENNAME\GRUPPENNAME an.

Wenn diese Einstellung hier konfiguriert ist, schließt die Profilverwaltung Mitglieder dieser Benutzergruppen aus. Wenn diese Einstellung deaktiviert ist, schließt die Profilverwaltung keine Benutzer aus. 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 Mitglieder aller Gruppen ausgeschlossen.

Anmeldungen lokaler Administratoren verarbeiten

Gibt an, ob Anmeldungen von Mitgliedern der Gruppe "VORDEFINIERT\Administratoren"verarbeitet werden. Wenn diese Richtlinie auf Maschinen mit Multisitzungs-OS (z. B. Citrix Virtual Apps-Umgebungen) deaktiviert oder nicht konfiguriert ist, nimmt die Profilverwaltung an, dass Anmeldungen von Domänenbenutzern, aber nicht von lokalen Administratoren, verarbeitet werden müssen. Unter Einzelsitzungs-OS (z. B. Citrix Virtual Desktops-Umgebungen) werden Anmeldungen lokaler Administratoren verarbeitet. Mit dieser Richtlinie können Domänenbenutzer mit lokalen Administratorrechten, normalerweise Citrix Virtual Desktops-Benutzer mit zugewiesenen virtuellen Desktops, die Verarbeitung umgehen, sich anmelden und Probleme mit der Desktoperfahrung mit der Profilverwaltung beheben.

Hinweis: Domänenbenutzeranmeldungen unterliegen möglicherweise Einschränkungen aufgrund ihrer Gruppenmitgliedschaft. Dies dient üblicherweise dazu, die Einhaltung von Lizenzvereinbarungen für Software zu gewährleisten.
Wenn diese Richtlinie deaktiviert ist, verarbeitet die Profilverwaltung die Anmeldungen lokaler Administratoren nicht. Wenn diese Richtlinie 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 Administratoren nicht verarbeitet.

Pfad zu Benutzerspeicher

Legt den Pfad zu dem Verzeichnis (dem Benutzerspeicher) fest, in dem die Benutzereinstellungen (Registrierungsänderungen und synchronisierte Dateien) gespeichert werden.

Mögliche Pfade:

- Relativer Pfad. Dieser Pfad muss relativ zum Stammverzeichnis sein (normalerweise mit dem Attribut #homeDirectory# für einen Benutzer in Active Directory konfiguriert).
- 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.

Folgende Variablentypen können für diese Richtlinie verwendet werden.

- Systemumgebungsvariablen in Prozentzeichen (z. B. %ProfVer%). Systemumgebungsvariablen erfordern im Allgemeinen eine zusätzliche Einrichtung.
- Attribute des Active Directory-Benutzerobjekts in Rauten (z. B. #sAMAccountName#).
- Profilverwaltungsvariablen: Weitere Informationen finden Sie in der Produktdokumentation unter "Profilverwaltungsvariablen".

Benutzerumgebungsvariablen können nicht verwendet werden. Ausnahmen sind %username% und %userdomain%. Sie können auch eigene 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$%USERNAME%.%USERDOMAIN%!CTX_OSNAME!!CTX_OSBITNESS! kann erweitert werden zu \server\profiles$\JohnSmith.DOMAINCONTROLLER1\Win8x64

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. Wenn sich diese Datei z. B. in \server\profiles$\JohnSmith.Finance\Win8x64\UPM_Profile befindet, geben Sie den Pfad zum Benutzerspeicher als \server\profiles$\JohnSmith.Finance\Win8x64 an (ohne den Unterordner \UPM_Profile).

Weitere Informationen dazu, wie Sie den Pfad zum Benutzerspeicher mit Variablen angeben, finden Sie in den folgenden Abschnitten:

- Gemeinsames Verwenden von Citrix-Benutzerprofilen auf mehreren Dateiservern
- Verwalten von Profilen in Organisationseinheiten und organisationseinheitsübergreifend
- Hochverfügbarkeit und Notfallwiederherstellung mit der Profilverwaltung

Wenn Pfad zum Benutzerspeicher deaktiviert ist, werden die Benutzereinstellungen im Windows-Unterverzeichnis des Basisverzeichnisses gespeichert.

Wenn diese Richtlinie deaktiviert ist, werden die Benutzereinstellungen im Windows-Unterverzeichnis des Basisverzeichnisses gespeichert. Wenn diese Richtlinie hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet. Wenn diese Richtlinie weder hier noch in der INI-Datei konfiguriert ist, wird das Windows-Verzeichnis auf dem Basislaufwerk verwendet.

Migrieren des Benutzerspeichers

Gibt den Pfad zu dem Ordner an, in dem die Benutzereinstellungen (Registrierungsänderungen und synchronisierte Dateien) zuvor gespeichert waren (d. h. der zuvor verwendete Benutzerspeicherpfad).

Wenn die Einstellung konfiguriert ist, werden die im vorherigen Benutzerspeicher gespeicherten Benutzereinstellungen in den aktuellen Benutzerspeicher migriert, der in der Richtlinie "Pfad zum Benutzerspeicher"angegeben ist.

Der Pfad kann ein absoluter UNC-Pfad oder ein relativer Pfad zum Basisverzeichnis sein.

In beiden Fällen können Sie sowohl Systemumgebungsvariablen, die in Prozentzeichen eingeschlossen sind, als auch Attribute des Active Directory-Benutzerobjekts in Rautenzeichen eingeschlossen verwenden.

Beispiele:

- Die Benutzereinstellungen werden von Ordner `Windows\\%ProfileVer%` in den Unterordner `Windows\W2K3` des Benutzerspeichers gespeichert (wenn %ProfileVer% eine Systemumgebungsvariable ist, die in W2K3 aufgelöst wird).
- `\\server\share\\#SAMAccountName#` speichert die Benutzereinstellungen im UNC-Pfad `\\server\share\<JohnSmith>` (wenn `#SAMAccountName#` für den aktuellen Benutzer in JohnSmith aufgelöst wird).

Im Pfad können Sie Benutzerumgebungsvariablen außer `%username%` und `%userdomain%` verwenden.

Wenn diese Einstellung deaktiviert ist, werden die Benutzereinstellungen im aktuellen Benutzerspeicher gespeichert.

Wenn diese Einstellung hier nicht konfiguriert ist, wird die zugehörige Einstellung in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden die Benutzereinstellungen im aktuellen Benutzerspeicher gespeichert.

Aktiv zurückschreiben

Geänderte Dateien und Ordner (aber keine Registrierungseinträge) können mitten in der Sitzung und vor der Abmeldung in den Benutzerspeicher synchronisiert werden.

Wenn diese Richtlinie hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet. Wenn diese Richtlinie weder hier noch in der INI-Datei konfiguriert ist, ist sie aktiviert.

Unterstützung von Offlineprofilen

Mit dieser Richtlinie können Profile zum nächstmöglichen Zeitpunkt mit dem Benutzerspeicher synchronisiert werden. Sie ist für mobile Benutzer gedacht, die Laptops oder andere mobile Geräte verwenden. 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 worden ist.

Wenn diese Richtlinie hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet. Wenn diese Richtlinie weder hier noch in der INI-Datei konfiguriert ist, sind Offlineprofile deaktiviert.

Aktives Zurückschreiben der Registrierung

Verwenden Sie diese Richtlinie zusammen mit "Aktiv zurückschreiben". Registrierungseinträge, die geändert wurden, können während der Sitzung mit dem Benutzerspeicher synchronisiert werden.

Wenn Sie diese Einstellung hier nicht konfigurieren, wird der Wert in der INI-Datei verwendet.

Wenn Sie diese Einstellung weder hier noch in der INI-Datei konfigurieren, ist das aktive Zurückschreiben der Registrierung deaktiviert.

Unterstützung von Offlineprofilen

Aktiviert Offlineprofile. Dieses Feature ist für Computer gedacht, die häufig aus Netzwerken entfernt werden, in der Regel Laptops oder mobile Geräte, nicht Server oder Desktops.

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.

Plattformübergreifende Richtlinieneinstellungen

November 30, 2020

Dieser Abschnitt enthält Richtlinieneinstellungen für die Konfiguration der plattformübergreifenden Einstellungen der Profilverwaltung.

Plattformübergreifende Einstellungen aktivieren

Um die Bereitstellung zu vereinfachen, sind die plattformübergreifenden Einstellungen standardmäßig deaktiviert. Aktivieren Sie die Verarbeitung, indem Sie diese Richtlinie aktivieren. Tun Sie dies nur, nachdem Sie dieses Feature ausreichend geplant und getestet haben.

Wenn diese Richtlinie 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 plattformübergreifenden Einstellungen angewendet.

Benutzergruppen für plattformübergreifende Einstellungen

Geben Sie mindestens eine Windows-Benutzergruppe ein. Sie möchten mit dieser Richtlinie z. B. erreichen, dass nur die Profile einer Testbenutzergruppe verarbeitet werden. Wenn diese Richtlinie konfiguriert ist, werden nur Mitglieder dieser Benutzergruppen vom Profilverwaltungs-Feature für plattformübergreifende Einstellungen verarbeitet. Wenn diese Richtlinie deaktiviert ist, verarbeitet das Feature alle Benutzer, die in der Richtlinie "Verarbeitete Gruppen"angegeben sind.

Wenn diese Richtlinie 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 alle Benutzergruppen verarbeitet.

Pfad zu plattformübergreifenden Definitionen

Gibt den Netzwerkspeicherort der Definitionsdateien an, die Sie aus dem Downloadpaket kopiert haben. Dies muss ein UNC-Pfad sein. Benutzer benötigen Lesezugriff auf diesen Speicherort und Administratoren benötigen Schreibzugriff. Der Speicherort muss ein Server Message Block (SMB) oder eine Common Internet File System (CIFS)-Dateifreigabe sein.

Wenn diese Richtlinie 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 plattformübergreifenden Einstellungen angewendet.

Pfad zum Speicher für plattformübergreifende Einstellungen

Gibt den Pfad zum Speicher für plattformübergreifende Einstellungen an. Dies ist der Ordner, in dem die plattformübergreifenden Einstellungen der Benutzer gespeichert werden. Benutzer benötigen

Schreibzugriff auf diesen Bereich. Der Pfad kann ein absoluter UNC-Pfad oder ein relativer Pfad zum Basisverzeichnis sein.

Dies ist der Bereich des Benutzerspeichers mit Profildaten, die von mehreren Plattformen gemeinsam verwendet werden. Benutzer benötigen Schreibzugriff auf diesen Bereich. Der Pfad kann ein absoluter UNC-Pfad oder ein relativer Pfad zum Basisverzeichnis sein. Sie können dieselben Variablen wie für Pfad zum Benutzerspeicher verwenden.

Wenn diese Richtlinie deaktiviert ist, wird der Pfad Windows\PM_CP verwendet. Wenn diese Richtlinie hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet. Wenn diese Richtlinie weder hier noch in der INI-Datei konfiguriert ist, wird der Standardwert verwendet.

Quelle für Erstellung plattformübergreifender Einstellungen

Legt eine Plattform als Basisplattform fest, wenn diese Richtlinie in der Organisationseinheit der Plattform aktiviert ist. Diese Richtlinie migriert Daten von den Profilen der Basisplattform in den Speicher für plattformübergreifende Einstellungen.

Die Profile jeder Plattform werden in einer separaten Organisationseinheit gespeichert. Sie müssen die Plattform auswählen, deren Profildaten zum Füllen des Speichers für plattformübergreifende Einstellungen verwendet werden sollen. Dies wird als Basisplattform bezeichnet. Wenn der Speicher für plattformübergreifende Einstellungen eine Definitionsdatei ohne Daten enthält oder die zwischengespeicherten Daten eines Einzelplattformprofils neuer sind als die Definitionsdaten im Speicher, migriert die Profilverwaltung die Daten des Einzelplattformprofils in den Speicher, wenn Sie diese Richtlinie nicht deaktivieren.

> **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 Richtlinie aktiviert.

Einstellungen der Richtlinie “Dateisystem”

November 30, 2020

Dieser Abschnitt enthält Richtlinien 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 30, 2020

Dieser Abschnitt enthält Richtlinieneinstellungen zum Konfigurieren der Dateien und Verzeichnisse in einem Benutzerprofil, die von der Synchronisierung ausgeschlossen werden sollen.

Ausschlussliste - Dateien

Liste der Dateien, die bei der Synchronisierung ignoriert werden. Dateinamen müssen Pfade sein, die relativ zum Benutzerprofil sind (%USERPROFILE%). Platzhalter sind zulässig und werden rekursiv angewendet.

Beispiele:

- “Desktop\Desktop.ini”ignoriert die Datei Desktop.ini im Verzeichnis “Desktop”.
- %USERPROFILE%*.tmp ignoriert alle Dateien mit der Erweiterung .tmp im gesamten Profil
- AppData\Roaming\MyApp*.tmp ignoriert alle Dateien mit der Erweiterung .tmp in einem Teil des Profils

Wenn diese Richtlinie deaktiviert ist, werden keine Dateien ausgeschlossen. Wenn diese Richtlinie 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 Dateien ausgeschlossen.

Standardausschlussliste der Verzeichnisse aktivieren

Die während der Synchronisierung ignorierte Standardliste der Verzeichnisse. Verwenden Sie diese Liste, um die GPO-Ausschlussverzeichnisse anzugeben, ohne sie manuell ausfüllen zu müssen.

Wenn Sie diese Richtlinie deaktivieren, werden keine Verzeichnisse standardmäßig von der Profilverwaltung ausgeschlossen. Wenn Sie diese Richtlinie hier nicht konfigurieren, wird der Wert in der INI-Datei von der Profilverwaltung verwendet. Wenn Sie diese Richtlinie hier oder in der INI-Datei nicht konfigurieren, werden standardmäßig keine Verzeichnisse von der Profilverwaltung ausgeschlossen.

Ausschlussliste - Verzeichnisse

Liste der Ordner, die bei der Synchronisierung ignoriert werden. Ordnernamen müssen Pfade sein, die relativ zum Benutzerprofil sind (%USERPROFILE%).

Beispiel:

- Desktop ignoriert den Ordner "Desktop"im Benutzerprofil.

Wenn diese Richtlinie deaktiviert ist, werden keine Ordner ausgeschlossen. Wenn diese Richtlinie 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 ausgeschlossen.

Anmeldeausschlussprüfung

Mit dieser Einstellung wird die Vorgehensweise der Profilverwaltung konfiguriert, falls ein Profil im Benutzerspeicher ausgeschlossene Dateien oder Ordner enthält.

Wenn die Einstellung deaktiviert oder auf den Standardwert **Ausgeschlossene Dateien oder Ordner bei Anmeldung synchronisieren** festgelegt ist, synchronisiert die Profilverwaltung die ausgeschlossenen Dateien oder Ordner vom Benutzerspeicher in das lokale Profil, wenn ein Benutzer sich anmeldet.

Wenn die Einstellung auf **Ausgeschlossene Dateien oder Ordner bei Anmeldung ignorieren** festgelegt ist, ignoriert die Profilverwaltung die ausgeschlossenen Dateien oder Ordner, wenn ein Benutzer sich anmeldet.

Wenn die Einstellung auf **Ausgeschlossene Dateien oder Ordner bei Anmeldung löschen** festgelegt ist, werden die ausgeschlossenen Dateien bei der Anmeldung eines Benutzers von der Profilverwaltung gelöscht.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn die Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden die ausgeschlossenen Dateien oder Ordner bei der Anmeldung eines Benutzers vom Benutzerspeicher in das lokale Profil synchronisiert.

Verarbeitung von großen Dateien: Dateien werden als symbolische Verknüpfungen erstellt

Um die Anmeldeleistung zu verbessern und große Dateien zu verarbeiten, wird eine symbolische Verknüpfung erstellt, anstatt die Dateien in dieser Liste zu kopieren.

Sie können Platzhalter in Richtlinien verwenden, die sich auf Dateien beziehen. Beispiel: `!ctx_localappdata!\Microsoft\Outlook\*.OST`.

Um die Offlineordnerdatei (`*.ost`) von Microsoft Outlook zu verarbeiten, stellen Sie sicher, dass der **Outlook**-Ordner nicht von der Citrix Profilverwaltung ausgeschlossen ist.

Hinweis: Auf diese Dateien kann nicht gleichzeitig in mehreren Sitzungen zugegriffen werden.

Einstellungen der Richtlinie "Synchronisierung"

November 30, 2020

Dieser Abschnitt enthält Richtlinieneinstellungen für die Angabe, welche Dateien und Ordner in einem Benutzerprofil zwischen dem System, auf dem das Profil installiert ist, und dem Benutzerspeicher synchronisiert werden.

Zu synchronisierende Verzeichnisse

Die Profilverwaltung synchronisiert die vollständigen Profile aller Benutzer zwischen dem System, auf dem sie installiert ist, und dem Benutzerspeicher. Es ist nicht erforderlich, Unterordner des Benutzerprofils einzuschließen, indem Sie sie dieser Liste hinzufügen.

Pfade in dieser Liste müssen relativ zum Benutzerprofil sein.

Beispiel:

- Desktop\ausschließen\aufnehmen gibt den Unterordner "aufnehmen"des Verzeichnisses Desktop\ausschließen an.

Deaktivieren dieser Richtlinie hat dieselbe Auswirkung, wie wenn Sie sie aktivieren und eine leere Liste konfigurieren.

Wenn diese Richtlinie 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 nur nicht ausgeschlossene Ordner im Benutzerprofil synchronisiert.

Zu synchronisierende Dateien

Die Profilverwaltung synchronisiert die vollständigen Profile aller Benutzer zwischen dem System, auf dem sie installiert ist, und dem Benutzerspeicher. Es ist nicht erforderlich, Dateien in dem Benutzerprofil einzuschließen, indem Sie sie dieser Liste hinzufügen.

Mit dieser Richtlinie können Dateien unter ausgeschlossenen Ordnern eingeschlossen werden. Pfade in dieser Liste müssen relativ zum Benutzerprofil sein. 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.

Deaktivieren dieser Richtlinie hat dieselbe Auswirkung, wie wenn Sie sie aktivieren und eine leere Liste konfigurieren.

Wenn diese Richtlinie 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 nur nicht ausgeschlossene Dateien im Benutzerprofil synchronisiert.

Zu spiegelnde Ordner

Diese Richtlinie kann zur Lösung von Problemen mit Transaktionsordnern beitragen (auch als Referenzordner bezeichnet). Dieser Ordner enthält voneinander abhängige Dateien, wobei eine Datei auf andere verweist. Durch das Spiegeln von Ordnern kann die Profilverwaltung einen Transaktionsordner und seinen Inhalt als eine Entität verarbeiten. So wird das Aufblähen von Profilen verhindert. Sie können z. B. den Cookies-Ordner von Internet Explorer spiegeln, damit Index.dat mit den Cookies synchronisiert wird, auf die die Datei verweist. In diesen Situationen hat der letzte Schreibvorgang Priorität. Also werden Dateien in gespiegelten Ordnern, die in mehr als einer Sitzung geändert wurden, von der letzten Aktualisierung überschrieben. Hierdurch gehen Profiländerungen verloren.

Überlegen Sie z. B., wie Index.dat auf Cookies verweist, während ein Benutzer im Internet browst. 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 auf dem neuesten Stand.

Wenn diese Richtlinie 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.

Profilcontainer

Ein Profilcontainer ist eine VHDX-basierte Profillösung, mit der Sie die Ordner angeben können, die im Profildatenträger enthalten sein sollen (VHDX-Datei). Der Profilcontainer fügt den Profildatenträger

an, der diese Ordner enthält, sodass keine Kopie der Ordner im lokalen Profil gespeichert werden muss. Dadurch verkürzt sich die Anmeldezeiten.

Um einen Profilcontainer zu verwenden, aktivieren Sie diese Richtlinie und fügen der Liste die relativen Pfade der Ordner hinzu. Citrix empfiehlt, die Ordner mit großen Cachedateien in die Liste aufzunehmen. Nehmen Sie beispielsweise den Inhaltscacheordner für **Citrix Files** in die Liste auf: `AppData\Local\Citrix\Citrix Files\PartCache`.

Es sind zwei Szenarien zu beachten:

- Profilcontainer unterstützen keinen gleichzeitigen Zugriff durch mehrere Sitzungen.
- Profilcontainer unterstützen nicht, dass das gesamte Profil darin enthalten ist.

Wenn diese Richtlinie hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet. Wenn diese Richtlinie weder hier noch in der INI-Datei konfiguriert ist, ist sie deaktiviert.

Einstellungen der Richtlinie "Ordnerumleitung"

November 30, 2020

Dieser Abschnitt 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.

> **Hinweis:**
>
> Durch diese Einstellung werden Berechtigungen Administratoren erteilt, die Vollzugriff auf die Domäne haben.

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)"

November 30, 2020

Dieser Abschnitt enthält Richtlinieneinstellungen für die Umleitung des Inhalts des Ordners **AppData(Roaming)** an einen freigegebenen Speicherort im Netzwerk.

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"

September 21, 2021

Dieser Abschnitt enthält Richtlinieneinstellungen für die Umleitung des Inhalts des Ordners **Kontakte** an einen freigegebenen Speicherort im Netzwerk.

'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"

November 30, 2020

Dieser Abschnitt enthält Richtlinieneinstellungen für die Umleitung des Inhalts des Ordners **Desktop** an einen freigegebenen Speicherort im Netzwerk.

'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"

September 21, 2021

Dieser Abschnitt enthält Richtlinieneinstellungen für die Umleitung des Inhalts des Ordners **Dokumente** an einen freigegebenen Speicherort im Netzwerk.

'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"

November 30, 2020

Dieser Abschnitt enthält Richtlinieneinstellungen für die Umleitung des Inhalts des Ordners **Downloads** an einen freigegebenen Speicherort im Netzwerk.

‘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”

November 30, 2020

Dieser Abschnitt enthält Richtlinieneinstellungen für die Umleitung des Inhalts des Ordners **Favoriten** an einen freigegebenen Speicherort im Netzwerk.

‘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"

November 30, 2020

Dieser Abschnitt enthält Richtlinieneinstellungen für die Umleitung des Inhalts des Ordners **Links** an einen freigegebenen Speicherort im Netzwerk.

'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"

November 30, 2020

Dieser Abschnitt enthält Richtlinieneinstellungen für die Umleitung des Inhalts des Ordners **Musik** an einen freigegebenen Speicherort im Netzwerk.

‘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”

January 8, 2021

Dieser Abschnitt enthält Richtlinieneinstellungen für die Umleitung des Inhalts des Ordners **Bilder** an einen freigegebenen Speicherort im Netzwerk.

‘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"

November 30, 2020

Dieser Abschnitt enthält Richtlinieneinstellungen für die Umleitung des Inhalts des Ordners **Gespeicherte Spiele** an einen freigegebenen Speicherort im Netzwerk.

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”

November 30, 2020

Dieser Abschnitt enthält Richtlinieneinstellungen für die Umleitung des Inhalts des Ordners **Startmenü** an einen freigegebenen Speicherort im Netzwerk.

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”

November 30, 2020

Dieser Abschnitt enthält Richtlinieneinstellungen für die Umleitung des Inhalts des Ordners **Suchen** an einen freigegebenen Speicherort im Netzwerk.

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"

November 30, 2020

Dieser Abschnitt enthält Richtlinieneinstellungen für die Umleitung des Inhalts des Ordners **Videos** an einen freigegebenen Speicherort im Netzwerk.

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 30, 2020

Dieser Abschnitt 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 nützlich sein, führen jedoch evtl. zu hohem Netzwerkdatenverkehr, was für Protokolldateien nicht angebracht 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"

September 21, 2021

Dieser Abschnitt enthält Richtlinieneinstellungen zum Konfigurieren der Verarbeitung von Benutzerprofilen durch die Profilverwaltung.

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.

Automatische Migration von Anwendungsprofilen

Diese Einstellung aktiviert oder deaktiviert die automatische Migration von Anwendungsprofilen über verschiedene Betriebssysteme. Die Anwendungsprofile umfassen die Anwendungsdaten im **AppData**-Ordner und die Registrierungseinträge `HKEY_CURRENT_USER\SOFTWARE`. Die Einstellung kann nützlich sein, wenn Sie Anwendungsprofile über verschiedene Betriebssysteme migrieren möchten.

Angenommen, Sie führen ein Upgrade von Windows 10 Version 1803 auf Windows 10 Version 1809 aus. Wenn die Einstellung aktiviert ist, migriert die Profilverwaltung die Anwendungseinstellungen automatisch nach Windows 10, Version 1809, wenn sich die Benutzer erstmals anmelden.

Somit werden die Anwendungsdaten im Ordner **AppData** und die Registrierungseinträge unter HKEY_CURRENT_USER\SOFTWARE migriert.

Gibt es mehrere Anwendungsprofile, führt die Profilverwaltung die Migration in der folgenden Prioritätsreihenfolge durch:

1. Profile des gleichen Betriebssystemtyps (Einzelsitzungs-OS zu Einzelsitzungs-OS und Multisitzungs-OS zu Multisitzungs-OS).
2. Profile derselben Windows-Betriebssystemfamilie (z. B. Windows 10 nach Windows 10 oder Windows Server 2016 nach Windows Server 2016).
3. Profile einer früheren Betriebssystemversion (z. B. Windows 7 nach Windows 10 oder Windows Server 2012 nach Windows 2016).
4. Profile des ähnlichsten Betriebssystems.

Hinweis: Sie müssen den Kurznamen des Betriebssystems über die Variable "!CTX_OSNAME!"im Benutzerspeicherpfad angeben. Dadurch kann die Profilverwaltung die vorhandenen Anwendungsprofile finden.

Wenn diese Einstellung hier nicht konfiguriert ist, wird die Einstellung in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, wird sie standardmäßig deaktiviert.

Pfad zum Vorlagenprofil

Mit dieser Einstellung geben Sie den Pfad zu dem Profil an, das die Profilverwaltung als Vorlage zum Erstellen von Benutzerprofilen 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 von Benutzerprofilen.

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 von Benutzerprofilen 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 von Benutzerprofilen.

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 von Benutzerprofilen 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 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 30, 2020

Dieser Abschnitt enthält Richtlinieneinstellungen, mit denen Sie festlegen können, welche Registrierungsschlüssel bei der Verarbeitung der Profilverwaltung berücksichtigt und welche ausgeschlossen werden sollen.

Ausschlussliste

Liste der Registrierungsschlüssel in der HKCU-Struktur, die bei der Abmeldung ignoriert werden.

Beispiel: Software\Richtlinien.

Wenn diese Richtlinie deaktiviert ist, werden keine Registrierungsschlüssel ausgeschlossen. Wenn diese Richtlinie 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 Registrierungsschlüssel ausgeschlossen.

Aufnahmeliste

Liste der Registrierungsschlüssel in der HKCU-Struktur, die bei der Abmeldung verarbeitet werden.

Beispiel: Software\Adobe.

Wenn diese Richtlinie aktiviert ist, werden nur Schlüssel von dieser Liste verarbeitet. Wenn diese Richtlinie deaktiviert ist, wird die gesamte HKCU-Struktur verarbeitet. Wenn diese Richtlinie hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet. Wenn diese Richtlinie weder hier noch in der INI-Datei konfiguriert ist, wird die gesamte HKCU-Struktur verarbeitet.

Standardausschlussliste aktivieren –Profilverwaltung 5.5

Standardliste der Registrierungsschlüssel in der HKCU-Struktur, die nicht mit dem Benutzerprofil synchronisiert werden. Verwenden Sie diese Liste, um die GPO-Ausschlussdateien anzugeben, ohne sie manuell ausfüllen zu müssen.

Wenn Sie diese Richtlinie deaktivieren, werden keine Registrierungsschlüssel standardmäßig von der Profilverwaltung ausgeschlossen. Wenn Sie diese Richtlinie hier nicht konfigurieren, wird der Wert in der INI-Datei von der Profilverwaltung verwendet. Wenn Sie diese Richtlinie hier oder in der INI-Datei nicht konfigurieren, werden standardmäßig keine Registrierungsschlüssel von der Profilverwaltung ausgeschlossen.

Backup von NTUSER.DAT

Aktiviert ein Backup der letzten bekannten fehlerfreien Kopie von NTUSER.DAT und ein Rollback für den Fall einer Beschädigung.

Wenn Sie diese Richtlinie hier nicht konfigurieren, wird der Wert in der INI-Datei von der Profilverwaltung verwendet. Wenn Sie diese Richtlinie hier oder in der INI-Datei nicht konfigurieren, wird NTUSER.DAT nicht von der Profilverwaltung gesichert.

Einstellungen der Richtlinie "Gestreamte Benutzerprofile"

March 15, 2022

Dieser Abschnitt enthält Richtlinieneinstellungen zum Konfigurieren der Verarbeitung von Benutzerprofilen durch die Profilverwaltung.

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 MB 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 Gestreamte Benutzerprofile.

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 für Benutzerpersonalisierungsrichtlinien

February 6, 2020

Um die Bereitstellung von Benutzerlayern in Virtual Delivery Agents zu aktivieren, verwenden Sie Konfigurationsparameter, um Folgendes zu definieren:

- Wo im Netzwerk auf die Benutzerlayer zugegriffen werden soll.
- Wie groß neue Benutzerlayer-Datenträger werden dürfen.

Hierfür werden folgende Richtlinien in der Liste der verfügbaren Richtlinien angezeigt:

- Repositorypfad für Benutzerlayer: Geben Sie einen Pfad im Format “Servername”oder “Adresse\Ordnername”in das Feld “Wert”ein.
- Größe von Benutzerlayer in GB: Ändern Sie den Standardwert 0 auf die maximale Größe (in GB) auf die der Benutzerlayer anwachsen darf. Wenn Sie den Standardwert beibehalten, beträgt die maximale Benutzerlayergröße 10 GB.

> Hinweis:
>
> Durch das Ändern der Benutzerlayergröße in der Richtlinie wird die Größe vorhandener Layer nicht geändert.

Die Standardgröße ist 0.

Weitere Informationen finden Sie unter Benutzerpersonalisierungslayer.

Einstellungen der Richtlinie "Virtual Delivery Agent"

January 8, 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"

February 6, 2020

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

March 15, 2022

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 VDAs für Multisitzungs-OS 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 VDAs für Einzelsitzungs-OS aktivieren

Standardmäßig werden nur Anwendungsfehler auf VDAs für Multisitzungs-OS überwacht. Um VDAs für Einzelsitzungs-OS 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"

February 6, 2020

> **Wichtig:**
>
> Windows 10 Enterprise-Multisitzungs-OS unterstützt keine IP-Virtualisierung (virtuelle IP) für Remotedesktops und Citrix unterstützt weder virtuelle IPs noch virtuelles Loopback für Windows 10-Multisitzungs-OS.

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.

In der Standardeinstellung sind keine ausführbaren Dateien angegeben.

Konfigurieren von COM-Port- und LPT-Portumleitungseinstellungen in der Registrierung

March 15, 2022

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

Registrierungsschlüssel	Beschreibung	Zulässige Werte
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

February 6, 2020

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 Multisitzungs-OS-Maschinenkataloge, die manuell oder über Provisioning Services verwaltet 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 Einzelsitzungs-OS-Katalogen Configuration Manager zur Benachrichtigung der Benutzer. Verwenden Sie bei mit Provisioning Services verwalteten Einzelsitzungs-OS-Katalogen 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

March 1, 2021

Zum Verwalten einer Citrix Virtual Apps and Desktops-Site gehören verschiedene Elemente und Aufgaben.

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.

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

Citrix Virtual Apps and Desktops unterstützt reines IPv4, reines IPv6 und duale Stapelbereitstellungen, die überlappende IPv4- und IPv6-Netzwerke verwenden. 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 10, 2022

> **Hinweis:**
>
> Studio und Director unterstützen Citrix Lizenzserver VPX nicht.

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 hier 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
Citrix Virtual Apps	Premium, Advanced, Standard	CCU
Citrix Virtual Desktops	Premium, Advanced, Standard	Benutzer/Gerät und Gleichzeitig

Weitere Informationen zum Teilen von Lizenzen finden Sie unter CCU-Lizenzen.

> **Wichtig:**
>
> Lizenzserver VPX ist veraltet und erhält keine weiteren Wartungs- oder Sicherheitskorrekturen. 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.

Unterstütztes aktuelles Release (CRs) und Long Term Service Release (LTSRs)

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.

Stellen Sie sicher, dass die Lizenzierungseinstellungen für die Site (Produkttyp, Lizenzversion und Lizenzmodell) den von Ihrem konfigurierten Lizenzserver verwendeten Lizenzen entsprechen. Andernfalls müssen Sie möglicherweise die Lizenzen herunterladen oder vorhandene Lizenzen zuweisen, um den Site-Lizenzeinstellungen entsprechen.

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 und dann **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.

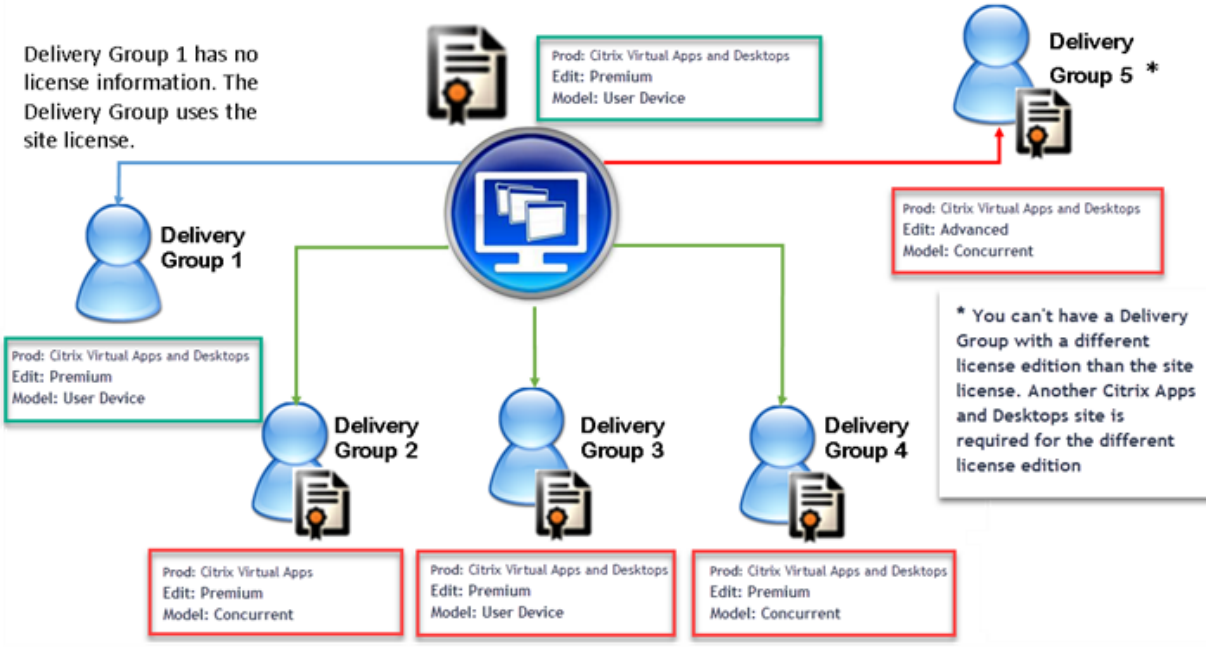
3. Wählen Sie im Aktionsbereich **Lizenzierungsadministratorengruppe bearbeiten** bzw. **Lizenzierungsadministratorengruppe löschen**.

Multityplizenzierung

March 9, 2022

Die Multityplizenzierung unterstützt den Verbrauch verschiedenartiger Lizenzen für Bereitstellungsgruppen in derselben Site von Citrix Virtual Apps and Desktops. Ein **Typ** ist eine Einzelkombination aus Produkt-ID (XDT oder MPS) und Modell (UserDevice oder Concurrent). Die Bereitstellungsgruppen müssen dieselbe Produktedition (PLT/Premium oder ENT/Advanced) verwenden, die auf Siteebene konfiguriert ist. Beachten Sie die Angaben unter Besondere Erwägungen am Ende dieses Artikels, wenn Sie die Multityplizenzierung für Ihre Citrix Virtual Apps and Desktops-Bereitstellungen konfigurieren möchten.

Wenn die Multityplizenzierung nicht konfiguriert ist, können unterschiedliche Lizenztypen nur dann verwendet werden, wenn sie für separate Sites konfiguriert sind. Für die Bereitstellungsgruppen wird die Sitelizenz verwendet. Wichtige Benachrichtigungseinschränkungen bei der Konfiguration der Multityplizenzierung finden Sie unter Besondere Erwägungen.



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.

Lizenzkompatibilitätsmatrix

In dieser Tabelle werden alte und neue Produktnamen sowie die zugehörigen Objektnamen aufgeführt. In den vier Kompatibilitätsspalten wird angegeben, welche Produkt- und Lizenzmodellkombinationen für eine Multityplizenzierung kompatibel sind. Beispielsweise sind alle Typen, bei denen Spalte **1** ein **X** enthält, kompatibel. CCU und CCS stehen für gleichzeitige Lizenzen und UD für Benutzer-/Gerätelizenzen.

Old Name	New Name	Feature	Multi-type licensing compatibility			
			1	2	3	4
Citrix XenApp Standard	Citrix XenApp Standard	MPS_STD_CCU	X			
Citrix XenApp Advanced	Citrix Virtual Apps Standard	MPS_ADV_CCU		X		
Citrix XenApp Enterprise	Citrix Virtual Apps Advanced	MPS_ENT_CCU			X	
Citrix XenApp Platinum	Citrix Virtual Apps Premium	MPS_PLT_CCU				X
CSP - Citrix XenApp Base	Citrix Virtual Apps Base	XDT_ADV_UD		X		
CSP Premium	Citrix Virtual Apps and Desktops Premium	XDT_PLT_UD				X
Citrix XenDesktop VDI Edition (XDT-U)	Citrix Virtual Desktops - Per User/Device	XDT_STD_UD	X			
Citrix XenDesktop VDI Edition (XDT-C)	Citrix Virtual Desktops - Concurrent	XDT_STD_CCS	X			
Citrix XenDesktop Enterprise Edition (XDT-C)	Citrix Virtual Apps and Desktops Advanced - Concurrent	XDT_ENT_CCS			X	
Citrix XenDesktop Enterprise Edition (XDT-U)	Citrix Virtual Apps and Desktops Advanced - Per User/Device	XDT_ENT_UD			X	
Citrix XenDesktop Platinum Edition (XDT-C)	Citrix Virtual Apps and Desktops Premium - Concurrent	XDT_PLT_CCS				X
Citrix XenDesktop Platinum Edition (XDT-U)	Citrix Virtual Apps and Desktops Premium - Per User/Device	XDT_PLT_UD				X

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	Ein Parameter (Concurrent oder UserDevice), der das Lizenzierungsmodell für die Gruppe angibt. Wenn keines angegeben wird, wird das siteweite Lizenzmodell verwendet.	Wenn die Featureumschaltung deaktiviert ist, kann keine Eigenschaft festgelegt werden.
ProductCode	Textzeichenfolge mit der Produkt-ID für die Gruppe (XDT bei Citrix Virtual Desktops oder MPS bei Citrix Virtual Apps) Wenn keiner angegeben wird, wird der siteweite Produktcode verwendet.	Wenn die Featureumschaltung deaktiviert ist, kann keine Eigenschaft festgelegt werden.

Weitere Hinweise zu **LicenseModel** und **ProductCode** finden Sie unter about_Broker_Licensing.

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/

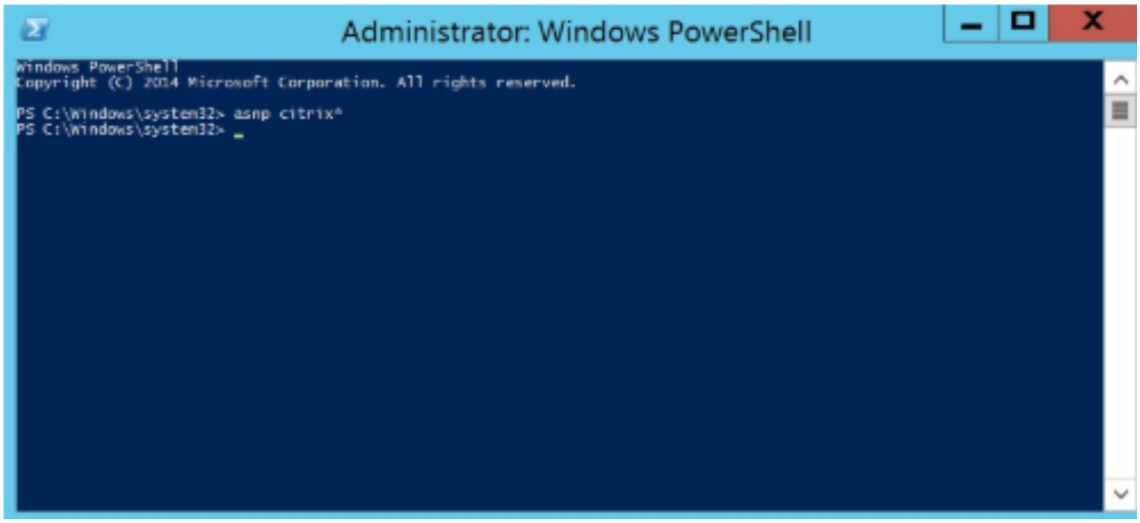
Get-BrokerDesktopGroup

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/.

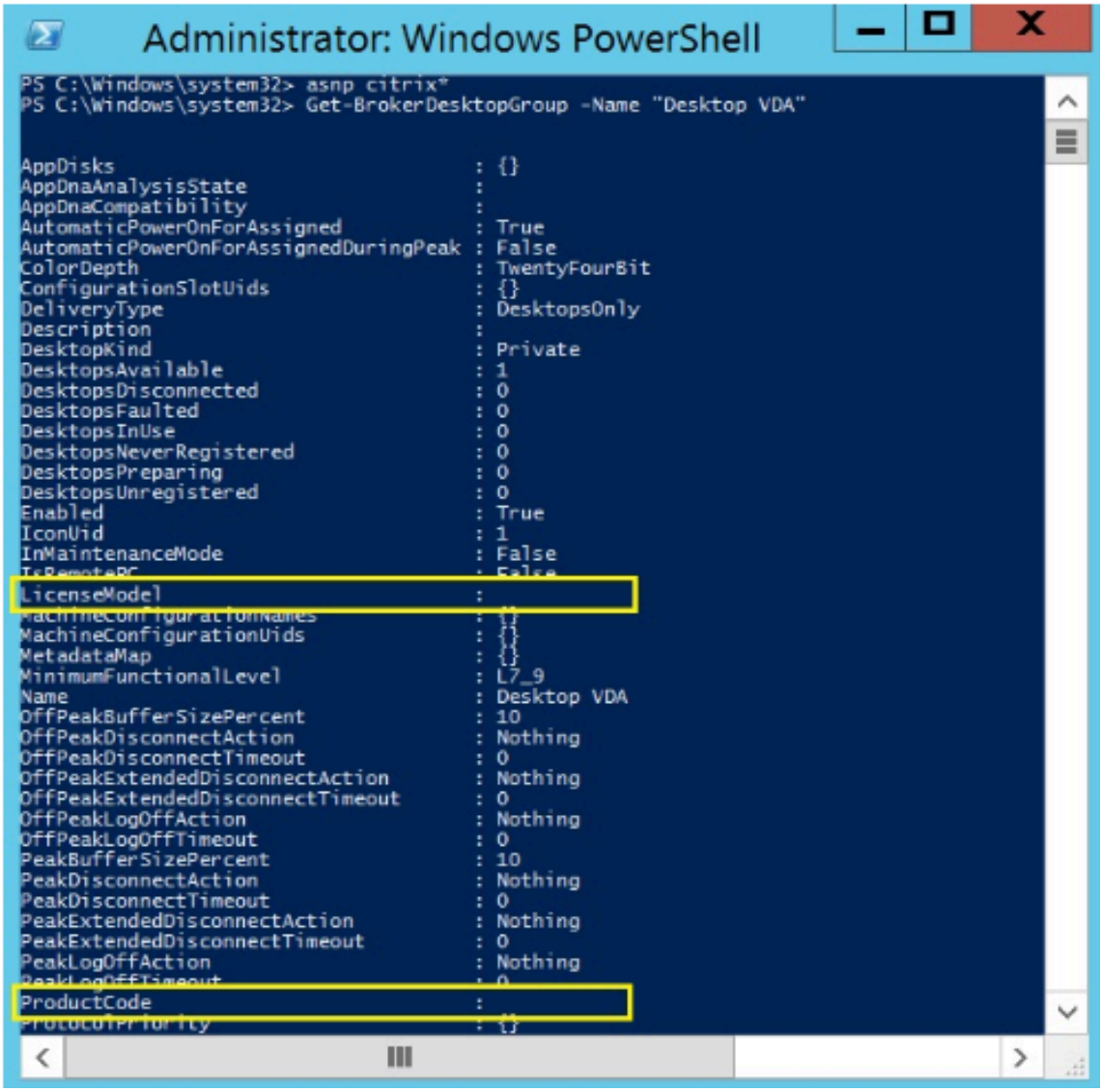
Konfigurieren verschiedener Lizenzprodukte und -modelle pro Bereitstellungsgruppe

1. Öffnen Sie PowerShell mit Administratorrechten und fügen Sie das Citrix Snap-In hinzu.

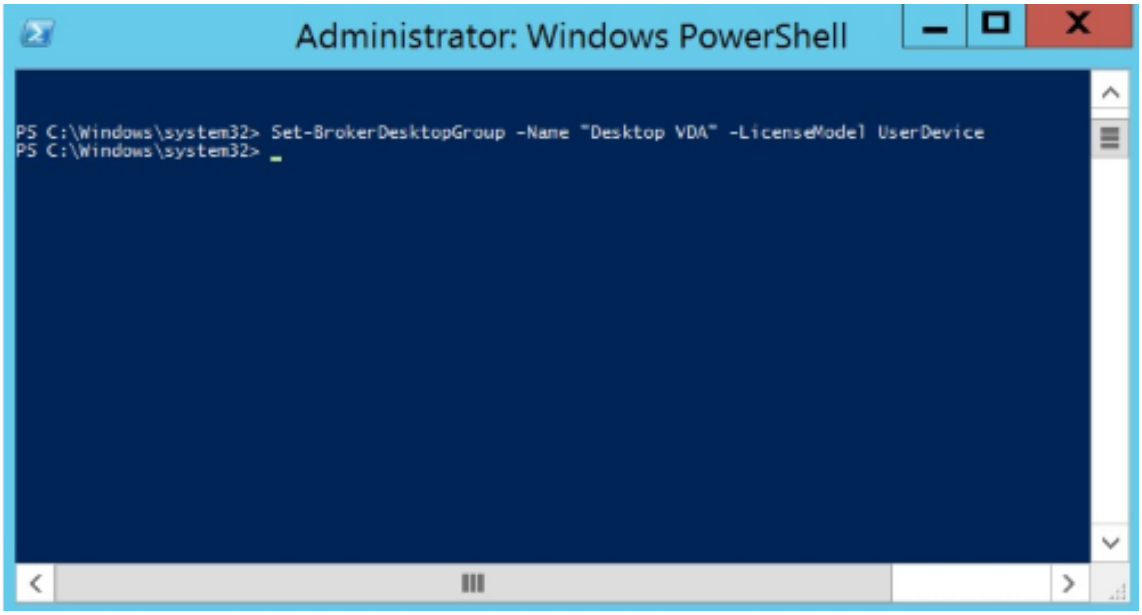


2. Führen Sie den Befehl **Get-BrokerDesktopGroup** –**Name** “**DeliveryGroupName**”, um die aktuelle Lizenzkonfiguration anzuzeigen. Suchen Sie die Parameter **LicenseModel** und **ProductCode**. Wenn Sie diese Parameter noch nicht konfiguriert haben, sind sie möglicherweise leer.

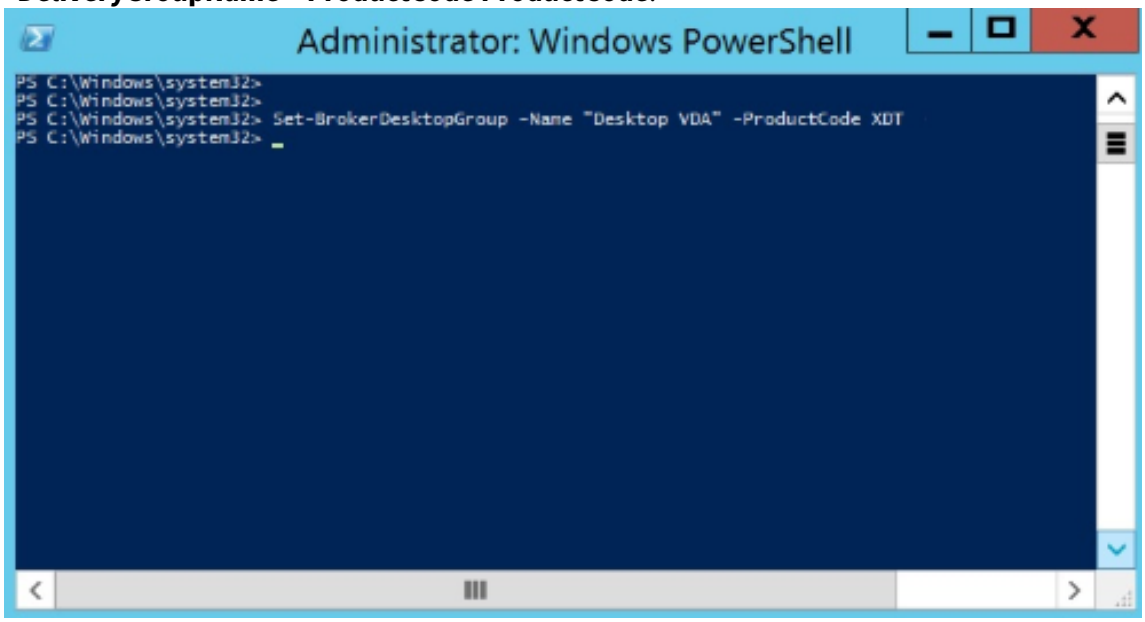
> Hinweis:
>
> Wenn für eine Bereitstellungsgruppe keine Lizenzinformationen festgelegt sind, wird standardmäßig die **Sitelizenz auf Siteebene** eingestellt.



3. Ändern Sie das Lizenzmodell durch Ausführen des Befehls **Set-BrokerDesktopGroup –Name “DeliveryGroupName”–LicenseModel LicenseModel**.

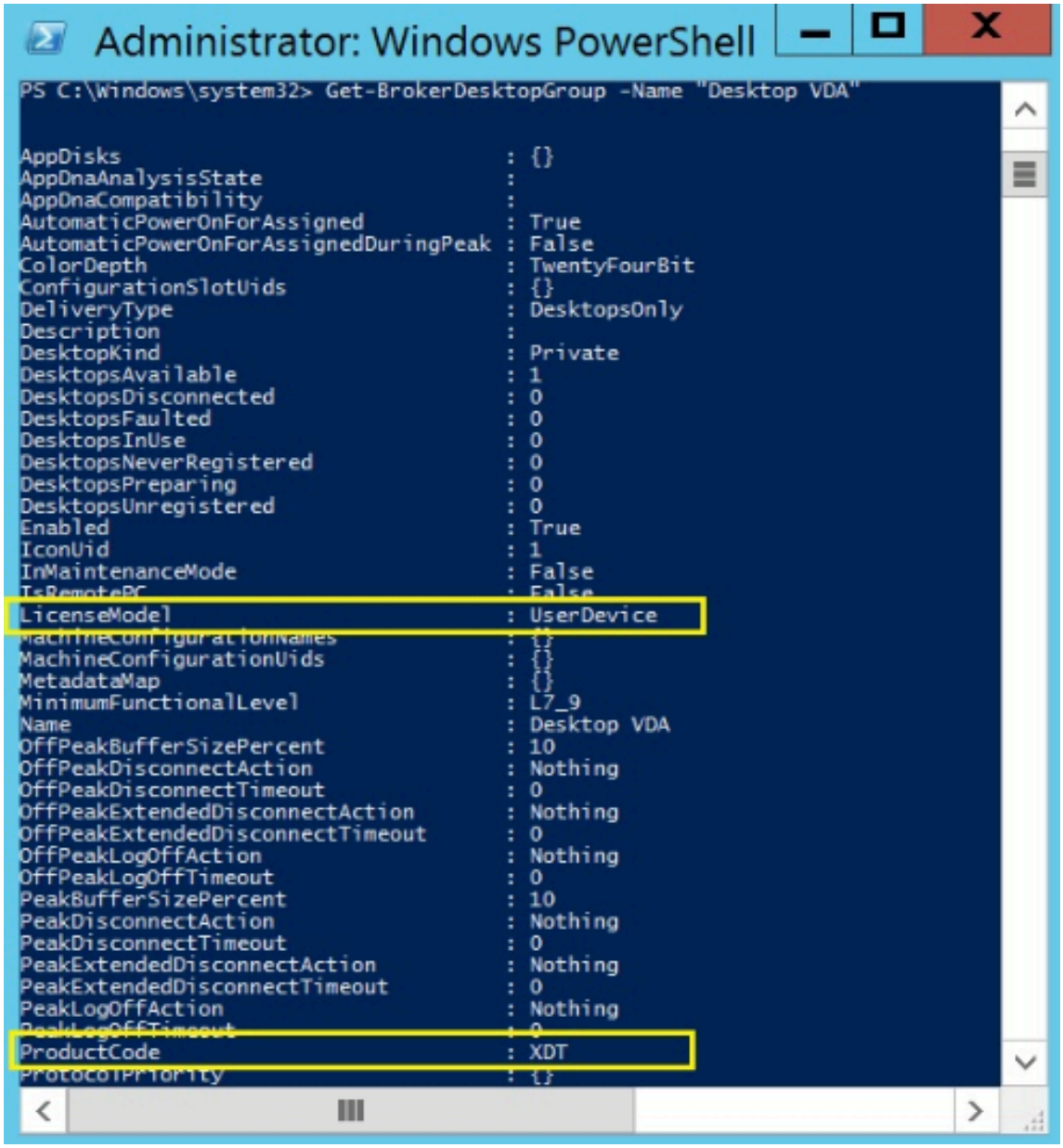


4. Ändern Sie das Lizenzprodukt durch Ausführen des Befehls **Set-BrokerDesktopGroup** –**Name “DeliveryGroupName”**–**ProductCode ProductCode**.



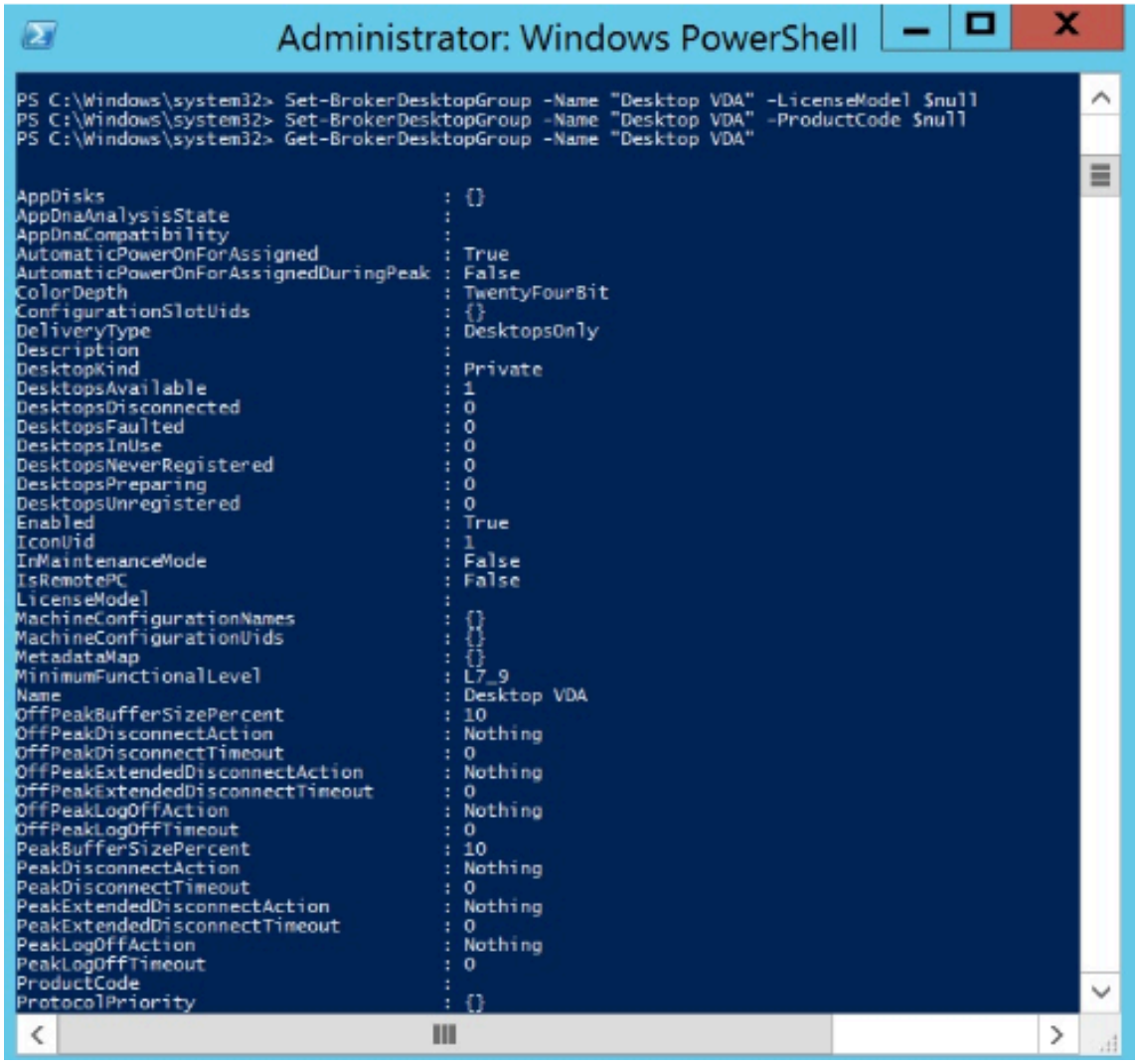
5. Geben Sie den Befehl **Get-BrokerDesktopGroup** –**Name “DeliveryGroupName”** ein, um die Änderungen zu überprüfen.

> Hinweis:
>
> Sie können Editionen in derselben Site nicht mischen. Zum Beispiel Premium- und Advanced-Lizenzen. Wenn Sie Lizenzen mit unterschiedlichen Editionen haben, sind mehrere Sites erforderlich.



6. Entfernen Sie die Lizenzkonfiguration durch Ausführen der o. a. **Set-BrokerDesktopGroup**-Befehle und Festlegen des Werts auf **$null**.

> 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 “Delivery group for Citrix Virtual Apps Premium Concurrent”-ProductCode MPS -LicenseModel Concurrent

2. Nun werden die zweite Bereitstellungsgruppe für XenDesktop sowie “Concurrent”festgelegt.

Set-BrokerDesktopGroup -Name “Delivery group for Citrix Virtual Desktops Premium Concurrent”-ProductCode XDT -LicenseModel Concurrent

3. Anschließend wird die dritte Bereitstellungsgruppe für XenDesktop und “UserDevice”erstellt und eingerichtet.

   New-BrokerDesktopGroup -Name “Delivery group for Citrix Virtual Desktops Premium UserDevice”-PublishedName “MyDesktop”-DesktopKind Private -ProductCode XDT -LicenseModel UserDevice

Besondere Erwägungen

Die Multityplizenzierung funktioniert anders als die normale Lizenzierung von Citrix Virtual Apps and Desktops.

Es gibt keine Warnungen und Benachrichtigungen von Director oder Studio für Bereitstellungsgruppen, deren Konfiguration einen Typ verwendet, der sich von der Sitekonfiguration unterscheidet:

- Keine Informationen über ein mögliches Erreichen des Lizenzlimits und des Auslösens bzw. Ablaufs des Zusatzkulanzzeitraums
- Keine Benachrichtigung bei Problemen mit einer bestimmten Gruppe

Bereitstellungsgruppen, die für Multityplizenzen konfiguriert sind, verbrauchen NUR diesen Lizenztyp und greifen nicht auf die Sitekonfiguration zurück, wenn die Lizenzen dieses Typs vollständig verbraucht sind.

Trotz der Ähnlichkeit im Namen gehören die Citrix Virtual Apps Standard- und Citrix Virtual Desktops Standard-Lizenzen nicht zu derselben Edition. Die Multityplizenzierung funktioniert nicht mit Citrix Virtual Apps Standard- und Citrix Virtual Desktop Standard-Lizenzen.

Häufig gestellte Fragen zur Lizenzierung

November 2, 2022

> **Hinweis:**
>
> - Ressourcen zur Geschäftskontinuität angesichts der aktuellen COVID-19-Pandemie finden Sie unter CTX27055.
> - Allgemeine Hinweise zur Aufrechterhaltung der Geschäftskontinuität finden Sie unter Business continuity –on demand.
> - Weitere Informationen zur aktuellen Version von Citrix Lizenzserver finden Sie unter Lizen-

> zierung.

Wie wird Citrix Virtual Apps and Desktops lizenziert?

Für Citrix Virtual Apps and Desktops werden ein Benutzer-/Gerätelizenzmodell und ein Gleichzeitig-Modell angeboten.

Benutzer-/Gerätelizenzmodell:

Das flexible Benutzer-/Gerätelizenzmodell ist ausgerichtet auf:

- Unternehmensweite Desktop-Nutzung
- Zugrunde liegende Lizenzierung für die Microsoft-Desktopvirtualisierung
- Gleichzeitige Lizenzierung für Kunden, bei denen Benutzer nur gelegentlich Zugriff auf virtuelle Desktops und Apps benötigen.

Mit der Benutzer-/Gerätelizenzierung haben Benutzer über beliebig viele Geräte Zugriff auf ihre virtuellen Desktops und Apps. Gerätelizenzen ermöglichen beliebig vielen Benutzern über ein einzelnes Gerät Zugriff auf ihre virtuellen Desktops und Apps. Dieser Ansatz bietet maximale Flexibilität und verbessert die Ausrichtung auf die Lizenzierung für die Microsoft-Desktopvirtualisierung.

> **Wichtig:**
>
> Sie können einem Benutzer oder Gerät keine Lizenzen manuell zuweisen. Der Lizenzserver oder der Clouddienst weist die Lizenzen zu. Bei der Benutzer-/Gerätelizenzierung kann eine zugewiesene Lizenz erst nach 90 Tagen Inaktivität einem anderen Benutzer zugewiesen werden.

Gleichzeitig-Modell:

Bei diesem Modell ist eine Verbindung zu beliebig vielen virtuellen Apps und Desktops für jeden Benutzer und jedes Gerät möglich. Eine Lizenz wird nur während einer aktiven Sitzung verbraucht. Wenn die Sitzung getrennt oder beendet wird, wird die Lizenz wieder in den Pool eingecheckt.

Weitere Informationen zum Benutzer-/Gerätelizenzmodell finden Sie unter Benutzer-/Gerätelizenzen und zum Gleichzeitig-Modell unter CCU-Lizenzen.

Kann Citrix Virtual Apps and Desktops vor dem Kauf von Lizenzen getestet werden?

Ja. Sie können Citrix Virtual Apps and Desktops herunterladen und im Testmodus ausführen. Im Testmodus können Sie Citrix Virtual Apps and Desktops 30 Tage lang im eigenen Rechenzentrum für 10 Verbindungen ohne Lizenz verwenden.

Citrix Virtual Apps and Desktops Service für Citrix Cloud steht nach entsprechender Genehmigung als Testservice zur Verfügung. Weitere Informationen erhalten Sie von Ihrem Citrix Vertreter.

Wie definiert Citrix Gleichzeitigkeit bei Citrix Virtual Apps and Desktops?

Bei dem Gleichzeitig-Modell für Citrix Virtual Apps and Desktops ist eine Verbindung zu beliebig vielen virtuellen Apps und Desktops für jeden Benutzer und jedes Gerät möglich. Eine Lizenz wird nur während einer aktiven Sitzung verbraucht. Wenn die Sitzung getrennt oder beendet wird, wird die Lizenz wieder in den Pool zur Wiederverwendung eingecheckt.

Wie weist Citrix Benutzern Lizenzen beim Benutzer-/Gerätelizenzmodell zu?

Beim Benutzer-/Gerätelizenzmodell weist der Lizenzserver eine Lizenz einer eindeutigen Benutzer-ID zu. Diese ermöglicht dem jeweiligen Benutzer beliebig viele Verbindungen über beliebig viele Geräte. Wenn ein Benutzer eine Verbindung zu einem Desktop oder Gerät herstellt, benötigt er für den Zugriff auf einen virtuellen Desktop oder eine virtuelle App eine Lizenz. Der Lizenzserver oder der Clouddienst weist die Lizenz zu. Sie können diese Lizenzen nicht manuell zuweisen. Die Lizenz wird dem Benutzer und nicht dem freigegebenen Gerät zugewiesen. Eine zugewiesene Lizenz kann erst nach 90 Tagen Inaktivität einem anderen Benutzer zugewiesen werden.

Wie definiert Citrix ein lizenziertes Gerät beim Benutzer-/Gerätelizenzmodell?

Ein lizenziertes Gerät erfordert eine eindeutige Endpunktgeräte-ID. Beim Benutzer-/Gerätelizenzmodell ist ein Gerät jeder Ausrüstungsgegenstand, den Sie für den Zugriff auf Instanzen von Citrix Virtual Apps and Desktops genehmigt haben. Bei gemeinsam genutzten Geräten kann eine Benutzer-/Gerätelizenz für Citrix Virtual Apps and Desktops mehrere Benutzer unterstützen, die das Gerät nutzen. Beispiele für gemeinsam genutzte Geräte sind Arbeitsstationen in Schulungsräumen oder einem Krankenhaus.

Kann ich meine Gleichzeitig-Lizenzen für Citrix Virtual Desktops Standard Edition in Benutzer-/Gerätelizenzen umwandeln?

Sie können Gleichzeitig-Lizenzen für Citrix Virtual Desktops Standard Edition nicht in Benutzer-/Gerätelizenzen umwandeln. Umgekehrt können auch Benutzer-/Gerätelizenzen für Citrix Virtual Desktops Standard Edition nicht in Gleichzeitig-Lizenzen umwandeln.

Wenn Sie Gleichzeitig-Lizenzen für Citrix Virtual Desktops Standard Edition haben und das Benutzer-/Gerätelizenzmodell verwenden möchten, führen Sie ein Upgrade auf Citrix Virtual Apps and Desktops Advanced oder Premium Edition durch.

Von	Auf Standard, Gleichzeitig	Auf Standard, Benutzer/Gerät	Auf Advanced, Benutzer/Gerät	Auf Premium, Benutzer/Gerät
Gleichzeitig-Lizenzen für Citrix Virtual Desktops Standard Edition	Nicht zutreffend	Umwandlung Gleichzeitig in Benutzer/Gerät NICHT zulässig	Sie können das Lizenzmodell nicht wechseln, aber Sie können ein Upgrade auf Citrix Virtual Apps and Desktops Advanced oder Premium Edition durchführen.	Sie können das Lizenzmodell nicht wechseln, aber Sie können ein Upgrade auf Citrix Virtual Apps and Desktops Advanced oder Premium Edition durchführen.
Benutzer-/Gerätelizenzen für Citrix Virtual Desktops Standard Edition	Umwandlung Benutzer/Gerät in Gleichzeitig NICHT zulässig	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend

Worin besteht der Unterschied zwischen der Gleichzeitig-Lizenzierung und der Benutzer-/Gerätelizenzierung?

Die Gleichzeitig-Lizenzierung basiert auf gleichzeitigen Geräteverbindungen. Eine Gleichzeitig-Lizenz wird nur verwendet, wenn ein Gerät eine aktive Verbindung hergestellt hat. Sobald die Verbindung getrennt wird, kehrt die Gleichzeitig-Lizenz zur sofortigen Wiederverwendung in den Lizenzpool zurück. Citrix empfiehlt dieses Lizenzmodell für die gelegentliche Nutzung. Benutzer-/Gerätelizenzen werden für einen bestimmten Zeitraum geleast und stehen erst nach Lease-Ablauf für andere Benutzer zur Verfügung.

Können bei dem Benutzer-/Gerät-Modell Lizenzen sowohl Benutzern als auch Geräten im selben Unternehmen zugewiesen werden?

Ja. Beide Typen können im selben Unternehmen vorhanden sein. Der Lizenzserver weist Benutzern oder Geräten entsprechend der Nutzung Lizenzen optimal zu. Sie können diese Lizenzen nicht manuell zuweisen.

Wie bestimme ich, wie viele Benutzer oder Geräte lizenziert werden sollen?

Bewerten Sie die Anforderungen des Anwendungsfalls, um die geeignete Anzahl von Lizenzen zu ermitteln. Beim Benutzer-/Gerätelizenzmodell haben Benutzer über beliebig viele Geräte unbegrenzt Zugriff auf unbegrenzte virtuelle Desktops und Apps. Bei der Gleichzeitig-Lizenzierung besteht unbegrenzter Zugriff auf unbegrenzte virtuelle Desktops und Apps über ein einzelnes Gerät, das beliebig viele Benutzern verwenden können. Verwenden Sie folgende Formel:

```
(Number of total users) – (number of users that only access
   exclusively
 with shared devices) + (number shared devices) = total number
 of licenses to buy.

For example, there are 1000 total users at the hospital. If 700 of them
    access only
Citrix Virtual Desktops from 300 shared devices in the hospital, the
   number of
licenses to purchase is 1000 – 700 + 300 = 600 licenses.
<!--NeedCopy-->
```

Wie viele Geräte kann ein lizenzierter Benutzer beim Benutzer-/Gerätelizenzmodell zur Herstellung einer Verbindung mit meiner Umgebung verwenden?

Jeder lizenzierte Benutzer kann beliebig viele verbundene Geräte oder Offlinegeräte nutzen.

Wie viele Benutzer haben beim Benutzer-/Gerätelizenzmodell maximal Zugang zu einem lizenzierten Gerät?

Jedes lizenzierte Gerät kann von beliebig vielen Benutzern innerhalb einer Organisation verwendet werden.

Wie viele virtuelle Desktops oder Remote Browser Isolation (RBI)-Webanwendungen kann ein lizenzierter Benutzer beim Benutzer-/Gerätelizenzmodell zu einem gegebenen Zeitpunkt verwenden?

Ein lizenzierter Benutzer kann eine Verbindung zu beliebig vielen virtuellen Desktops oder Webanwendungen herstellen.

Maximal wie viele virtuelle Anwendungen kann ein lizenzierter Benutzer zu einem gegebenen Zeitpunkt verwenden?

Ein lizenzierter Benutzer kann eine Verbindung zu beliebig vielen virtuellen Anwendungen herstellen.

Was passiert, wenn ein lizenzierter Benutzer meine Organisation verlässt?

Wenn ein lizenzierter Benutzer Ihre Organisation verlässt, können Sie dessen Lizenz freigeben, ohne Citrix zu benachrichtigen. Verwenden Sie das Hilfsprogramm `udadmin`, um Lizenzen freizugeben. Wenn Sie eine Lizenz nicht freigeben, wird sie vom Lizenzserver automatisch nach 90 Tagen Inaktivität freigegeben. Diese Informationen unterliegen den in der EULA festgelegten Bedingungen.

Was passiert, wenn ein lizenzierter Benutzer über einen längeren Zeitraum abwesend ist?

Wenn ein lizenzierter Benutzer über einen längeren Zeitraum abwesend ist, können Sie dessen Lizenz freigeben, ohne Citrix zu benachrichtigen, damit sie für eine Neuzuweisung verfügbar ist. Verwenden Sie das Hilfsprogramm `udadmin`, um Lizenzen freizugeben.

Was passiert, wenn wir ein lizenziertes Gerät ersetzen?

Wenn Sie ein lizenziertes Gerät ersetzen, können Sie die Lizenz freigeben, ohne Citrix zu benachrichtigen, damit sie für die Neuzuweisung verfügbar ist. Verwenden Sie das Hilfsprogramm `udadmin`, um Lizenzen freizugeben.

Was passiert, wenn ein lizenziertes Gerät über einen längeren Zeitraum außer Betrieb ist?

Wenn ein lizenziertes Gerät über einen längeren Zeitraum außer Betrieb ist, können Sie dessen Lizenz freigeben, ohne Citrix zu benachrichtigen, damit sie für eine Neuzuweisung verfügbar ist. Verwenden Sie das Hilfsprogramm `udadmin`, um Lizenzen freizugeben. Wenn Sie eine Lizenz nicht freigeben, wird sie vom Lizenzserver automatisch nach 90 Tagen Inaktivität freigegeben. Diese Informationen unterliegen den in der EULA festgelegten Bedingungen.

Kann ich Benutzerlizenzen in Gerätelizenzen umwandeln und umgekehrt, nachdem ich sie einem Gerät oder Benutzer zugewiesen habe?

Ja. Diese Umwandlung erfolgt automatisch. Der Lizenzserver weist Benutzern oder Geräten entsprechend der Nutzungsmuster Lizenzen zu. Wenn sich Nutzungsmuster ändern, ändert der Lizenzserver ggf. die Zuweisung entsprechend. Der Lizenzserver weist Lizenzen immer auf die für den Kunden wirtschaftlichste Art und Weise zu. Außerdem überwacht der Lizenzserver die Lizenzen, um **nicht verwendete** Lizenzen nach dem 90-tägigen Zuweisungszeitraum zu identifizieren. Sie können Lizenzen, die nach dem 90-tägigen Zuweisungszeitraum als nicht verwendet identifiziert wurden, anderen Benutzern oder Geräten zuweisen.

Wie viele virtuelle Desktops kann ein lizenzierter Citrix Virtual Apps and Desktops-Benutzer beim Gleichzeitig-Modell zu einem gegebenen Zeitpunkt verwenden?

Ein Endpunkt kann von vielen Benutzern verwendet werden und ermöglicht unbegrenzte Verbindungen.

Kann ich Citrix Virtual Apps and Desktops-Lizenzen erwerben, um die Anzahl der lizenzierten Benutzer/Geräte in meiner Citrix Virtual Apps and Desktops-Umgebung zu erhöhen?

Ja. Sie können Citrix Virtual Apps and Desktops-Lizenzen erwerben, um die Anzahl der lizenzierten Benutzer/Geräte in Ihrer Citrix Virtual Apps and Desktops-Umgebung zu erhöhen.

Kann ich Gleichzeitig-Lizenzen aus einer früheren Citrix Virtual Apps and Desktops-Version und neue Benutzer-/Gerät- oder Gleichzeitig-Lizenzen auf demselben Lizenzserver bereitstellen?

Ja. Sie können denselben Lizenzserver weiterverwenden, um Bereitstellungen mit Benutzer-/Gerät- oder Gleichzeitig-Lizenzen zu unterstützen.

Kann ich Gleichzeitig-Lizenzen und Benutzer-/Gerät- oder Gleichzeitig-Lizenzen auf demselben Lizenzserver bereitstellen?

Ja. Sie können denselben Lizenzserver weiterverwenden, um Bereitstellungen mit Gleichzeitig-Lizenzen und Benutzer-/Gerät- oder Gleichzeitig-Lizenzen zu unterstützen.

Kann ich mehrere Editionen von Citrix Virtual Apps and Desktops-Lizenzen auf einem gemeinsamen Lizenzserver bereitstellen?

Ja. Der Lizenzserver verwaltet Lizenzen für mehrere Citrix Virtual Apps and Desktops-Editionen gleichzeitig. Wir empfehlen, dass Sie die aktuelle Version des Lizenzservers installieren. Wenn Sie nicht sicher sind, ob Ihre Version des Lizenzservers aktuell ist, vergleichen Sie dessen Version mit der Nummer auf der Citrix Downloadseite.

Kann eine einzelne Site sowohl Citrix Virtual Apps- als auch Citrix Virtual Apps and Desktops-Lizenzen verwenden?

Je nach Version kann eine Citrix Virtual Apps- oder Citrix Virtual Apps and Desktops-Site beide Lizenzierungsmodelle, Benutzer/Gerät und Gleichzeitig, unterstützen. Eine einzelne Citrix Virtual Apps- oder eine Citrix Virtual Apps and Desktops-Site kann nur eine Edition unterstützen. Weitere Informationen finden Sie unter Multityplizenzierung.

Die Mindestversionen, die mehrere Lizenzierungsmodelle zugleich unterstützen, sind XenApp und XenDesktop 7.15 Long Term Service Release (LTSR) und Citrix Virtual Apps and Desktops 7 1808.

Kann ich gleichzeitige Citrix Virtual Apps-Lizenzen als Produktmodell wählen, wenn auf dem Lizenzserver Benutzer-/Gerät- oder gleichzeitige Lizenzen für Citrix Virtual Apps and Desktops installiert sind?

Wenn Sie Citrix Virtual Apps als Feature von Citrix Virtual Apps and Desktops Advanced oder Premium Edition verwenden, entspricht das Lizenzmodell für Citrix Virtual Apps dem Modell der Advanced bzw. Premium Edition von Citrix Virtual Apps and Desktops. Wenn Sie Citrix Virtual Apps and Desktops erworben haben, konfigurieren Sie die Lizenzierung als Citrix Virtual Apps and Desktops, selbst wenn Sie nur Citrix Virtual Apps verwenden möchten. Wählen Sie Citrix Virtual Apps nur dann als Produktmodell, wenn auf dem Lizenzserver gleichzeitige eigenständige Lizenzen für Citrix Virtual Apps installiert sind.

Überziehungslizenzen

In diesem Abschnitt werden Fragen zu Überziehungslizenzen beantwortet.

Wie erhalte ich Überziehungslizenzen? Die Lizenzüberziehung gilt für alle Benutzer-/Gerätelizenzen. Wenn Sie Benutzer-/Gerätelizenzen erwerben, können Sie Ihre Lizenzanzahl um 10 % überziehen. Diese Überziehungslizenzen sind verfügbar, nachdem Sie alle erworbenen Lizenzen und Evaluationen zugeteilt haben. Die Überziehungsfunktion wird als Hilfe angeboten und sind nicht als

Lizenzberechtigung zu verstehen. Wenn Sie Überziehungslizenzen häufig in Anspruch nehmen, empfehlen wir den Erwerb zusätzlicher Lizenzen.

Wie kann ich eine Lizenzüberziehung identifizieren? Sie können Nutzungsinformationen, einschließlich der Anzahl der Überziehungslizenzen, in Citrix Licensing Manager anzeigen. Auch Studio enthält Informationen zur Nutzung von Überziehungslizenzen.

Was passiert, wenn eine Überziehungslizenz verwendet wird?
Aus den installierten Lizenzen wird eine Lizenz zugewiesen, um den Zugriff auf Ihre Citrix Virtual Apps and Desktops-Umgebung zu ermöglichen. Diese Überziehungslizenz bietet denselben Zugriff und dieselbe Funktionalität wie die anderen Lizenzen.

Kann ich eine Benachrichtigung erhalten, wenn meine Überziehungslizenzen verwendet werden?
Derzeit gibt es keine Warnungen, wenn Überziehungslizenzen verwendet werden.

Wie lange kann eine Überziehungslizenz verwendet werden?
Sie müssen Überziehungslizenzen innerhalb von 30 Tagen nach der ersten Verwendung erwerben.

Welche Produktkomponenten gehören zu den einzelnen Citrix Virtual Apps- und Citrix Virtual Apps and Desktops-Edition?

Eine vollständige Funktionsmatrix nach Edition finden Sie unter Citrix Virtual Apps and Desktops.

Wie lizenziere ich Citrix Virtual Desktops-Umgebungen gemäß der Citrix Virtual Apps and Desktops-EULA?

Um Citrix Virtual Apps and Desktops unter dem Benutzer-/Gerätelizenz- oder dem Gleichzeitig-Lizenzmodell gemäß den Richtlinien der Citrix Virtual Apps and Desktops-EULA bereitzustellen, wenden Sie die Lizenzdateien auf Ihren Lizenzserver an. Der Lizenzserver kontrolliert und überwacht dann die Lizenzcompliance. Wir empfehlen die Konfiguration basierend auf dem erworbenen Produkt. Wenn Sie beispielsweise Citrix Virtual Apps and Desktops Premium erwerben aber nur Citrix Virtual Apps verwenden möchten, konfigurieren Sie das Produkt für Citrix Virtual Apps and Desktops, um die Compliancerichtlinien zu erfüllen. Weitere Informationen finden Sie im Product License Compliance Center.

Wie lizenziere ich Citrix Virtual Apps-Umgebungen gemäß der Citrix Virtual Apps-EULA?

Um Citrix Virtual Apps unter dem Gleichzeitig-Lizenzmodell gemäß den Richtlinien der Citrix Virtual Apps-EULA bereitzustellen, wenden Sie die Lizenzdateien auf Ihren Lizenzserver an. Der Lizenzserver kontrolliert und überwacht dann die Lizenzcompliance.

Enthalten die Advanced- und die Premium-Edition von Citrix Virtual Apps and Desktops Gleichzeitig-Lizenzen für Citrix Virtual Apps?

Die Benutzer/Gerät-Lizenzen der Advanced- und der Premium-Edition von Citrix Virtual Apps and Desktops umfassen Gleichzeitig-Lizenzen für Citrix Virtual Apps nur zum Zweck der Kompatibilität. Diese Gleichzeitig-Lizenzen sind nur für frühere Produktversionen gedacht, die nicht mit Benutzer-/Gerätelizenzen kompatibel sind. Die Verwendung der Gleichzeitig-Kompatibilitätslizenzen, die in den Benutzer-/Gerätelizenzen enthalten sind, ist nur für die XenApp-Versionen vor 6.5 und XenDesktop-Versionen vor 5.0 Service Pack 1 zulässig.

Wie erhalte ich meine Lizenzdatei?

Wir senden den Lizenzzugangscode per E-Mail. Es gibt drei Möglichkeiten, Lizenzdateien mit dem Lizenzzugangscode zu generieren:

- Über die Toolbox “Manage Licenses”auf der Seite “My Account”auf citrix.com
- Citrix Studio zur Zuweisung Ihres Erwerbs, die Lizenzdatei wird automatisch auf Ihrem Citrix Lizenzserver installiert.
- Citrix Licensing Manager im Citrix Lizenzserver zur Zuweisung Ihres Erwerbs und Installation Ihrer Lizenzdatei

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

Welche TCP-Ports werden von der Citrix Lizenzierung verwendet?

- Die Portnummer für den Lizenzserver ist 27000.
- Die Portnummer für den Vendor Daemon ist 7279.
- Die Webportnummer für die Verwaltungskonsole ist 8082.
- Die Portnummer der Web Services for Licensing ist 8083.

Was ist der Citrix Lizenzserver?

Der Citrix Lizenzserver ist ein System, das die Freigabe von Lizenzen im Netzwerk ermöglicht. Weitere Informationen finden Sie unter Lizenzierungsübersicht.

Kann ich den Citrix Lizenzserver virtualisieren oder clustern?

Ja. Sie können den Citrix Lizenzserver virtualisieren und clustern. Weitere Informationen finden Sie unter Lizenzservercluster.

Welche Vorteile bringt mir die Virtualisierung des Citrix Lizenzservers?

Die Virtualisierung des Citrix Lizenzservers bietet Redundanz. Diese Lösung ermöglicht den Wechsel zwischen mehreren physischen Servern ohne Ausfallzeit.

Gelten bei der Virtualisierung des Citrix Lizenzservers Einschränkungen?

Nein.

Verwaltet der Citrix Lizenzserver alle Lizenzen für meine Citrix Virtual Apps and Desktop-Bereitstellung?

Der Citrix Lizenzserver verwaltet alle Lizenzen, die Sie für Citrix Virtual Apps and Desktops erhalten, mit Ausnahme von Lizenzen der Premium Edition, die mit Citrix Gateway verwendet werden. Lizenzserver, die in die Netzwerk-Appliances integriert sind, wie es für diese sicherheitsorientierten Netzwerkgeräte erforderlich ist, verwalten diese Lizenzen.

Was ist der Citrix Licensing Manager?

Der Citrix Licensing Manager ermöglicht das Herunterladen und Zuteilen von Lizenzdateien vom Lizenzserver, auf dem Sie den Citrix Licensing Manager installiert haben. Der Citrix Licensing Manager ist die empfohlene Lizenzserver-Verwaltungsmethode, die Folgendes ermöglicht:

- Shortcode-Registrierung des Lizenzservers bei Citrix Cloud und einfaches Entfernen der Registrierung.
- Konfigurieren von Benutzer- und Gruppenkonten.
- Verwenden des Dashboards zum Anzeigen installierter, genutzter, abgelaufener und verfügbarer Lizenzen sowie der Daten für Customer Success Services.
- Exportieren von Lizenznutzungsdaten für die Berichterstellung
- Konfigurieren der Aufbewahrungsdauer von Nutzungsverlaufsdaten. Daten werden standardmäßig 180 Tage lang beibehalten.
- Vereinfachte Installation von Lizenzdateien auf dem Lizenzserver mit einem Lizenzzugangscode oder einer heruntergeladenen Datei.
- Aktivieren und Deaktivieren des zusätzlichen Kulanzzeitraums.
- Konfigurieren des Programms zur Verbesserung der Benutzerfreundlichkeit (CEIP) und von Call Home.
- Automatische oder manuelle Suche nach Customer Success Services-Verlängerungslizenzen und Benachrichtigung oder Installation der gefundenen Lizenzen.
- Benachrichtigung über den Zustand des Lizenzservers - fehlende Startlizenz, zeitliche Probleme, Uploaderfehler.

- Ändern dieser Ports:
  - Lizenzserverport (Standard 27000)
  - Vendor Daemon (Standard 7279)
  - Port für Web Services for Licensing (Standard 8083)

Weitere Informationen finden Sie unter Citrix Licensing Manager.

Was ist die Citrix License Administration Console?

Die License Administration Console ist eine Schnittstelle, mit der Sie die Lizenzen für die Citrix Infrastruktur verwalten können. Über sie können Sie außerdem die Einstellungen für den Lizenzserver konfigurieren und die aktuelle Lizenzverwendung anzeigen.

Sie können die Lizenzierung in Studio verwalten und nachverfolgen, sofern der Lizenzserver in derselben Domäne wie Studio oder in einer vertrauenswürdigen Domäne ist.

Weitere Informationen finden Sie unter License Administration Console.

Was ist der Lizenzzuweisungszeitraum?

Der Lizenzzuweisungszeitraum ist die Zeitdauer, für die einem Benutzer oder Gerät eine Lizenz für Citrix Virtual Apps and Desktops zugewiesen wird. Der Standardzuweisungszeitraum beträgt 90 Tage.

Wie gebe ich eine autorisierte Benutzer-/Gerätelizenz frei?

Um die Zuweisung einer autorisierten Benutzer-/Gerätelizenz freizugeben, verwenden Sie das Hilfsprogramm `udadmin` gemäß den EULA-Bedingungen. Der Lizenzserver weist die Lizenz dann dem nächsten geeigneten Benutzer oder Gerät zu.

Woher weiß ich, wie viele Lizenzen meine Organisation erworben hat?

Alle erworbenen Lizenzen sind rund um die Uhr über die sichere Toolbox **Manage Licenses** der Seite **My Account** auf https://www.citrix.com zugänglich.

Woher weiß ich, wie viele Lizenzen zu einem gegebenen Zeitpunkt verwendet werden?

Der Citrix Licensing Manager, die License Administration Console und Studio enthalten Details zur Echtzeit-Lizenzverwendung.

Was passiert, wenn ich die Zahl der erworbenen Benutzer-/Gerätelizenzen überschreite?

Benutzer-/Gerätelizenzen sind bei ihrer Generierung mit einer Überziehungslizenz von 10 % ausgestattet. Die Überziehungslizenz ist in der Anzahl der installierten Lizenzen enthalten. Übersteigt die Nutzung die Anzahl installierter Lizenzen einschließlich Überziehungslizenzen, wird der Zugriff für weitere Nutzer verweigert. Sie müssen eine neue Lizenz erwerben und bereitstellen, um den Zugriff für weitere Benutzer zu ermöglichen.

Wenn alle Lizenzen (einschließlich der Überziehungslizenzen) verwendet werden, ermöglicht der Zusatzkulanzzeitraum unbegrenzte Verbindungen zu einem Produkt. Der Zusatzkulanzzeitraum gibt Ihnen Zeit, den Grund für das Überschreiten der maximalen Lizenzanzahl festzustellen und weitere Lizenzen zu erwerben, ohne dass Störungen für Benutzer auftreten. Der Zeitraum endet nach 15 Tagen oder mit der Installation weiterer Volllizenzen (Retail), je nachdem, welcher Fall zuerst eintritt. Weitere Informationen finden Sie unter Zusatzkulanzzeitraum.

Director zeigt den Status des Kulanzzeitraums an. Weitere Informationen finden Sie in den Fenstern im Director-Dashboard.

Was passiert, wenn ich die Zahl der erworbenen Gleichzeitig-Lizenzen überschreite?

Wenn alle Lizenzen verwendet werden, ermöglicht der Zusatzkulanzzeitraum unbegrenzte Verbindungen zu einem Produkt. Der Zusatzkulanzzeitraum gibt Ihnen Zeit, den Grund für das Überschreiten der maximalen Lizenzanzahl festzustellen und weitere Lizenzen zu erwerben, ohne dass Störungen für Benutzer auftreten. Der Zeitraum endet nach 15 Tagen oder mit der Installation weiterer Volllizenzen (Retail), je nachdem, welcher Fall zuerst eintritt. Weitere Informationen finden Sie unter Zusatzkulanzzeitraum.

Director zeigt den Status des Kulanzzeitraums an. Weitere Informationen finden Sie in den Fenstern im Director-Dashboard.

Gibt es eine Lizenzanforderung für Citrix Virtual Apps and Desktops-Wartungsoptionen: Long Term Service Release oder Current Release (LTSR) oder aktuelles Release (CR)?

Citrix Virtual Apps and Desktops-Wartungsoptionen wie Long Term Service Release sind ein Vorteil des Customer Success Services-Programms. Sie müssen über aktive Customer Success Services verfügen, um einen Anspruch auf die LTSR-Vorteile zu haben. Weitere Informationen finden Sie unter Citrix Virtual Apps, Citrix Virtual Apps and Desktops, and Citrix Hypervisor Servicing Options.

Wie funktioniert die gepoolten Stunden für RBI Service?

Wenn Sie den Service für mindestens 25 Benutzer erwerben, erhalten Sie einen für alle Benutzer zusammen geltenden Pool von 5000 Stunden Nutzungsberechtigung. Bei anschließenden Käufen von Benutzerrechten wird die Zahl der Stunden im Pool nicht erhöht. Um Anspruch auf weitere Service-Zeit zu erhalten, erwerben Sie Add-On-Pakete.

Notfallwiederherstellung und Wartung des Lizenzservers

Informationen zur Notfallwiederherstellung und Wartung des Lizenzservers finden Sie unter Notfallwiederherstellung und Wartung in der Dokumentation zur Citrix Lizenzierung.

Kann ich Remote-PC-Zugriff mit CCU-Lizenzen verwenden?

Ja.

Informationen über Remote-PC-Zugriff finden Sie unter Remote-PC-Zugriff.

Produktspezifische Informationen zur Lizenzierung

- Citrix ADC
- Citrix Cloud
- Citrix Endpoint Management
- Citrix Gateway
- Citrix Hypervisor

Anwendungen

April 19, 2024

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 der Citrix Workspace-App 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.

Einzelheiten finden Sie in den folgenden Abschnitten:

- Erstellen von Bereitstellungsgruppen
- Erstellen von Anwendungsgruppen
- 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 Anwendungen, die Sie hinzufügen, 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 `Application`s bereits vorhanden ist und Sie versuchen, dem Ordner eine andere Anwendung mit dem Namen `app` 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 XenDesktop 7.x-Version vor Version 7.9 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 Anwendung 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 von App-Eigenschaften

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.

Eigenschaft	Seite
Kategorie/Ordner, in der/dem die Anwendung in der Citrix Workspace-App angezeigt wird	Bereitstellung
Befehlszeilenargumente (siehe Übergeben von Parametern an veröffentlichte Anwendungen)	Speicherort
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 (siehe Konfigurieren von Anwendungslimits)	Bereitstellung
Name: die Namen, die Benutzer und Administrator sehen	Identifizierung
Pfad zur ausführbaren Datei (siehe Übergeben von Parametern an veröffentlichte Anwendungen)	Speicherort
Verknüpfung auf dem Desktop des Benutzers: aktivieren oder deaktivieren	Bereitstellung
Sichtbarkeit: legt fest, welche Benutzer die Anwendung in der Citrix Workspace-App sehen (eine unsichtbare Anwendung kann trotzdem gestartet werden; damit sie auch nicht verfügbar ist, fügen Sie sie einer anderen Gruppe hinzu)	Sichtbarkeit beschränken
Arbeitsverzeichnis	Speicherort

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. der Citrix Workspace-App und von 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 ein beliebiges oder alle der möglichen Anwendungslimits konfigurieren:

- Maximale Anzahl gleichzeitiger Instanzen der Anwendung für alle Benutzer in der Bereitstellungsgruppe
- Eine Anwendungsinstanz pro Benutzer in der Bereitstellungsgruppe
- Maximale Anzahl gleichzeitiger Instanzen der Anwendung pro Maschine (nur PowerShell)

Wenn ein Limit konfiguriert ist und ein Benutzer versucht, eine Anwendungsinstanz zu starten, durch die das Limit überschritten würde, wird eine Fehlermeldung generiert. Wenn mehrere Limits konfiguriert sind, wird eine Fehlermeldung generiert, sobald das erste Limit erreicht ist.

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.
- **Maximale Anzahl gleichzeitiger Instanzen pro Maschine und Verwendung von Tagbeschränkungen:** Anwendung Charlie hat Lizenzierungs- und Leistungsanforderungen, die bestimmen, wie viele Instanzen gleichzeitig auf einem bestimmten Server ausgeführt werden können und wie viele Instanzen gleichzeitig auf allen Servern der Site ausgeführt werden können.

  Das Limit für die Anzahl der Anwendungsinstanzen pro Maschine gilt für jeden Server der Site (nicht nur für Maschinen in einer bestimmten Bereitstellungsgruppe). Angenommen, die Site hat drei Server. Sie konfigurieren für die Anwendung Charlie ein Limit von 2 für die Anwendungsinstanzen pro Maschine. In der gesamten Site dürfen daher maximal sechs Instanzen der Anwendung Charlie starten. (Maximal zwei Instanzen von Charlie auf jedem der drei Server)

  Um die Verwendung einer Anwendung auf spezifische Maschinen einer Bereitstellungsgruppe zu beschränken (zusätzlich zur siteweiten Beschränkung für alle Maschinen), konfigurieren Sie die maximale Anzahl von Instanzen pro Maschine über Tags.

Werden Anwendungsinstanzen auch über andere Methoden als das Controllerbrokering gestartet (z. B. wenn ein Controller im Ausfallmodus ist) 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 der maximalen Anzahl Instanzen pro Bereitstellungsgruppe und des Limits von einer Instanz pro Benutzer:

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:

   - 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

4. Klicken Sie auf **OK**, um die Änderung zu übernehmen und das Dialogfeld zu schließen, oder auf **Anwenden**, um die Änderung zu übernehmen und das Dialogfeld geöffnet zu lassen.

Konfigurieren der maximalen Anzahl von Instanzen pro Maschine (nur PowerShell):

- Geben Sie in PowerShell (Remote-PowerShell-SDK für Citrix Cloud-Bereitstellungen oder PowerShell-SDK für On-Premises-Bereitstellungen) das entsprechende `BrokerApplication` -Cmdlet mit dem Parameter `MaxPerMachineInstances` ein.
- Hilfe können Sie mit dem Cmdlet `Get-Help` aufrufen. Beispiel:

  ```
  Get-Help Set-BrokerApplication –Parameter MaxPerMachineInstances
  ```

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:\Program Files\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.

- **Anzeigen aller Ordner (unter Ausschluss verschachtelter Ordner):** Klicken Sie oberhalb der Ordnerliste auf **Alle anzeigen**.
- **Erstellen eines (unverschachtelten) Ordners auf der höchsten Ebene:** Wählen Sie den Ordner "Applications". 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.
- **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. Die einfachste Möglichkeit zum Verschieben von Ordnern ist das Drag & Drop.
- **Umbenennen eines Ordners:** Wählen Sie den Ordner und dann im Aktionsbereich **Ordner umbenennen**. Geben Sie einen Namen ein.
- **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 Ob-

jekte auch gelöscht. Beim Löschen einer Anwendung wird die Anwendungszuweisung aus der Bereitstellungsgruppe aber nicht aus der Maschine entfernt.

- **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.

Steuern des lokalen Starts von Anwendungen auf veröffentlichten Desktops

Wenn Benutzer eine veröffentlichte Anwendung auf einem veröffentlichten Desktop starten, können Sie steuern, ob die Anwendung in der Desktopsitzung oder als veröffentlichte Anwendung gestartet wird. Die Citrix Workspace-App sucht in der Windows-Registrierung auf dem VDA den Installationspfad der Anwendung und startet die lokale Instanz, sofern eine solche vorhanden ist. Andernfalls wird eine gehostete Instanz gestartet. Wenn Sie eine Anwendung starten, die nicht auf dem VDA installiert ist, wird die gehostete Anwendung gestartet. Weitere Informationen finden Sie unter vPrefer-Start.

In PowerShell (Remote-PowerShell-SDK für Citrix Cloud-Bereitstellungen oder PowerShell-SDK für On-Premises-Bereitstellungen) können Sie diese Aktion ändern.

Verwenden Sie im Cmdlet `New-Broker Application` oder `Set-BrokerApplication` die Option `LocalLaunchDisabled`. Beispiel:

```
Set-BrokerApplication -LocalLaunchDisabled <Boolean>
```

Standardmäßig ist der Wert dieser Option "false"(`-LocalLaunchDisabled $false`). Wird eine veröffentlichte Anwendung auf einem veröffentlichten Desktop gestartet, dann wird die Anwendung in der betreffenden Desktopsitzung gestartet.

Wenn Sie den Wert der Option auf "true"setzen (`-LocalLaunchDisabled $true`), wird die veröffentlichte Anwendung gestartet. Dabei wird mit der Citrix Workspace-App für Windows eine zusätzliche, eigene Sitzung zwischen dem veröffentlichten Desktop und der veröffentlichten Anwendung erstellt.

Anforderungen und Einschränkungen:

- Der `ApplicationType`-Wert für die Anwendung muss `HostedOnDesktop` sein.
- Diese Option ist nur über das entsprechende PowerShell-SDK verfügbar. Sie ist derzeit nicht in der grafischen Oberfläche von Studio verfügbar.
- Die Option erfordert mindestens StoreFront 3.14, Citrix Receiver für Windows 4.11 und Delivery Controller 7.17.

Apps für die Universelle Windows-Plattform

January 24, 2023

Informationen zu Universelle Windows-Plattform (UWP)-Apps finden Sie in der folgenden Dokumentation von Microsoft:

- What's a Universal Windows Platform (UWP) app?
- Windows-Paket-Manager

Anforderungen und Einschränkungen

Citrix Virtual Apps and Desktops unterstützt UWP-Apps mit VDAs auf den folgenden Windows-Maschinen:

- Windows 10 und spätere Versionen
- Windows Server 2016 und spätere Versionen

Die VDAs müssen mindestens in Version 7.11 vorliegen.

Folgende Citrix Virtual Apps and Desktops-Features werden entweder nicht unterstützt oder unterliegen Einschränkungen, wenn UWP-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 UWP-Apps nicht unterstützt.
- Wartungscenter-Remoting: UWP-Apps können das Wartungscenter zur Anzeige der Meldungen in der Sitzung nutzen. Diese Nachrichten werden derzeit nicht an den Endpunkt umgeleitet, um dem Benutzer angezeigt zu werden.

Das Starten von UWP-Apps und Nicht-UWP-Apps von dem gleichen Server wird nicht unterstützt. Platzieren Sie stattdessen UWP-Apps und Nicht-UWP-Apps in separate Bereitstellungsgruppen oder Anwendungsgruppen.

Da alle UWP-Apps auf einer Maschine enumeriert werden, empfiehlt Citrix, den Benutzerzugriff auf den Windows Store zu deaktivieren. Dadurch wird verhindert, dass ein Benutzer auf eine von einem anderen Benutzer installierte UWP-App zugreift.

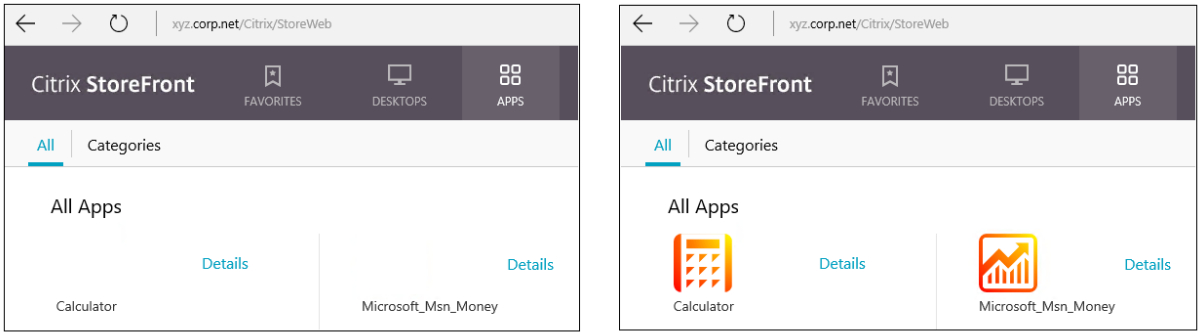
Beim Sideloading werden UWP-Apps auf der Maschine installiert und sind für andere Benutzer verfügbar. Wenn ein anderer Benutzer die App startet, wird sie installiert, und das Betriebssystem aktualisiert die AppX-Datenbank, um anzuzeigen, dass die App von diesem Benutzer installiert wurde.

Eine ordnungsgemäße Abmeldung von einer veröffentlichten UWP-App, die in einem festen oder Seamlessfenster gestartet wurde, verhindert möglicherweise, dass die VDA-Sitzung geschlossen und der Benutzer zwangsweise abgemeldet wird. In diesem Fall verhindern mehrere in der VDA-Sitzung verbleibende Prozesse, dass sie richtig geschlossen wird. Zur Problemlösung ermitteln Sie, welche Prozesse das Schließen der VDA-Sitzung verhindern, und fügen Sie diese dann dem Wert des Registrierungsschlüssels "LogoffCheckSysModules"hinzu. Folgen Sie hierfür den Anweisungen unter CTX891671.

Namen und Beschreibungen UWP-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 Bekannte Probleme.

Derzeit haben mehrere UWP-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. Am Ende der Datei fügen Sie `.storeapp-icon { background-image: radial-gradient( circle at top right, yellow, red ); }` an. Die Abbildung unten zeigt die Anzeige vor und nach dieser Korrektur.



Before **After**

Unter Windows Server 2016 und höher wird beim Starten einer universellen App möglicherweise auch der Server-Manager gestartet. Um dies zu verhindern, deaktivieren Sie den automatischen Start des Server-Managers über den Registrierungsschlüssel HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ServerManager' Einzelheiten finden Sie unter https://blog.rmilne.ca/2014/05/30/how-to-hide-server-manager-at-logon/.

UWP-Apps installieren und veröffentlichen

Unterstützung für UWP-Apps ist standardmäßig aktiviert.

Verwenden Sie zum Installieren einer oder mehrerer UWP-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 Windows Package Manager.
- Laden Sie die Apps per Sideloading. Weitere Informationen finden Sie unter Sideload line of business (LOB) apps in Windows client devices.
- Installieren Sie die UWP-Apps für jeden Zielbenutzer direkt aus dem Windows Store for Business.

UWP-Apps zu Citrix Virtual Apps oder Citrix Virtual Desktops hinzufügen (veröffentlichen):

1. Nachdem die UWP-Apps auf der Maschine installiert sind, fügen Sie die UWP-Apps einer Bereitstellungsgruppe oder Anwendungsgruppe hinzu. Sie können dies beim Erstellen der Gruppe oder später tun. Wählen Sie auf der Seite **Anwendungen** im Menü **Hinzufügen** die Option **Vom Startmenü**.
2. Wenn die Liste der Anwendungen angezeigt wird, aktivieren Sie die UWP-Apps, die Sie veröffentlichen möchten.
3. Fahren Sie mit dem Assistenten fort oder schließen Sie das Bearbeitungsdialogfeld.

Informationen zu zusätzlichen Konfigurationsanforderungen bei der Verwendung von User Profile Manager (UPM) finden Sie unter
Windows Apps - Microsoft Store.

Um die Verwendung von UWP-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.

UWP-Apps deinstallieren

Wenn Sie eine UWP-App mit einem Befehl wie `Remove-AppXPackage` deinstallieren, wird sie 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

June 27, 2024

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 Citrix Virtual Apps-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 Citrix Virtual Apps- oder Citrix Virtual Desktops-Site auf maximal 50 beschränken.

  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 Citrix Gateway. Die Sitedatenbank muss immer in der primären Zone sein.

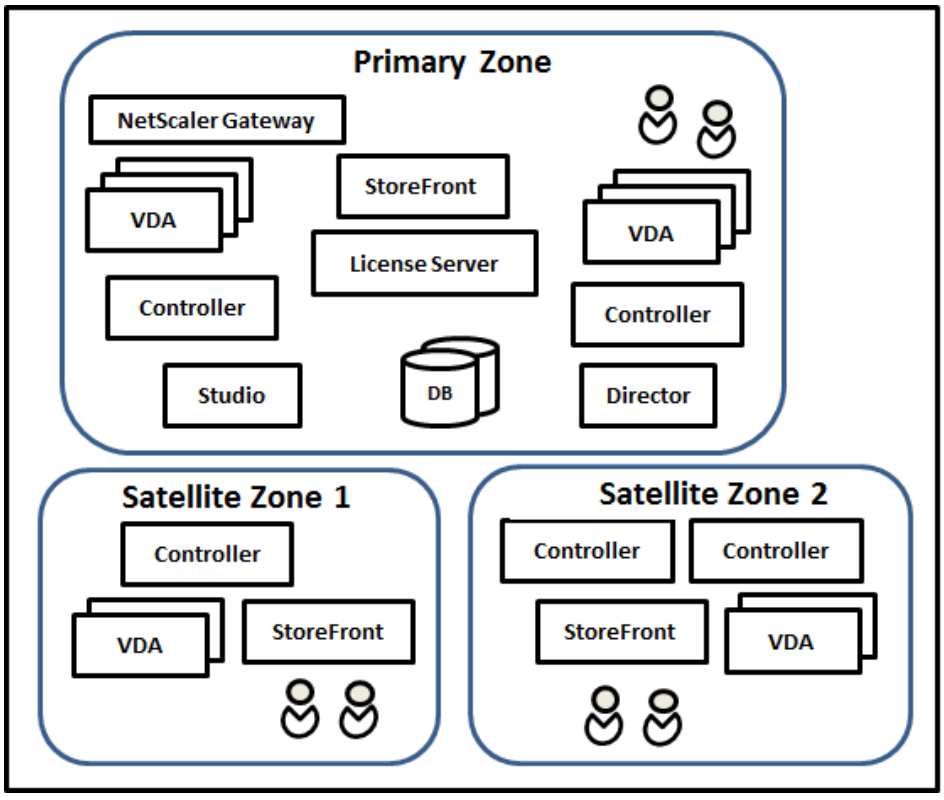
Die primäre Zone sollte aus Redundanzgründen außerdem mindestens zwei Controller enthalten und kann einen oder mehrere VDAs mit Anwendungen umfassen, die eng an die Datenbank und Infrastruktur gekoppelt sind.

Satellitenzonen:

Eine Satellitenzone enthält einen oder mehrere VDAs, Controller und StoreFront- sowie Citrix 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.



Erläuterung der Abbildung:

- **Primary 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 Citrix Gateway.

- **Satellite zone 1:** 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 lokalem Hostcache 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.

- **Satellite zone 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 andere Zone verschieben, stellen Sie sicher, dass diese mit Zone mit der zugehörigen Hostverbindung ordnungsgemäß verbunden ist. Bei begrenzter Bandbreite oder hoher Latenz verschieben Sie die Hostverbindung in die Zone, die den zugehörigen Maschinenkatalog enthält.)

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

Zur Verwendung des Zonenpräferenz-Features müssen Sie mindestens StoreFront 3.7 und Citrix 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.

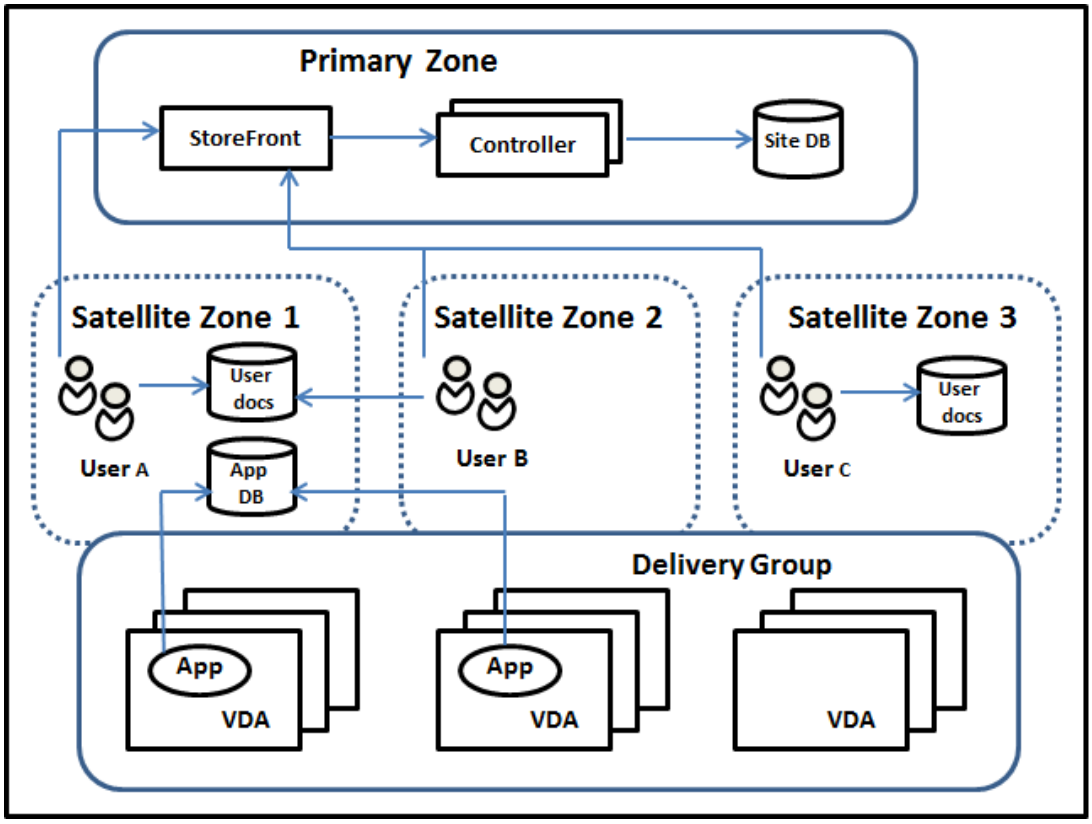
Funktionsweise der Zonenpräferenz

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 die Citrix Workspace-App 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 die Citrix Workspace-App an diversen Standorten ausführen können: Benutzer A verwendet ein Gerät mit der Citrix Workspace-App 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 Homezone 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. Sie haben folgende Möglichkeiten:

- 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 die Reihenfolge einschränken (siehe Anpassen der Zonenpräferenz). Ein Benutzer startet eine Anwendung:

- 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 Workspace-App-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 Workspace-App-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 der Citrix Workspace-App auf dem Endpunktgerät durch das Citrix Gateway erforderlich, über welches das Gerät eine Verbindung herstellt. Hierfür muss das Citrix Gateway 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. (Bei Verbindungen mit niedriger Latenz und hoher Bandbreite können sie sich jedoch in verschiedenen Zonen befinden.)
- 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 Citrix 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 Site. Wenn ein Citrix 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 Citrix 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 Citrix 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 Citrix Provisioning: Die mit diesem Release bereitgestellte Citrix Provisioning Console 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 Citrix Provisioning Console zum Bereitstellen von Maschinen in diesem Katalog. Wenn Sie den Katalog mit dem Citrix Provisioning-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 werden 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

September 21, 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 unter Delegierte Administration.

Informationen zu Verbindungstypen

Mit den unterstützten Virtualisierungsplattformen können Sie Maschinen in der Citrix Virtual Apps- oder Citrix Virtual Desktops-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 Azure Resource Manager:**
  - Artikel über Microsoft Azure Resource 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. Geben Sie auch die Werte für Region, Availability Zone, VPC-Namen, Subnetzadressen, Domänenname, Namen der Sicherheitsgruppen und Anmeldeinformationen an.
  - Konfigurieren Sie eine AWS-Hostingverbindung für die Verwendung von IAM-Rollen, indem Sie **role_based_auth** als Wert für die Felder "Zugriffsschlüssel"und "Geheimer Schlüssel"eingeben. Eine IAM-Rolle, über welche die für Citrix erforderlichen Richtlinien und Berechtigungen festgelegt sind, ist beim Anfügen an von AWS gehostete Delivery Controller bzw. Cloud Connector-Instanzen erforderlich.
  - 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.

- **Citrix Hypervisor (ehemals XenServer):**
  - Citrix Hypervisor-Virtualisierungsumgebungen.
  - Citrix Hypervisor-Dokumentation.
- **Nutanix Acropolis:**
  - Nutanix-Virtualisierungsumgebungen
  - Nutanix-Dokumentation.
- **VMware:**
  - VMware-Virtualisierungsumgebungen
  - VMware-Produktdokumentation
- **Microsoft Hyper-V:**
  - Artikel über Microsoft System Center Virtual Machine Manager-Virtualisierungsumgebungen
  - Microsoft-Dokumentation
- **Microsoft Azure (Classic):**
  - Dieser Hosttyp ist veraltet.
  - Microsoft Azure-Virtualisierungsumgebungen
  - Microsoft-Dokumentation
- **CloudPlatform:**
  - Dieser Hosttyp ist veraltet.

- 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.

Hostspeicher

Speicherprodukte werden unterstützt, wenn sie von einem unterstützten Hypervisor verwaltet werden. Der Citrix Support unterstützt Anbieter von Speicherprodukten bei der Problembehandlung und dokumentiert Probleme nach Bedarf im Knowledge Center.

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. Durch das Speichern von Daten 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.

Wenn Sie auf Citrix Hypervisor-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. Diese Methode erfordert keine Persistenz und weniger Resilienz wie 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. Citrix Hypervisor 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

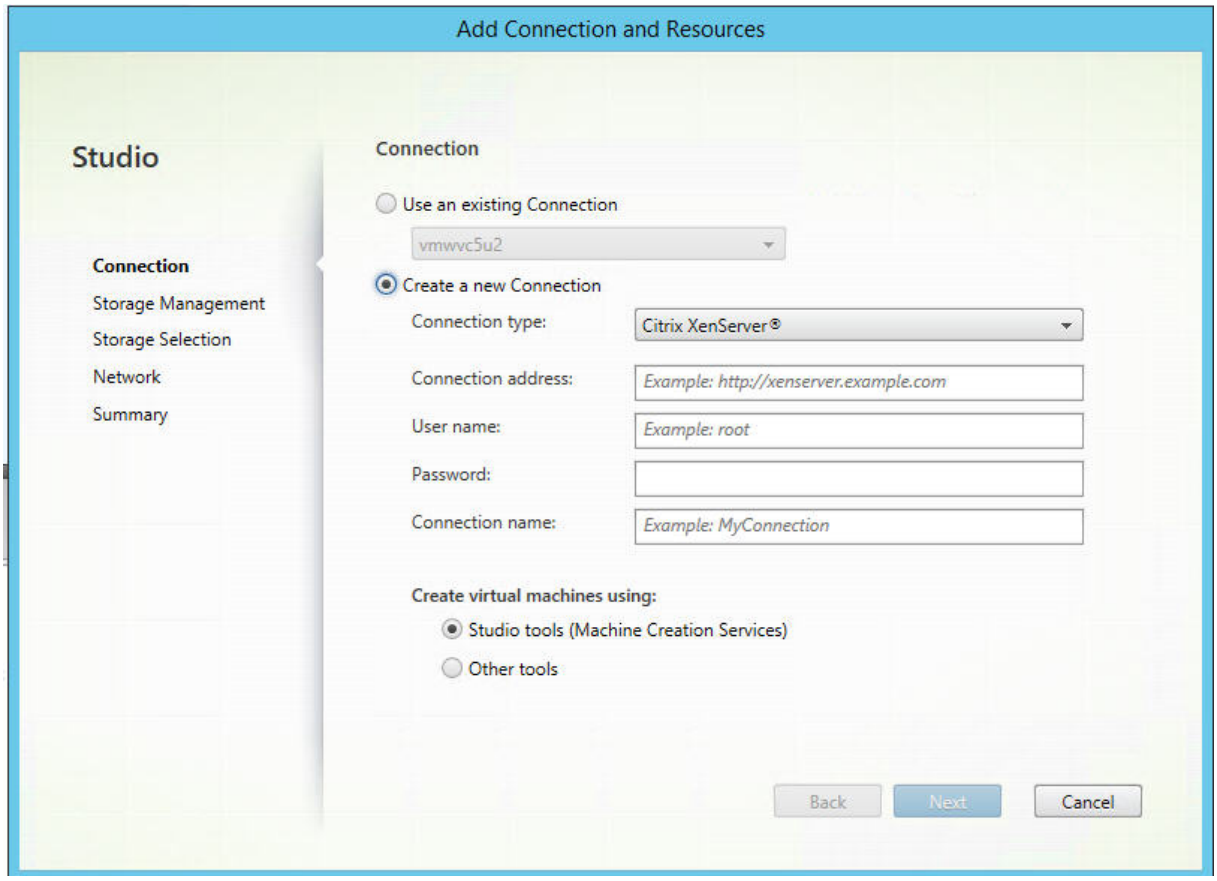
Sie können die erste Verbindung beim Erstellen der Site erstellen. Der Assistent für die Siteerstellung enthält die nachfolgend beschriebenen Seiten für Verbindungen: Verbindung, Speicherverwaltung, Speicherauswahl und Netzwerk.

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 erstellen.

1. Wählen Sie im **Studio**-Navigationsbereich **Konfiguration > Hosting**.
2. Wählen Sie im Bereich **Aktionen** die Option **Verbindung und Ressourcen hinzufügen**.
3. 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.

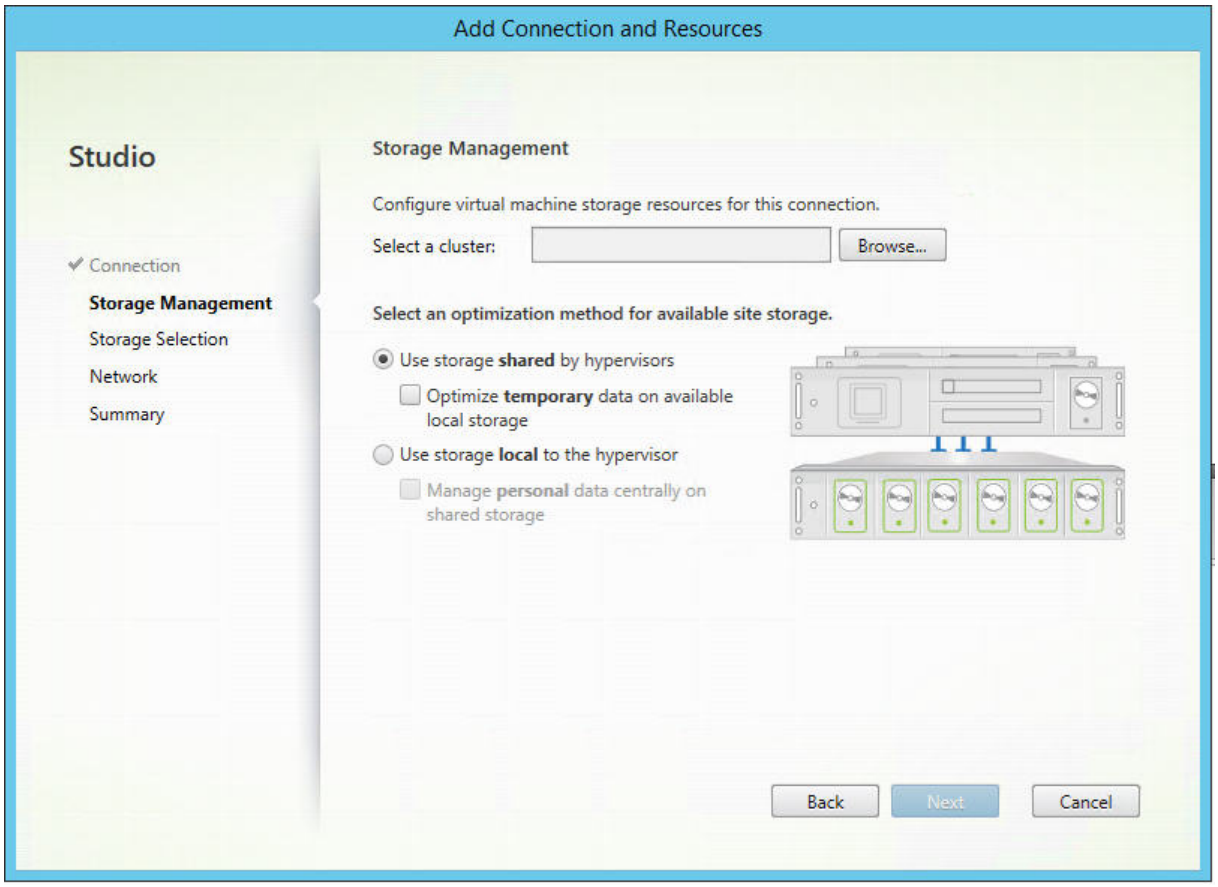
Verbindung



Auf der Seite **Verbindung**:

- Um eine 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 oder Citrix Provisioning) oder andere Tools.

Speicherverwaltung



Informationen zur Speicherverwaltungstypen und -methoden finden Sie unter Hostspeicher.

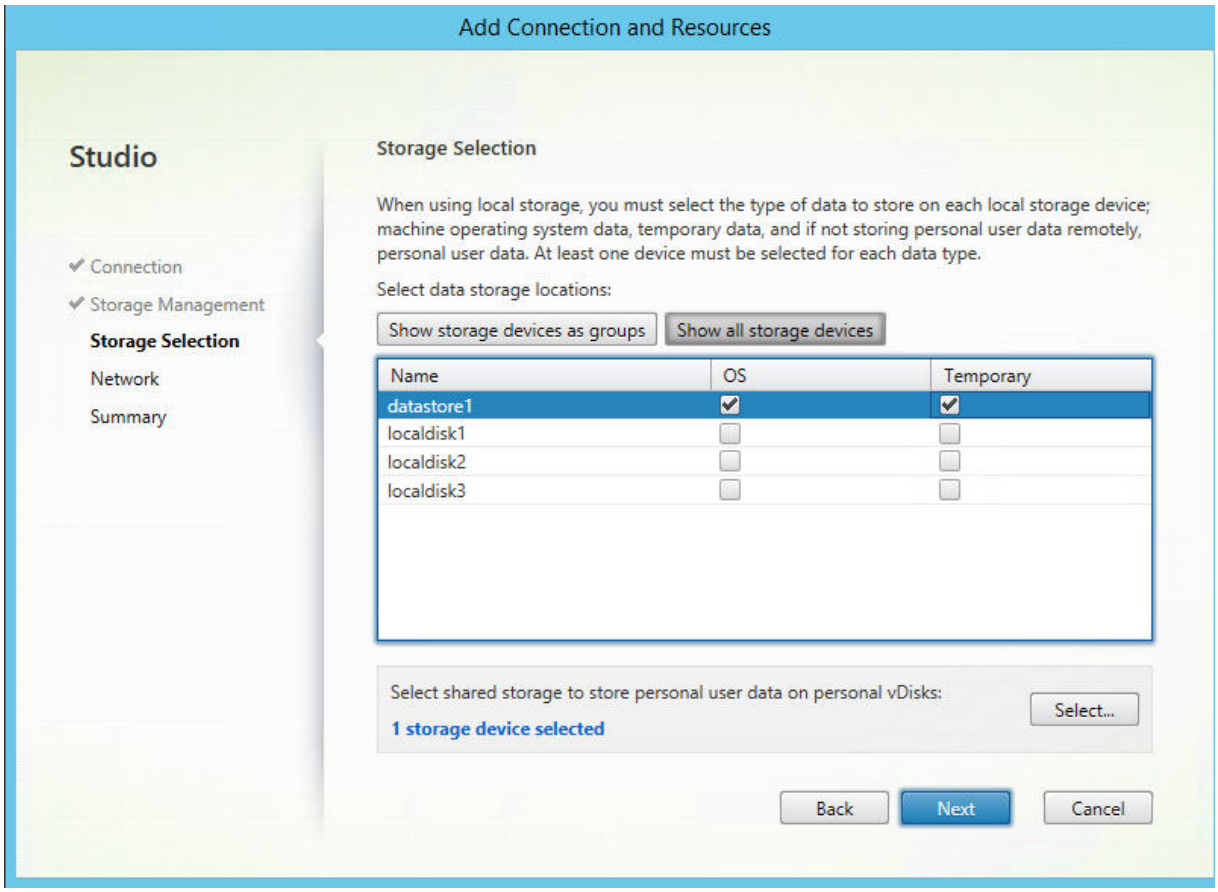
Wenn Sie eine Verbindung zu einem Hyper-V- oder VMware-Host konfigurieren, navigieren Sie zu einem Clusternamen und wählen Sie ihn aus. Andere Verbindungstypen erfordern keine Clusternamen.

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 in einem Citrix Hypervisor-Pool verwenden, geben Sie an, ob Sie IntelliCache zum Reduzieren der Last auf dem freigegebenen Speichergerät verwenden. Siehe Verwenden von IntelliCache für Citrix Hypervisor-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 weitere 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**.

Netzwerk

Geben Sie auf der Seite **Netzwerk** 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 auf der Seite **Zusammenfassung** Ihre Angaben. Wenn Sie fertig sind, 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. Informationen finden Sie unter Erstellen eines Maschinenkatalogs.

Bearbeiten von Verbindungseinstellungen

Verwenden Sie diese Vorgehensweise nicht, um eine Verbindung umzubenennen oder 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 einer 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 Citrix Hypervisor-Verbindung wählen Sie **Server mit hoher Verfügbarkeit bearbeiten**. Citrix empfiehlt, dass Sie alle Server im Pool auswählen, um die Kommunikation mit Citrix Hypervisor 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 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 sowohl ganze als auch prozentuale Werte angeben. Der Grenzwert ist der niedrigere Wert.

  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.
- Geben Sie die Informationen im Feld **Verbindungsoptionen** nur unter der Anleitung eines Supportmitarbeiters von Citrix oder gemäß expliziter Anweisungen in der Dokumentation 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. Sie können den Wartungsmodus auch für Maschinen in Maschinenkatalogen und Bereitstellungsgruppen aktivieren oder deaktivieren.

Löschen einer Verbindung

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.

Aktion	Beschreibung
Starten	Die Maschine wird gestartet, wenn sie ausgeschaltet oder angehalten wurde.
Suspend	Die Maschine wird angehalten, ohne sie herunterzufahren, und die Liste der Maschinen aktualisiert.
Herunterfahren	Das Betriebssystem wird heruntergefahren.
Herunterfahren erzwingen	Das Abschalten der Maschine wird erzwungen und die Liste der Maschinen wird aktualisiert.

Aktion	Beschreibung
Restart	Das Betriebssystem wird heruntergefahren und die Maschine dann 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 Maschinenkatalog der Bereitstellungsgruppe gelöscht. Sie können Maschinen nur entfernen, wenn kein Benutzer mit ihnen verbunden ist. Aktivieren Sie den Wartungsmodus, um zu verhindern, dass Benutzer eine Verbindung herstellen, während Sie eine 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 von 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**.

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.

Problembehandlung

Anhand der Informationen in diesem Abschnitt können Sie Probleme bei Hostverbindungen beheben.

Zugriffsschlüsselfehler beim Hinzufügen der AWS EC2-URL auf der Hostingressource

Das Hinzufügen von AWS EC2 als Hostingverbindung und die Angabe des **API**-Schlüssels, des geheimen Schlüssels und des Verbindungsnamens im Citrix Studio-Knoten **Hosting** generiert einen SSL-Fehler. Es wird folgende Meldung angezeigt: Bei der Kombination aus **API**-Schlüssel und geheimem Schlüssel ist ein Fehler aufgetreten. Prüfen Sie die Eingabe.

Das Problem hat folgende Ursachen:

- Herstellen einer Verbindung mit dem externen Netzwerk über den Proxyserver
- Verwenden einer anderen EC2-Verbindung mit einer anderen URL-Verbindung vom Amazon AWS-Server

Im **Hostingknoten** von Studio ist die Standardadresszeichenfolge für eine EC2-Verbindung als globale Endpunkt-URL hartcodiert (`https://ec2.amazonaws.com`). Wenn der AWS-Dienst die Endpunkt-URL nicht an die von Ihnen angegebene weiterleiten kann, können Zugriffsschlüssel, einschließlich Zugriffsschlüssel-ID und geheimem Zugriffsschlüssel, nicht überprüft werden.

Um dieses Problem zu beheben, fügen Sie die EC-Verbindung mit einer anderen URL hinzu oder verwenden Sie für die Verbindung mit dem Internet einen Proxyserver. Erstellen Sie außerdem manuell über PowerShell anstelle von Citrix Studio eine EC2-Hostingverbindung:

1. Starten Sie PowerShell über den DDC-Host und laden Sie alle Citrix Module mit dem Befehl `asnp Citrix`.
2. Konfigurieren Sie Umgebungsvariablen für den Proxyserver und Port:


```
$server = "<PROXY_SERVER>"
$port = "<PROXY_SERVER_PORT>"
$options = "ProxyHost=$server,ProxyPort=$port"
<!--NeedCopy-->
```

Führen Sie die folgenden Befehle aus, um die EC2-Hostingverbindung hinzuzufügen:

```
$hyp= New-Item -Path xdhyp:\Connections -AdminAddress "localhost" -Name
     " AWSEC2 "  -ConnectionType "AWS" -HypervisorAddress @[AWS URL](
    https://<AWS_URL>) -UserName "APIkey" -Password "Secret key" -
    Metadata @{
  "Citrix_MachineManagement_Options" = $options  }
  -Persist
<!--NeedCopy-->
```

```
New-BrokerHypervisorConnection -HypHypervisorConnectionUid $hyp.
    HypervisorConnectionUid
<!--NeedCopy-->
```

Starten Sie Citrix Studio, und überprüfen Sie die Hostverbindung auf die Generierung der AWS EC2-Site.

Lokaler Hostcache

April 19, 2024

Um sicherzustellen, dass die Citrix Virtual Apps and Desktops-Sitedatenbank immer verfügbar ist, empfiehlt Citrix, unter Befolgung der bewährten Methoden zur hohen Verfügbarkeit von Microsoft mit einer fehlertoleranten SQL Server-Bereitstellung zu beginnen. (Eine Liste der unterstützten SQL Server-Features für hohe Verfügbarkeit finden Sie unter Datenbanken.) 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 Site. Es kommt zu einem Ausfall, wenn ein Fehler bei der Verbindung zwischen einem Delivery Controller und der Sitedatenbank in einer On-Premises-Citrix Umgebung auftritt Der lokale Hostcache wird aktiviert, wenn die Sitekonfigurationsdatenbank für 90 Sekunden nicht verfügbar ist.

Ab XenApp und XenDesktop 7.16 gibt es das Feature “Verbindungsleasing”(eine Vorgängerfunktion für hohe Verfügbarkeit) nicht mehr.

Dateninhalt

Der lokale Hostcache enthält folgende Informationen (die eine Teilmenge der Informationen in der Hauptdatenbank sind):

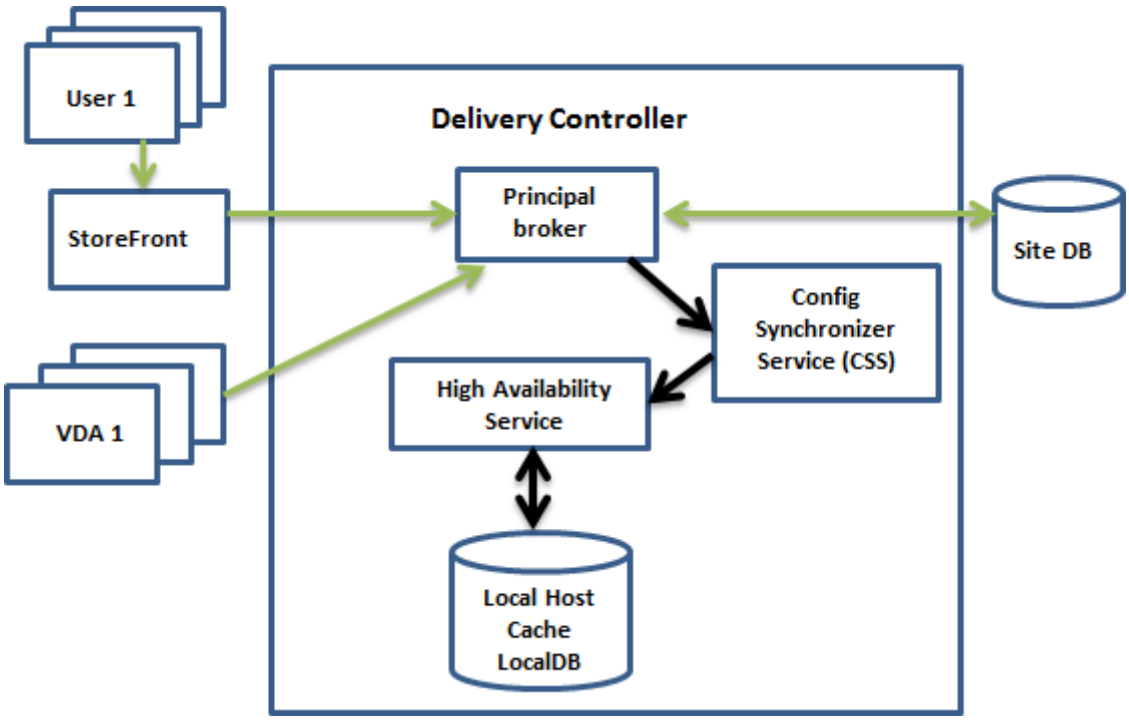
- Identität der Benutzer und Gruppen, denen Rechte für die in der Site veröffentlichte Ressourcen zugewiesen wurden.
- Identität der Benutzer, die Ressourcen der Site gerade verwenden oder kürzlich verwendet haben.
- Identität von VDA-Maschinen (einschließlich Remote-PC-Zugriffsmaschinen), die in der 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

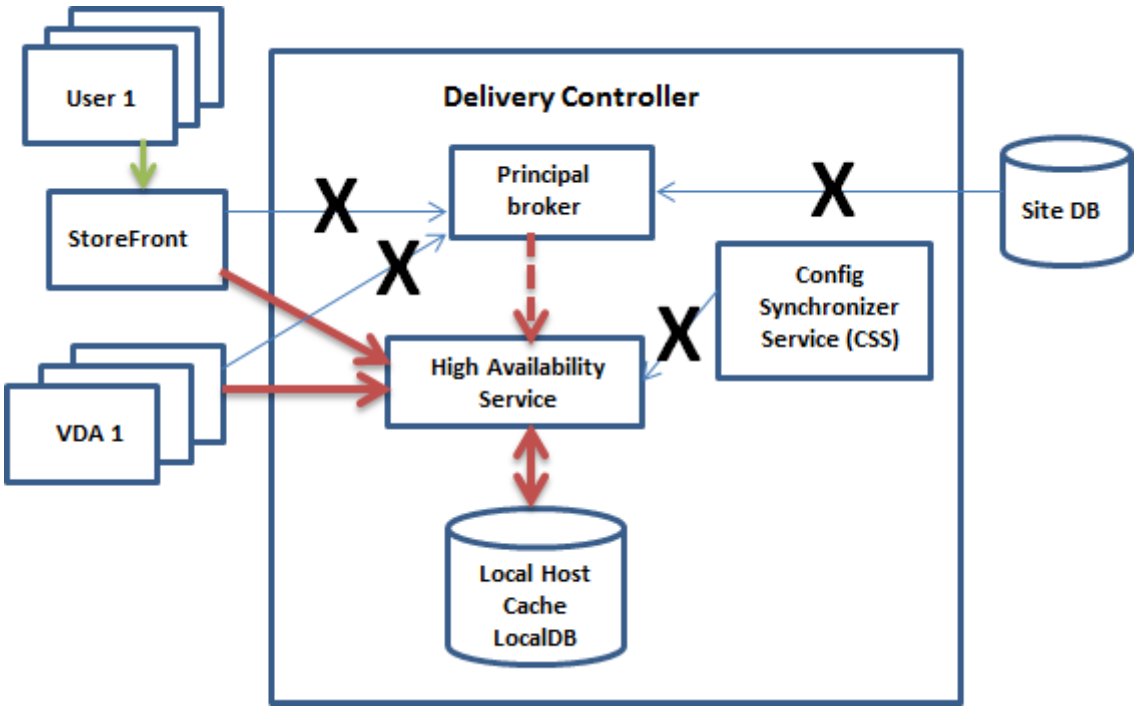
Die folgende Abbildung zeigt die Komponenten des lokalen Hostcaches und die im Normalbetrieb verwendeten Kommunikationspfade:



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.
- In regelmäßigen Abständen (eine Minute nach Abschluss der vorherigen Prüfung) 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, synchronisiert (d. h. kopiert) CSS (Citrix Config Sync-Dienst) die Informationen an CAS (Citrix Dienst für hohe Verfügbarkeit) auf dem Controller. (In einigen Teilen der Dokumentation wird der Dienst für hohe Verfügbarkeit als "sekundärer Broker"bezeichnet.) Alle Brokerkonfigurationsdaten, nicht nur die seit der letzten Überprüfung geänderten Elemente, werden kopiert. Der Dienst für hohe Verfügbarkeit importiert die Daten in eine Microsoft SQL Server Express-LocalDB-Datenbank auf dem Controller. Der CSS stellt sicher, dass die Informationen in dieser Datenbank 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 Dienst für hohe Verfügbarkeit an, auf Verbindungsanforderungen zu lauschen und diese zu verarbeiten (rote gestrichelte Linie in der Abbildung). Der Dienst für hohe Verfügbarkeit verwirft alle Anrufe vom CSS ab.
- Bei Ausfallbeginn hat der Dienst für hohe Verfügbarkeit keine aktuellen VDA-Registrierungsdaten, aber sobald der VDA mit ihm kommuniziert, wird eine Neuregistrierung ausgelöst. Während dieses Vorgangs erhält der Dienst für hohe Verfügbarkeit auch aktuelle Sitzungsinformationen zu dem betreffenden VDA.
- Während der Dienst für hohe Verfügbarkeit Verbindungen verarbeitet, überwacht der Hauptbroker weiterhin die Verbindung mit der Sitedatenbank. Wenn die Verbindung wiederhergestellt ist, weist der Hauptbroker den Dienst für hohe Verfügbarkeit 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 Dienst für hohe Verfügbarkeit entfernt alle verbleibenden VDA-Registrierungen aus dem vorherigen Ausfall und aktualisiert wieder die LocalDB-Datenbank mit den vom CSS empfangenen Konfigurationsänderungen.

Der Wechsel zwischen dem normalen und dem Ausfallmodus wirkt sich nicht auf bestehende Sitzungen aus, sondern nur auf den Start neuer Sitzungen.

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 Dienst für hohe Verfügbarkeit 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 Dienst für hohe Verfügbarkeit über alle anderen Dienste für hohe Verfügbarkeit informiert.

Die Dienste für hohe Verfügbarkeit kommunizieren miteinander über einen anderen Kanal. Anhand einer alphabetischen Liste der FQDNs der Maschinen, auf denen sie ausgeführt werden, ermitteln (wählen) sie, welcher Dienst für hohe Verfügbarkeit bei einem Ausfall das Brokering in der Zone übernimmt. Bei einem Ausfall registrieren sich alle VDAs bei dem gewählten Dienst für hohe Verfügbarkeit neu. Die nicht gewählten Dienste für hohe Verfügbarkeit in der Zone weisen eingehende Verbindungs- und VDA-Registrierungsanfragen aktiv ab.

Wenn ein gewählter Dienst für hohe Verfügbarkeit während eines Ausfalls ausfällt, wird ein anderer Dienst zur Übernahme ausgewählt 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

Es gibt keine zeitliche Begrenzung für den Betrieb in Ausfallmodus. Allerdings sollten Sie den Normalbetrieb so schnell wie möglich wiederherstellen.

Während eines Ausfalls nicht verfügbare Elemente und weitere Unterschiede

- 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 Dienst für hohe Verfügbarkeit enthält. Startvorgänge über Zonen hinweg (von einem Dienst für hohe Verfügbarkeit in einer Zone zu einem VDA in einer anderen Zone) werden während eines Ausfalls nicht unterstützt.
- Fällt vor einem geplanten Neustart von VDAs in einer Bereitstellungsgruppe die Sitedatenbank aus, beginnt der Neustart erst nach Ende des Ausfalls. Dies kann zu unbeabsichtigten Ergebnissen führen. Weitere Informationen finden Sie unter Verzögerung geplanter Neustarts aufgrund eines Datenbankausfalls.
- Tagbeschränkungen, bei denen Tags zur Bezeichnung von Zonen verwendet werden, werden für Sitzungsstarts nicht unterstützt. Wenn solche Tagbeschränkungen konfiguriert sind und die Option Erweiterte Integritätsprüfung eines StoreFront-Stores aktiviert ist, können Sitzungen sporadisch evtl. nicht gestartet werden.

Der lokale Hostcache wird für servergehostete Anwendungen und Desktops und statische (zugewiesene) Desktops unterstützt.

Standardmäßig sind energieverwaltete Desktop-VDAs in gepoolten (über MCS oder Citrix Provisioning erstellten) Bereitstellungsgruppen, für die die Eigenschaft `ShutdownDesktopsAfterUse` aktiviert ist, während eines Ereignisses mit dem lokalen Hostcache nicht für neue Verbindungen verfügbar. Sie können diese Standardeinstellung ändern, damit solche Desktops während des Ereignisses 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 folgende PowerShell-Cmdlets aus:


```
Set-BrokerSite -ReuseMachinesWithoutShutdownInOutageAllowed $true 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. Wenn dieses Feature aktiviert ist, werden VDAs nach Abschluss des LHC-Ereignisses nicht automatisch neu gestartet. Energieverwaltete Desktop-VDAs in gepoolten Bereitstellungsgruppen können Daten aus früheren Sitzungen beibehalten, bis der VDA neu gestartet wird. Dies kann auftreten, wenn sich ein Benutzer bei Nicht-LHC-Vorgängen vom VDA abmeldet oder der Neustart manuell ausgelöst werden kann.

> **Wichtig:**
>
> Ohne die Aktivierung von ReuseMachinesWithoutShutdownInOutageAllowed auf Siteebene und ReuseMachinesWithoutShutdownInOutage auf Bereitstellungsgruppenebene schlagen alle Sitzungsstartversuche für energieverwaltete Desktop-VDAs in gepoolten Bereitstellungsgruppen während eines lokalen Hostcache-Ereignisses fehl.

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. Auf dem Laufwerk, auf dem die LocalDB installiert ist, muss ausreichend Speicherplatz für das Wachstum der Datenbank vorhanden sein. 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 Dienst für hohe Verfügbarkeit alle Verbindungen. In Sites (oder Zonen) mit Lastausgleich zwischen mehreren Controllern muss der gewählte Dienst für hohe Verfügbarkeit daher möglicherweise viel mehr Anfragen verarbeiten als im Normalbetrieb. Die CPU-Anforderungen sind somit höher. Jeder einzelne Dienst für hohe Verfügbarkeit 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 Dienst für hohe Verfügbarkeit 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 Dienst für hohe Verfügbarkeit benötigt wird, hat dieser 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"Dienst für hohe Verfügbarkeit) 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 neu registrieren müssen:

- Ausfallbeginn: bei der Migration von einem Hauptbroker zu einem Dienst für hohe Verfügbarkeit
- Ausfall des Diensts für hohe Verfügbarkeit während eines Ausfalls: Bei der Migration von einem ausgefallenen Dienst für hohe Verfügbarkeit zu einem neu gewählten.
- 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
```

Seien Sie vorsichtig, wenn Sie den Heartbeatwert ändern. Eine Erhöhung führt zu einer größeren Last auf den Controllern im normalen und im Ausfallmodus.

Das Intervall kann nicht vollständig eliminiert werden, egal wie schnell die VDAs registrieren.

Die Dauer der Synchronisierung zwischen den Diensten für hohe Verfügbarkeit erhöht sich mit steigender Anzahl der Objekte (VDAs, Anwendungen, Gruppen usw.). Die Synchronisierung von 5000 VDAs kann beispielsweise zehn Minuten oder länger dauern. Informationen zu Synchronisierungseinträgen im Ereignisprotokoll finden Sie unter Überwachen.

Unterschiede zu XenApp 6.x-Versionen

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.

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 Dienst für hohe Verfügbarkeit kommuniziert mit dieser Datenbank. Sie können PowerShell-Cmdlets nicht verwenden, um Änderungen an dieser Datenbank vorzunehmen. 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 Dienst für hohe Verfügbarkeit verwenden.

Die Installation der LocalDB-Datenbank ist irrelevant für die Entscheidung, ob Sie SQL Server Express zur Verwendung als Sitedatenbank installieren.

Informationen zum Ersetzen einer älteren Version von SQL Server Express LocalDB durch eine neuere finden Sie unter Ersetzen von SQL Server Express LocalDB.

Standardeinstellungen nach Installation bzw. Upgrade des Produkts

Bei einer Neuinstallation von Citrix Virtual Apps and Desktops (Mindestversion 7.16) ist der lokale Hostcache aktiviert. Nach einem Upgrade (auf Version 7.16 oder höher) wird der lokale Hostcache aktiviert, wenn die Bereitstellung insgesamt weniger als 10.000 VDAs umfasst.

Aktivieren und Deaktivieren des lokalen Hostcaches

- Zum Aktivieren des lokalen Hostcache geben Sie Folgendes ein:

  ```
  Set-BrokerSite -LocalHostCacheEnabled $true
  ```

  Um zu ermitteln, ob der lokale Hostcache aktiviert ist, geben Sie Folgendes ein:

  ```
  Get-BrokerSite
  ```

  Überprüfen Sie, ob die Eigenschaft "LocalHostCacheEnabled"auf "True"festgelegt ist.
- Zum Deaktivieren des lokalen Hostcache geben Sie Folgendes ein:

  ```
  Set-BrokerSite -LocalHostCacheEnabled $false
  ```

Ab XenApp und XenDesktop 7.16 gibt es das Verbindungsleasing (Vorgängerfeature des lokalen Hostcache ab Version 7.6) nicht mehr.

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` als `REG_DWORD` auf 1 fest. Dadurch wird der Broker angewiesen, unabhängig vom Zustand der Datenbank in den Ausfallmodus zu wechseln. Wenn Sie den Wert auf 0 festlegen, wird der Ausfallmodus auf dem Server beendet.

Überwachung

Ereignisprotokolle enthalten Informationen zu Synchronisierungen und Ausfällen.

Config Synchronizer Service:

Im Normalbetrieb können beim Kopieren und Exportieren der Brokerkonfiguration durch den CSS und beim Importieren in die LocalDB unter Einsatz des Dienst für hohe Verfügbarkeit 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).
- 507: Import wurde aufgrund eines ausstehenden Ausfalls abgebrochen. Wenn ein Ausfall während einer Synchronisierung beginnt, wird der aktuelle Import verworfen und die letzte bekannte Konfiguration verwendet.
- 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 Dienst für hohe Verfügbarkeit hat das Brokering übernommen.
- 3503: Ein Ausfall wurde behandelt und der Normalbetrieb wieder aufgenommen.
- 3504: Gibt an, welcher Dienst für hohe Verfügbarkeit gewählt wurde und welche anderen 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: Sie können einen Bericht mit Informationen zu dem Fehlerpunkt erstellen. 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 Folgendes ein:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name
EnableCssTraceMode -PropertyType DWORD -Value 1
```

Der HTML-Bericht wird in folgendem Ordner gespeichert: C:\Windows\ServiceProfiles\NetworkService\AppData\L

Wenn der Bericht generiert wurde, deaktivieren Sie das Berichtsfeature mit folgendem Befehl:

```
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`.

Sicherheitsschlüssel verwalten

June 27, 2024

> **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 Studio, um die Feature-Einstellungen anzuzeigen.
2. Konfigurieren Sie die Einstellungen für Ihre Site (mit der Studio-Konsole oder PowerShell).
3. Konfigurieren Sie die Einstellungen in StoreFront (mit PowerShell).
4. Konfigurieren Sie die Einstellungen in Citrix ADC (mit PowerShell).

Studio aktivieren, um die Feature-Einstellungen anzuzeigen

Standardmäßig sind die Einstellungen für Sicherheitsschlüssel in Studio ausgeblendet. Verwenden Sie das PowerShell-SDK wie folgt, damit Studio sie anzeigen kann:

Führen Sie folgende Schritte aus, um das Feature zu aktivieren:

1. Führen Sie das Citrix Virtual Apps and Desktops 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"`

Weitere Informationen zum Remote PowerShell SDK finden Sie unter SDKs und APIs.

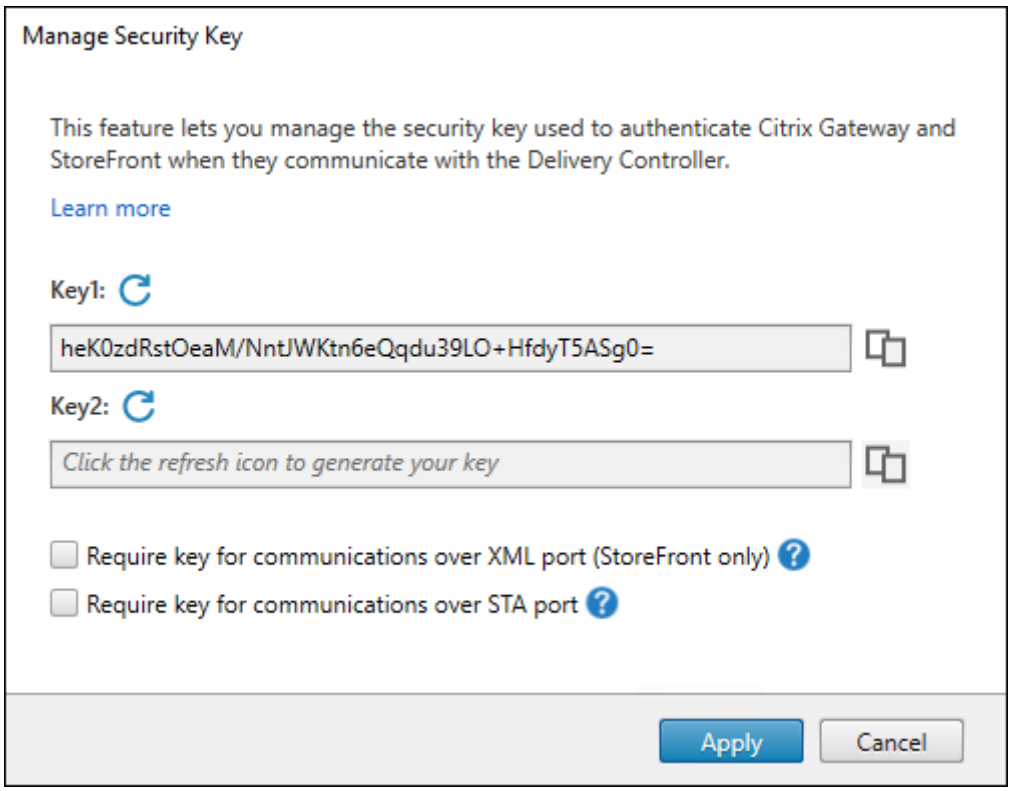
Einstellungen für die Site konfigurieren

Sie können Einstellungen in Studio über die Studio-Konsole oder PowerShell konfigurieren.

Verwenden der Studio-Konsole

Nachdem Sie Studio aktiviert haben, um die Feature-Einstellungen anzuzeigen, 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.

PowerShell verwenden

Nachfolgend sind die den Studio-Vorgängen entsprechenden PowerShell-Schritte aufgeführt.

1. Führen Sie das Citrix Virtual Apps and Desktops 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 den Befehl [Set-STFStoreFarm	https://developer-docs.citrix.com/en-us/storefront-powershell-sdk/current-release/Set-STFStoreFarm.html]. Beispiel

```
1 $store = Get-STFStoreService -VirtualPath [Path to store]
2 $farm = Get-STFStoreFarm -StoreService $store -FarmName [Resource feed
     name]
3 Set-STFStoreFarm -Farm $farm -XMLValidationEnabled $true -
     XMLValidationSecret [secret]
4 <!--NeedCopy-->
```

Geben Sie die entsprechenden Werte für die folgenden Parameter ein:

- `Path to store`
- `Resource feed name`
- `secret`

Um den Schlüssel für die Kommunikation über den STA-Port zu konfigurieren, verwenden Sie die Befehle `New-STFSecureTicketAuthority` und `Set-STFRoamingGateway`. Beispiel:

```
1 $gateway = Get-STFRoamingGateway -Name [Gateway name]
2 $sta1 = New-STFSecureTicketAuthority -StaUrl [STA1 URL] -
     StaValidationEnabled $true -StaValidationSecret [secret]
3 $sta2 = New-STFSecureTicketAuthority -StaUrl [STA2 URL] -
     StaValidationEnabled $true -StaValidationSecret [secret]
4 Set-STFRoamingGateway -Gateway $gateway -SecureTicketAuthorityObjs
     $sta1,$sta2
5 <!--NeedCopy-->
```

Geben Sie die entsprechenden Werte für die folgenden Parameter ein:

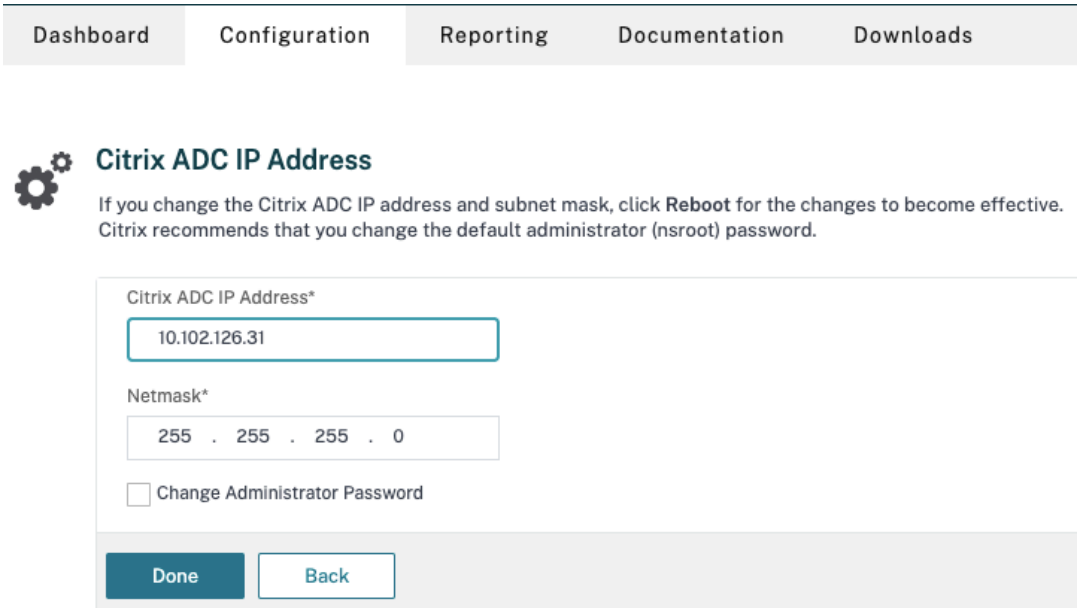
- `Gateway name`
- `STA URL`
- `Secret`

Anleitungen und Informationen zur Syntax finden Sie in der Hilfe zu PowerShell-Befehlen.

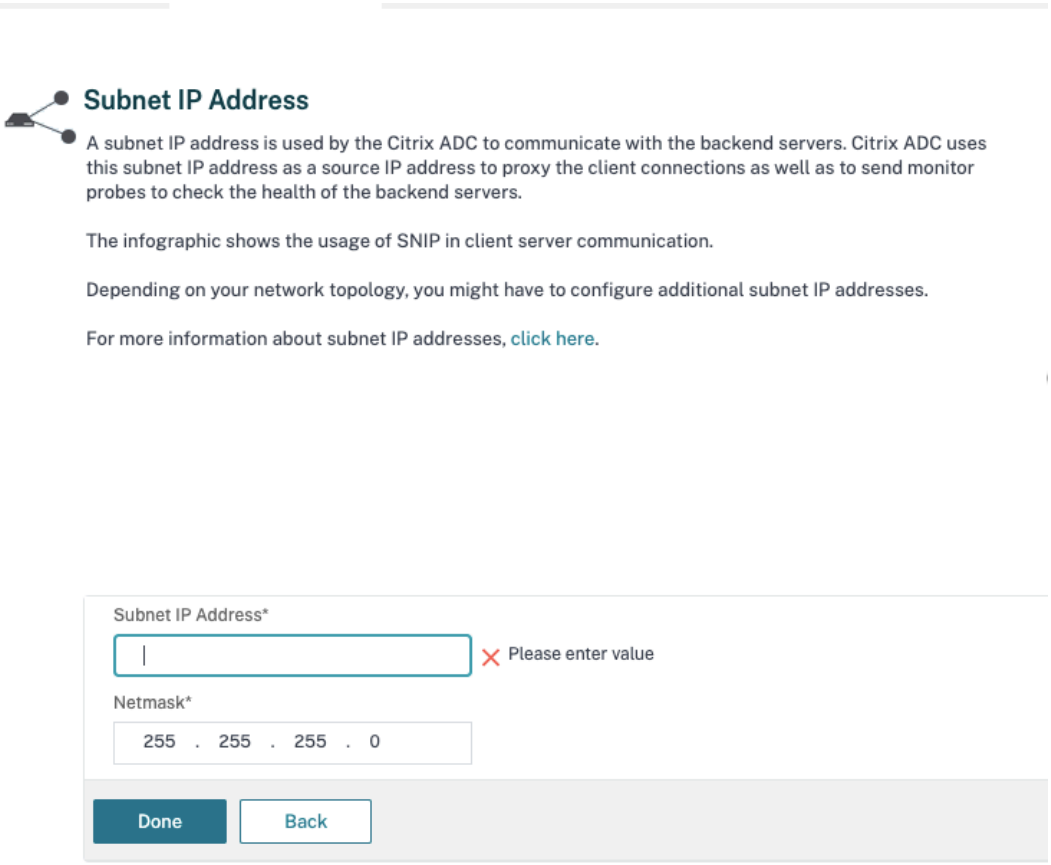
Konfigurieren der Einstellungen in Citrix ADC

> **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.

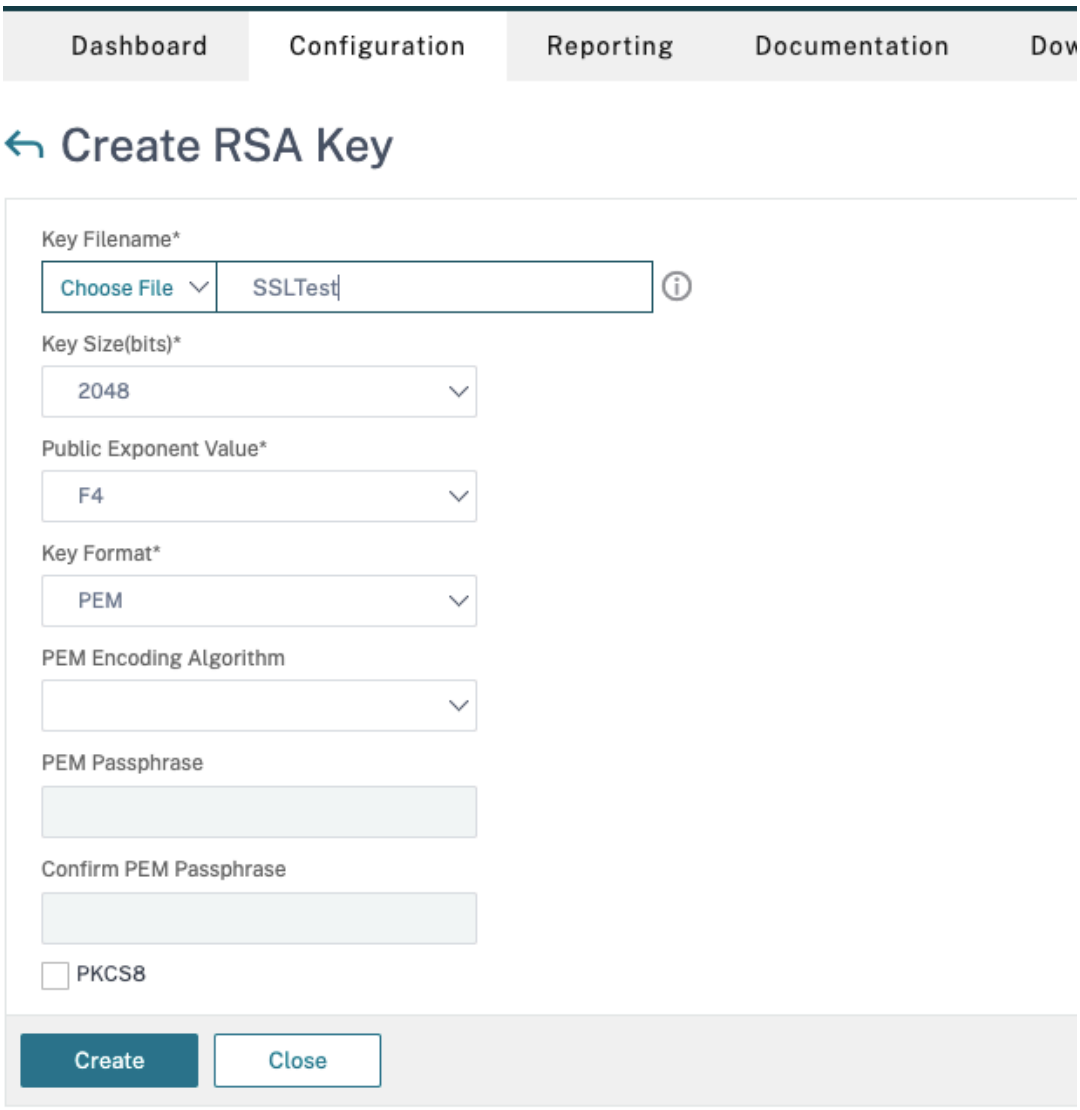
1. Vergewissern Sie sich, dass die erforderliche Konfiguration ausgeführt wurde:
   - Die folgenden IP-Adressen im Zusammenhang mit Citrix ADC wurden konfiguriert.
     - Citrix ADC Management-IP-Adresse (NSIP) für den Zugriff auf die Citrix ADC-Konsole. Weitere Informationen finden Sie unter Konfigurieren der NSIP-Adresse.



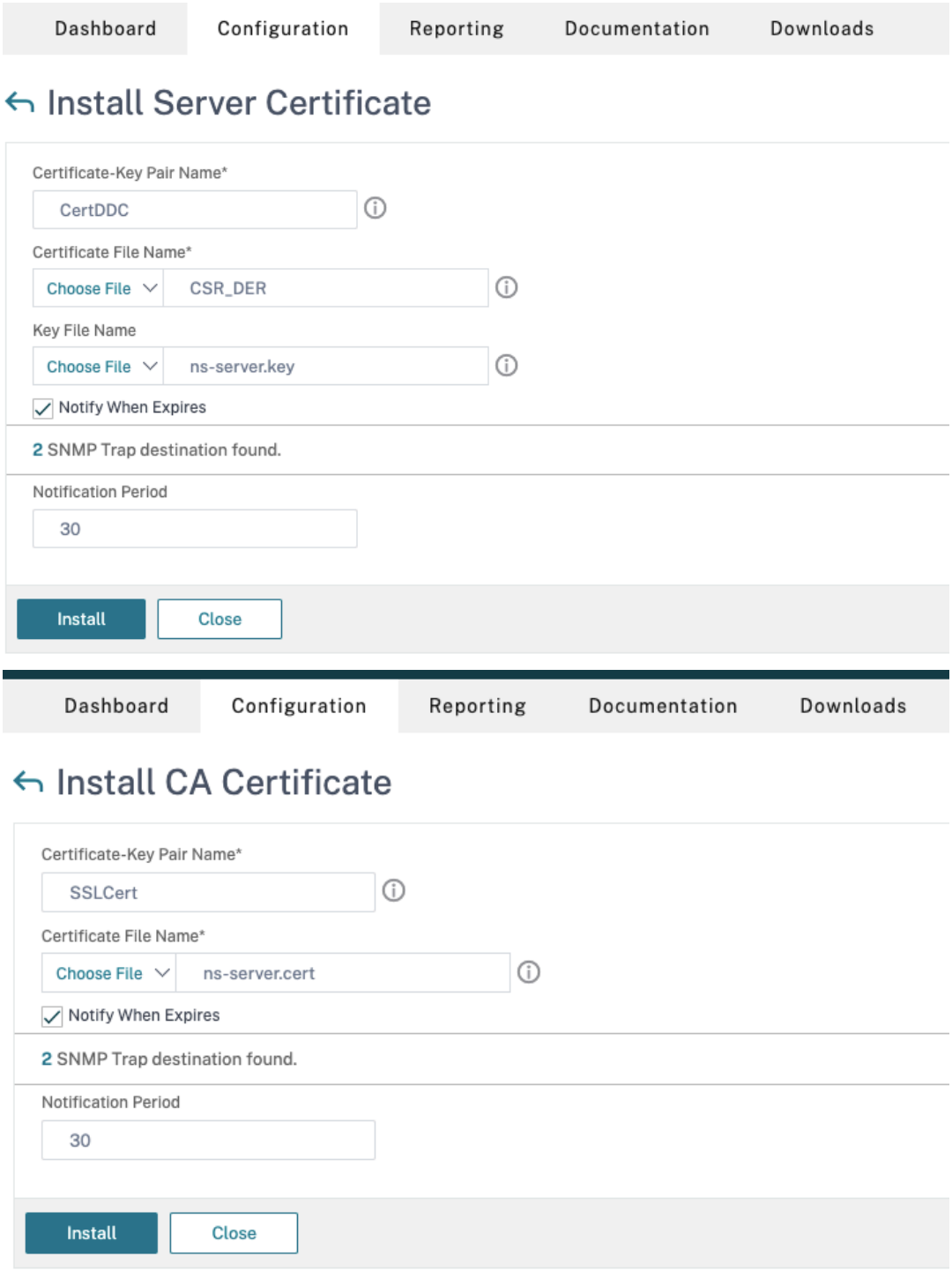
     - Subnetz-IP-Adresse (SNIP) zur Kommunikation zwischen der Citrix ADC Appliance und den Back-End-Servern. Weitere Informationen finden Sie unter Konfigurieren von Subnetz-IP-Adressen.
     - Virtuelle IP-Adresse von Citrix Gateway und des Load Balancers zur Anmeldung bei der ADC Appliance für den Sitzungsstart. Weitere Informationen finden Sie unter Erstellen eines virtuellen Servers.



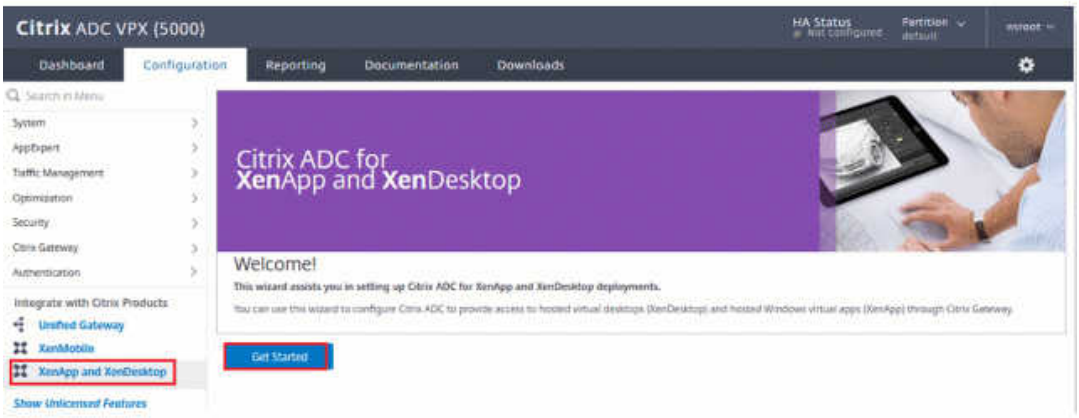
- Die erforderlichen Modi und Features in der Citrix ADC Appliance sind aktiviert.
  - Um die Modi zu aktivieren, gehen Sie in Citrix ADC zu **System > Settings > Configure Mode**.
  - Um die Features zu aktivieren, gehen Sie in Citrix ADC zu **System > Settings > Configure Basic Features**.
- Die Konfiguration 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.



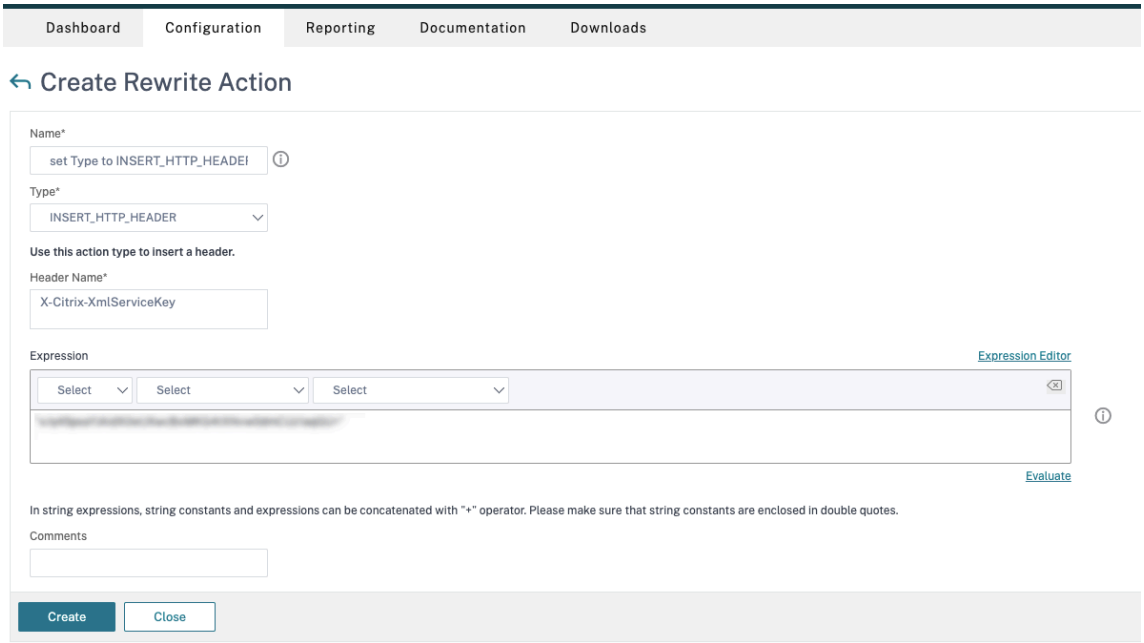
- Für Citrix Virtual Desktops wurde ein Citrix Gateway erstellt. Testen Sie die Verbindung durch Klicken auf die Schaltfläche **Test STA Connectivity**, um sicherzustellen, dass die virtuellen Server online sind. Weitere Informationen finden Sie unter Einrichten von Citrix ADC für Citrix Virtual Apps 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 Rewrite-Aktion hinzuzufügen. Sie können die Aktion "set Type to INSERT_HTTP_HEADER"nennen.

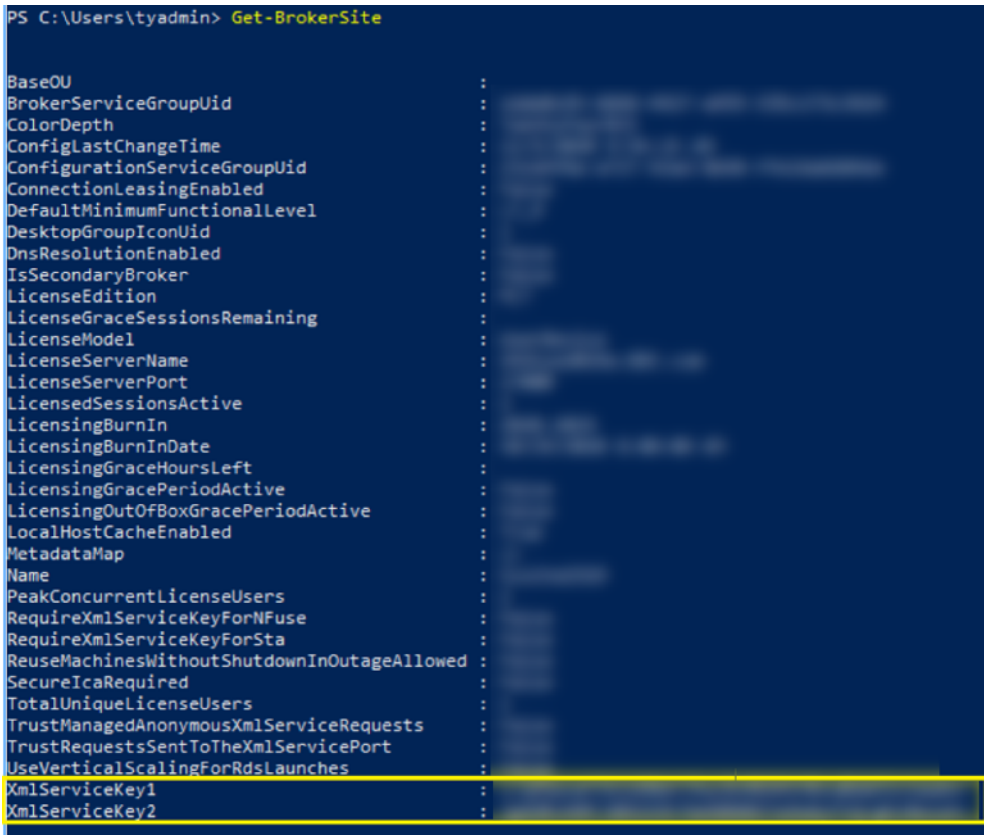


   a) Wählen Sie unter **Type** die Option **INSERT_HTTP_HEADER**.

   b) Geben Sie im Feld **Header Name** "X-Citrix-XmlServiceKey"ein.

   c) Fügen Sie unter **Ausdruck** <`XmlServiceKey1 value`> mit Anführungszeichen hinzu.

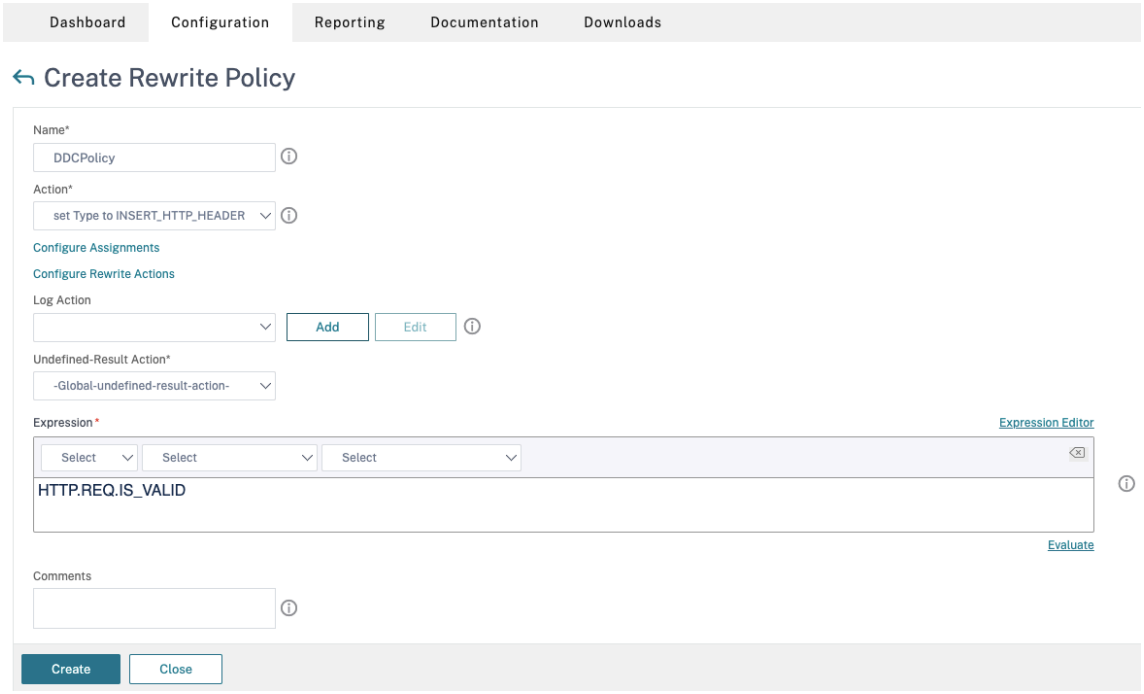
Sie können den XmlServiceKey1-Wert aus der Desktop Delivery Controller-Konfiguration kopieren.



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 **Hinzufügen**, um eine Richtlinie hinzuzufügen.



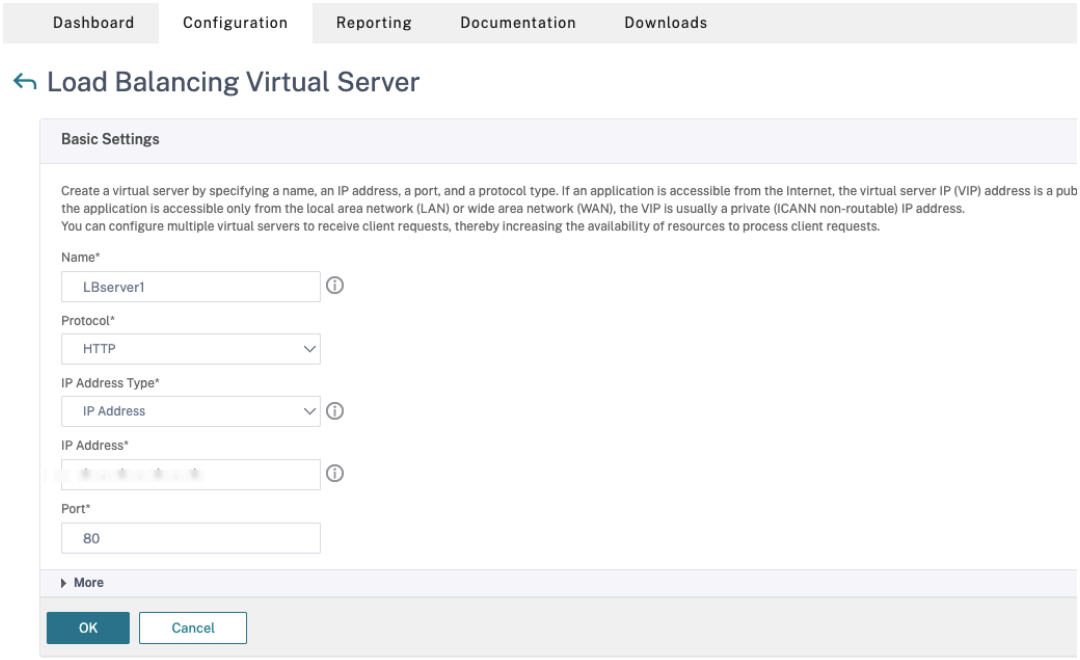
a) Wählen Sie unter **Action** die im vorherigen Schritt erstellte Aktion aus.
b) Fügen Sie unter **Expression** “HTTP.REQ.IS_VALID”hinzu.
c) Klicken Sie auf **OK**.

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.

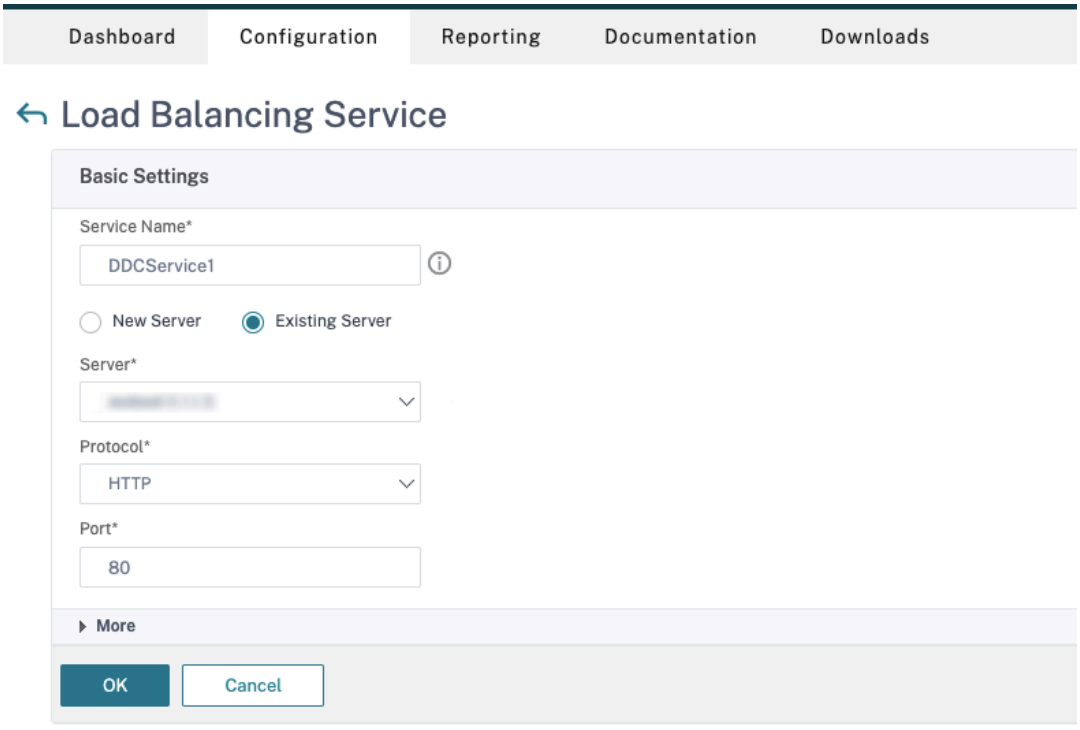
      - Gehen Sie zu **Traffic Management > Load Balancing > Servers**.
      - Klicken Sie auf der Seite **Virtual Servers** auf **Add**.



- 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.

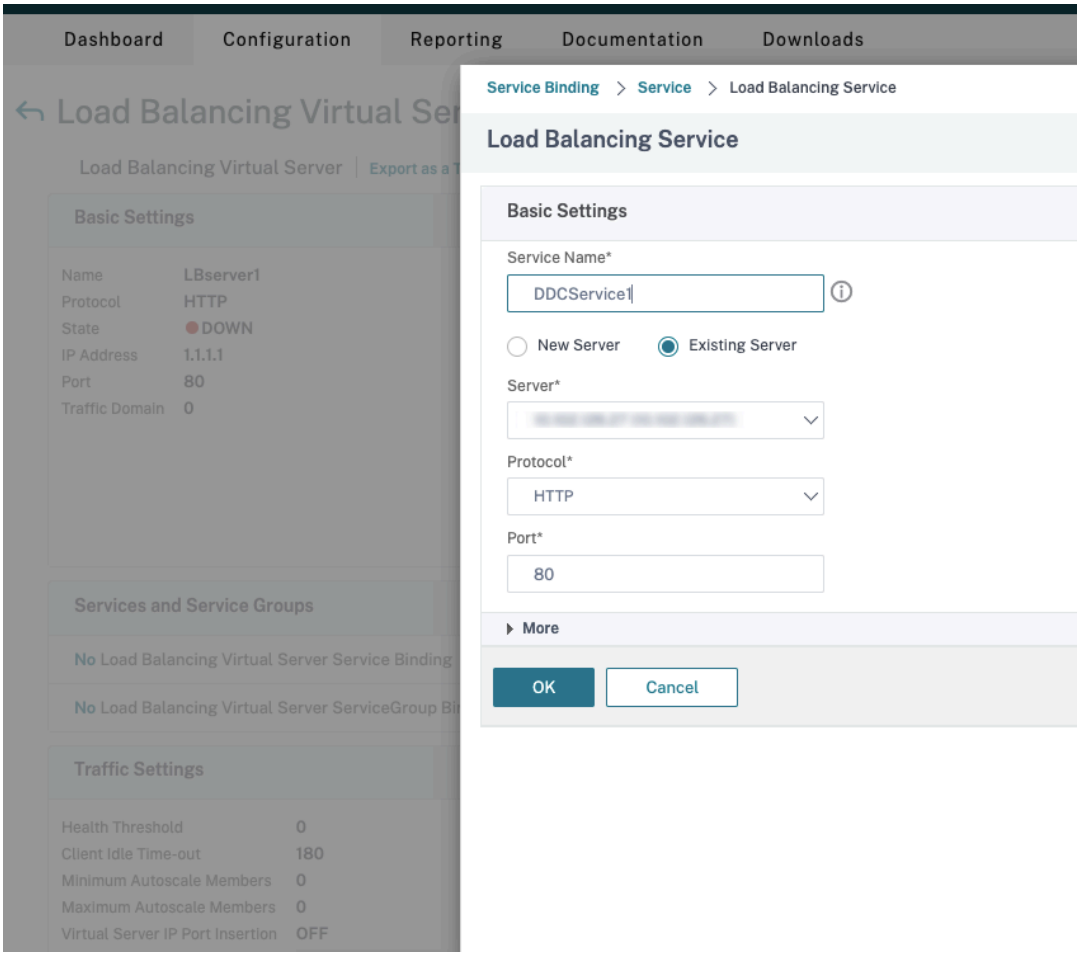
- Gehen Sie zu **Traffic Management > Load Balancing > Services**.



- 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.

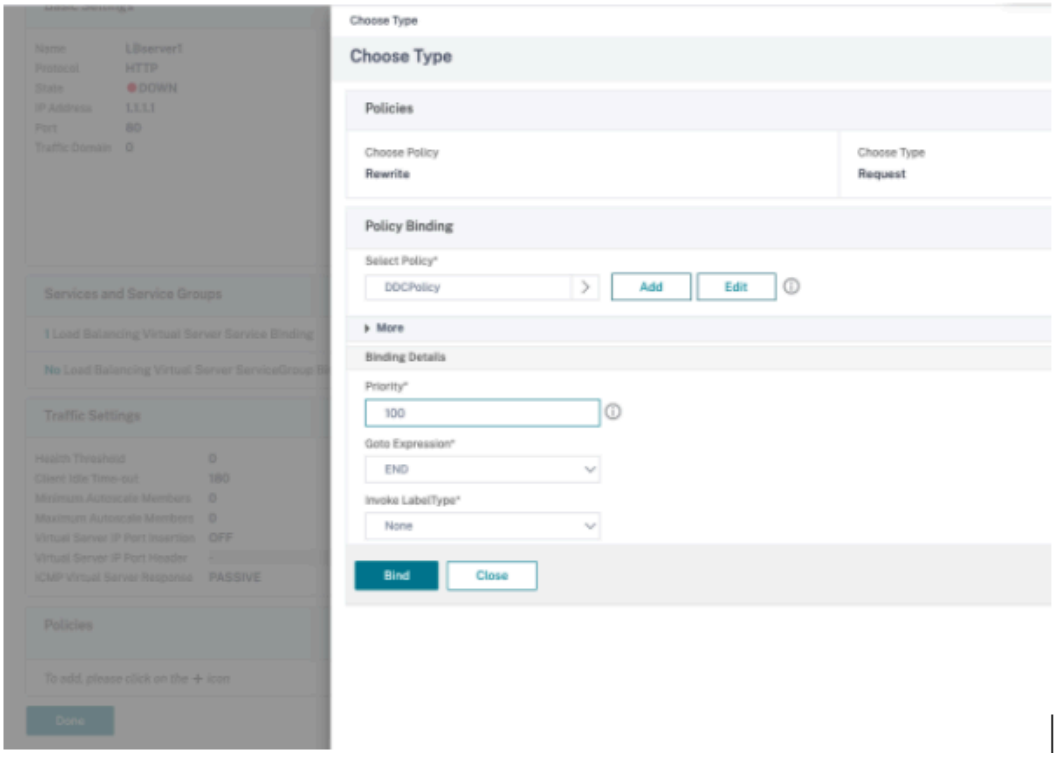
- Wählen Sie den zuvor erstellten virtuellen Server aus und klicken Sie auf **Edit**.
- Klicken Sie in **Services and Service Groups** auf **No Load Balancing Virtual Server Service Group Binding**.



- 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.

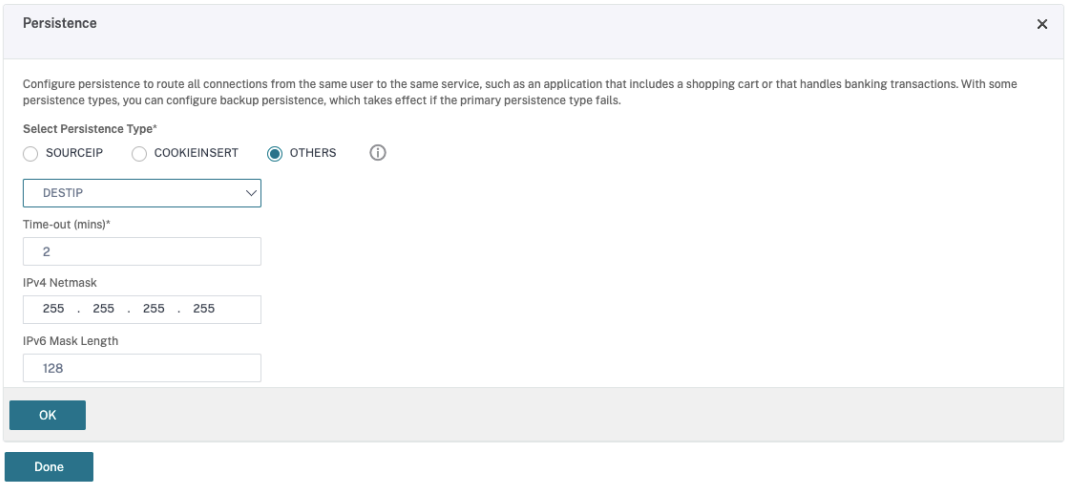
- Wählen Sie den zuvor erstellten virtuellen Server aus und klicken Sie auf **Edit**.
- Klicken Sie unter **Advanced Settings** auf **Policies** und im Bereich **Policies** auf **+**.



- Wählen Sie unter **Choose Policy** die Option **Rewrite** und für **Choose Type**, die Option **Request**.
- Klicken Sie auf **Continue**.
- 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**.

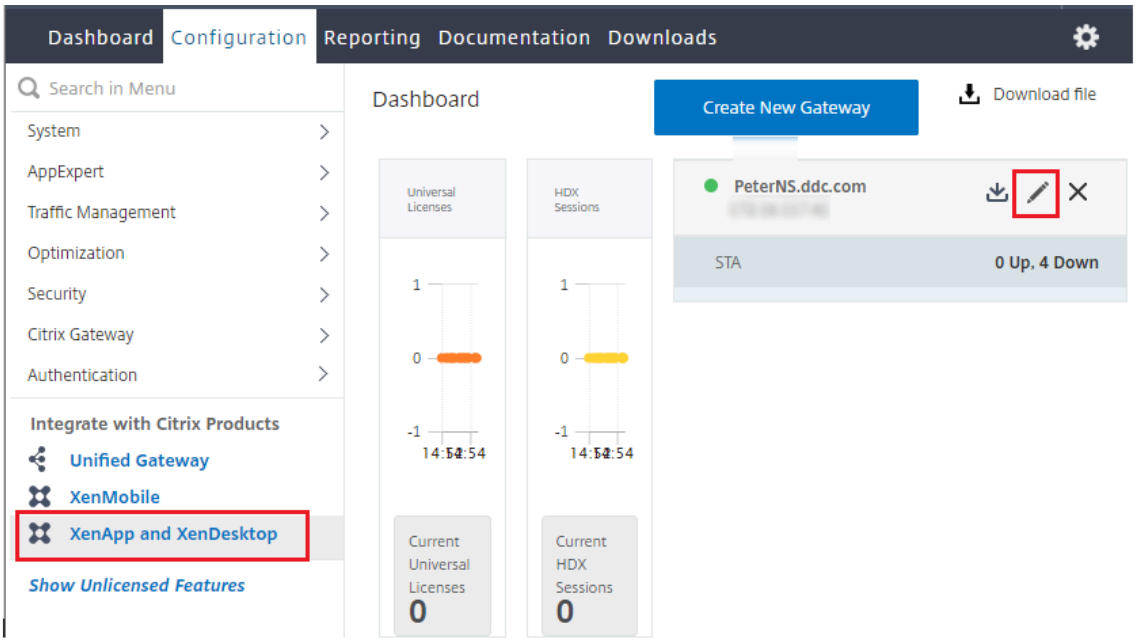
f) Wiederholen Sie diese Schritte für den anderen virtuellen Server.

Konfigurationsänderungen bei bereits mit Citrix Virtual Desktops konfigurierter Citrix ADC Appliance

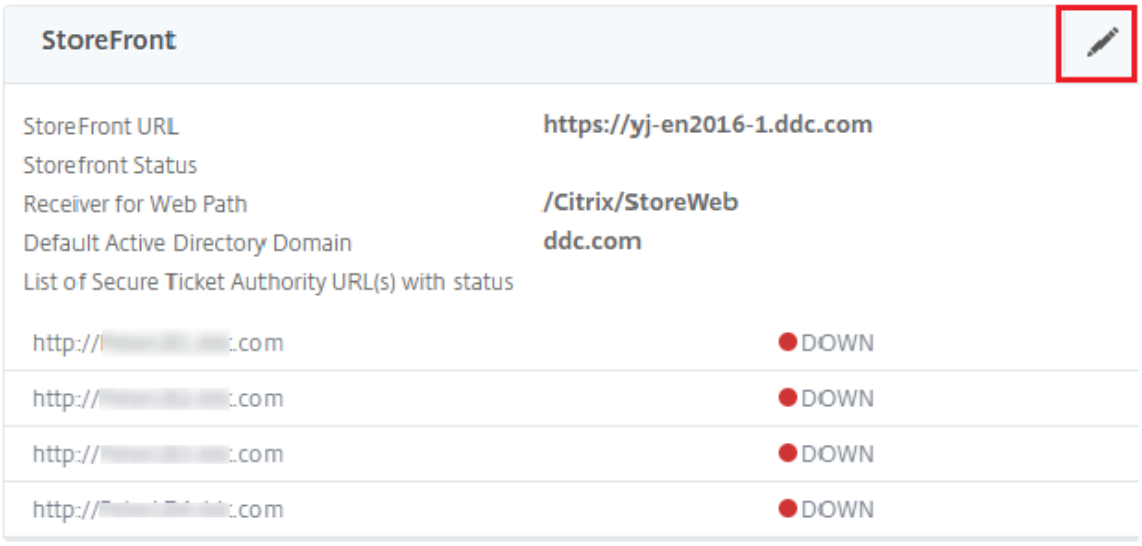
Wenn die Citrix ADC Appliance bereits mit Citrix Virtual Desktops konfiguriert ist, müssen Sie zur Verwendung von Secure XML die folgenden Konfigurationsänderungen vornehmen.

- 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.

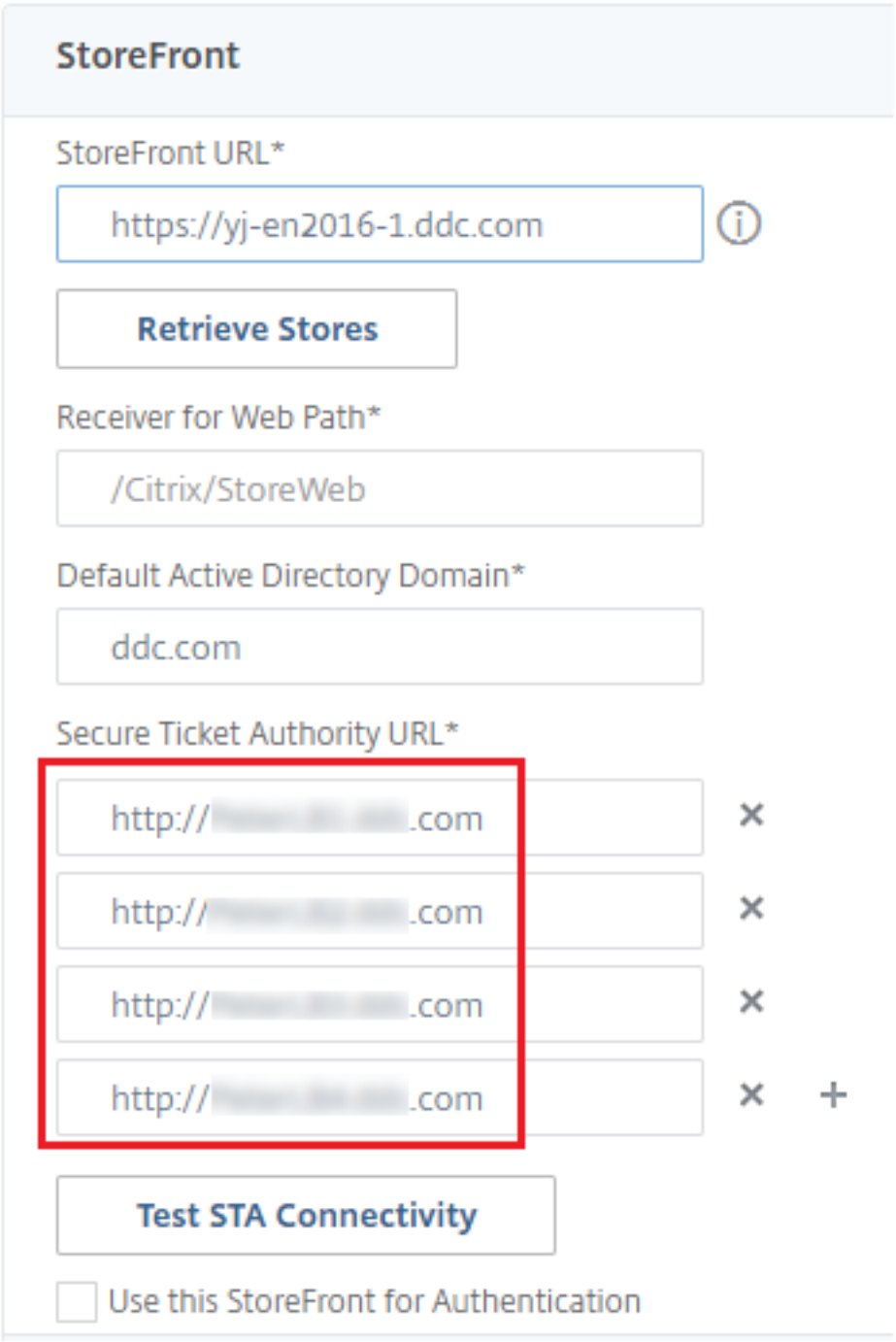


3. Klicken Sie im StoreFront-Bereich auf das Bearbeitungssymbol.



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.



Virtuelle IP und virtuelles Loopback

February 17, 2023

> **Wichtig:**
>
> Windows 10 Enterprise-Multisitzungs-OS unterstützt keine IP-Virtualisierung (virtuelle IP) für Remotedesktops und Citrix unterstützt weder virtuelle IPs noch virtuelles Loopback für Windows 10-Multisitzungs-OS.

Virtuelle IPs und virtuelles Loopback werden auf Windows Server 2016-Maschinen unterstützt. Die Features 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 Citrix Virtual Apps-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 Citrix Virtual Apps-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 2016 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.

- Nachdem eine Adresse einer Sitzung zugewiesen wurde, verwendet die Sitzung bei jedem der folgenden Aufrufe die virtuelle Adresse anstelle der primären IP-Adresse für das System: `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 (z. B. `GetAddrInfo()`, was über eine Windows-Richtlinie gesteuert wird), 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. Weitere Informationen zu Windows-Richtlinien finden Sie unter RDS IP Virtualization in Windows Server.

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

deaktiviert. 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:

- 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
- Name: PreferLoopback, Typ: REG_DWORD, Wert: 1
- Name: PreferLoopbackProcesses, Type: REG_MULTI_SZ, Data: <Liste der Prozesse>

Delivery Controller

September 21, 2021

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. Weitere 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.

Hinzufügen, Entfernen oder Verschieben von Controllern

Um einen Controller hinzuzufügen, zu entfernen oder zu verschieben, benötigen Sie die unter Datenbanken aufgeführten Serverrollen- und Datenbankrollenberechtigungen.

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.

   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

Durch das Entfernen eines Controllers von einer Site werden weder die Citrix Software noch andere Komponenten deinstalliert. Es wird der Controller aus der Datenbank entfernt, sodass er nicht mehr als Verbindungsbroker und zum Ausführen anderer Aufgaben verwendet werden kann. 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. Die Serverrollenberechtigung `securityadmin` ist erforderlich, um die Anmeldung zu entfernen.

> **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 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 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 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 Citrix Provisioning bereitgestellt wurde oder wenn es sich bei ihm um ein bestehendes Image handelt, können Sie ihn in eine andere Site (von Site 1 in Site 2) verschieben, wenn Sie ein Upgrade vornehmen. Sie können auch 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 MCS bereitgestellte VDAs überprüfen immer die ListOfDDCs, die mit der Site verknüpft 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.

Installer Führen Sie das Installationsprogramm aus und fügen Sie einen Controller hinzu, wobei Sie in Site 2 einen vollqualifizierten Domänennamen (DNS-Eintrag) eines Controllers angeben.

Geben Sie Controller im Installationsprogramm nur dann an, wenn die Richtlinieneinstellung "Controller"nicht verwendet wird.

Gruppenrichtlinien-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 empfangene Liste der Controller (weil die automatische Aktualisierung deaktiviert ist). Der VDA 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.

VDA-Registrierung

June 27, 2024

Einführung

VDAs können erst verwendet werden, wenn sie bei mindestens einem Controller oder einem Cloud Connector der Site registriert wurden (Herstellen der Kommunikation). (In lokalen Bereitstellungen von Citrix Virtual Apps and Desktops werden VDAs bei einem Controller registriert. In Citrix Virtual Apps and Desktops 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?

- Die Registrierung ist sicherheitsrelevant. 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 hinzufügen und entfernen und ein VDA keine präzisen und aktuellen Controller-/Cloud Connector-Informationen hat, kann er Sitzungsstarts ablehnen, die von einem nicht aufgelisteten Controller 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.

Zusätzlich zur Liste `ListOfDDCs` enthält die Liste `ListOfSIDs` (Sicherheits-IDs) 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 Citrix Virtual Apps and Desktops 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 ignorieren (oder wenn Sie während der VDA-Installation keine Controller-/Cloud Connector-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.

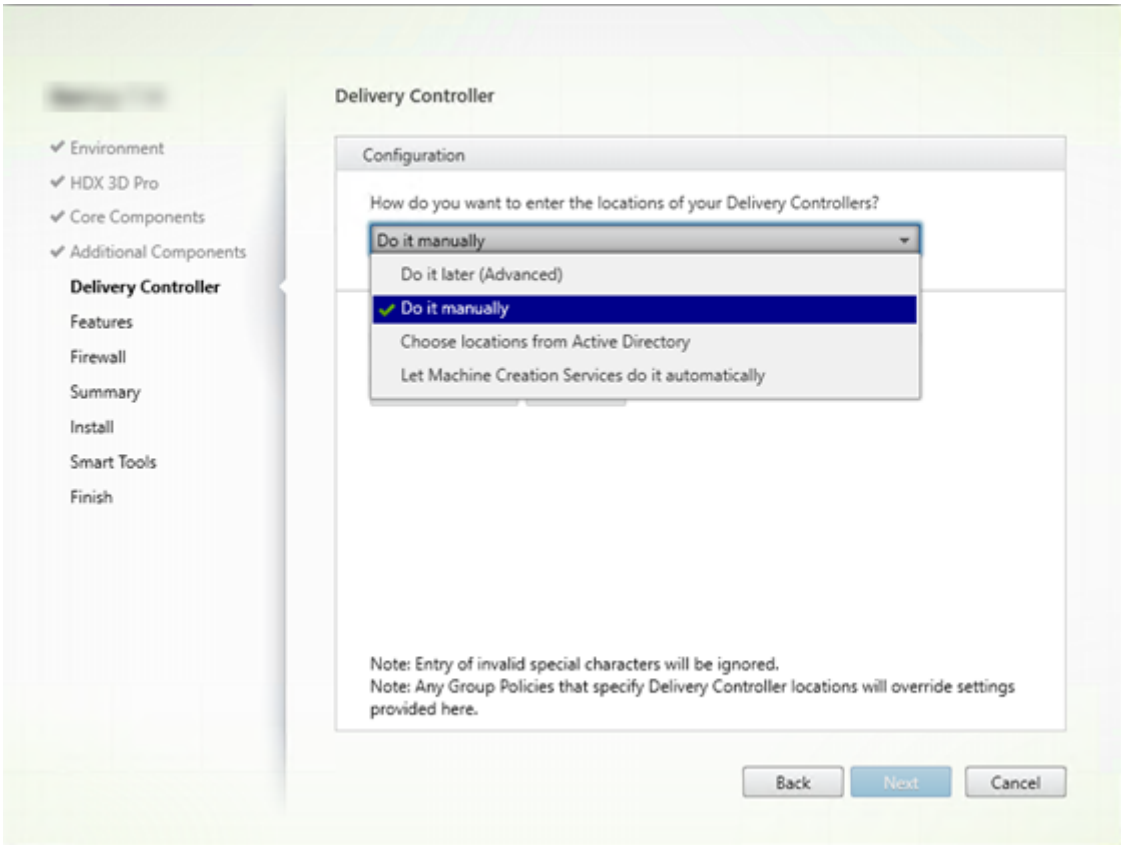
Die einfachste Methode des Abrufs dieser Liste bei späteren Registrierungen ist die Verwendung des Features zur automatischen Aktualisierung. Die automatische Aktualisierung ist standardmäßig aktiviert. Weitere Informationen finden Sie unter Automatische Aktualisierung.

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. Die automatische Aktualisierung hat zwar eigentlich die höchste Priorität, sie wird jedoch erst 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.

Registrierungsbasiert

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 `/controllers` 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 das Registrierungsverzeichnis `HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgen` die Schlüssel `ListOfDDCs` und `FarmGUID` enthält, wird für die Controller- oder Cloud Connector-Discovery `ListOfDDCs` verwendet. `FarmGUID` ist vorhanden, wenn bei der Installation des VDAs die Organisationseinheit der Site 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 Meth-

ode.

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 MCS zur Bereitstellung von VMs verwenden, richtet MCS die Liste der Controller oder Cloud Connectors ein. Dieses Feature wirkt mit der automatischen Aktualisierung zusammen. MCS fügt bei der Katalogerstellung die Controller-/Connectorliste bei der ersten Bereitstellung in die Datei `Personality.ini` ein. Die automatische Aktualisierung bewirkt, dass die Liste immer aktuell bleibt.

Wählen Sie hierfür 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.
- Listen Sie mehrere Controller durch Leerzeichen getrennt im Registrierungsschlüssel "ListOfDDCs"auf, um Registrierungsprobleme bei Ausfall eines Controllers zu vermeiden.

  Beispiel:

`DDC7x.xd.local DDC7xHA.xd.local`

32 Bit: `HKEY_LOCAL_MACHINE \Software\Citrix\VirtualDesktopAgent\ListOfDDCs`

`HKEY_LOCAL_MACHINE \Software\Citrix\VirtualDesktopAgent\ListOfDDCs (REG_SZ)`

- Stellen Sie sicher, dass alle unter `ListOfDDCs` aufgelisteten Einträge auf einen gültigen vollqualifizierten Domänennamen verweisen, um Verzögerungen bei der Registrierung zu vermeiden.

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 `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 Citrix Provisioning erfolgt, außer bei Verwendung eines Citrix Provisioning-Servercache. 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:

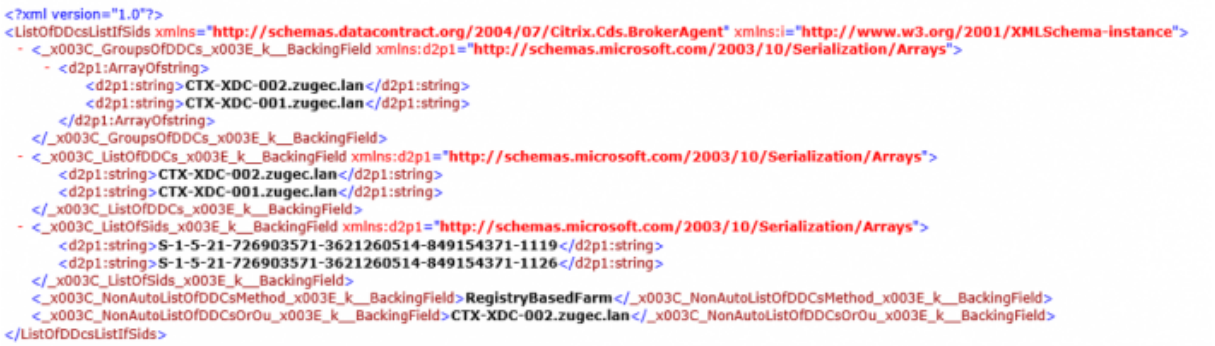
- Bei jeder erneuten Registrierung eines VDAs (z. B. nach einem Neustart der Maschine) wird der Cache aktualisiert. Außerdem überprüft jeder Controller (bzw. Cloud Connector) alle 90 Minuten die Sitedatenbank. Wenn seit der letzten Überprüfung ein Controller hinzugefügt oder entfernt wurde oder bei einer Änderung der Richtlinie, die sich auf die VDA-Registrierung auswirkt, sendet der Controller eine aktualisierte Liste an die bei ihm registrierten VDAs und der Cache wird aktualisiert. Der VDA nimmt alle Verbindungen von allen Controllern 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 wurde aus der Site entfernt), nimmt der VDA eine neue Registrierung bei einem der Controller 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 Backupgruppe 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.

> **Wichtig:**
>
> 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

Berücksichtigen Sie beim Konfigurieren von Elementen, die sich auf die VDA-Registrierung auswirken können, die nachfolgenden Punkte.

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
- Gegenseitige Authentifizierung mit Kerberos

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

In manchen Fällen können Sie Controller bzw. Cloud Connectors in Gruppen zusammenfassen, von denen eine bevorzugt wird und die andere bei Ausfall aller Controller/Connectors für ein Failover verwendet wird. Controller bzw. Cloud Connectors werden zufällig aus der Liste ausgewählt, eine Gruppierung kann daher zur Durchsetzung einer bevorzugten Verwendung helfen.

Die Gruppen sind für die Verwendung innerhalb einer Site (nicht mehrerer Sites) vorgesehen.

Verwenden Sie Klammern, um Controller-/Connectorgruppen anzugeben. Beispiel für vier Controller (zwei primäre und zwei als Backup):

```
(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.

Bei XenDesktop ab Version 7.0 müssen Sie zur Verwendung des Features **Registrierungsgruppen** einen weiteren Schritt ausführen. Sie müssen die Richtlinie **Automatische Aktualisierung von Controllern** in Citrix Studio auf "Nicht zulassen"festlegen.

ListOfSIDs

`ListOfDDCs` ist die Liste der Controller, die ein VDA zur Registrierung ansprechen kann. Ein VDA muss außerdem wissen, welchen Controllern er vertrauen kann. VDAs vertrauen den Controllern auf der `ListOfDDCs` nicht automatisch. 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.

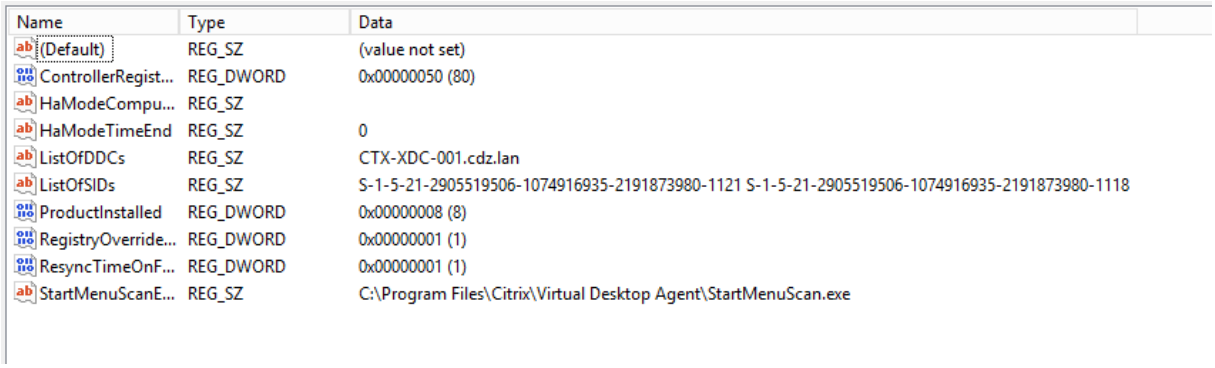
Im Allgemeinen besteht keine Notwendigkeit einer manuellen Änderung der Liste `ListOfSIDs`. Es müssen allerdings einige Ausnahmen berücksichtigt werden. Die ersten beiden Ausnahmen sind nicht mehr relevant, da neuere Technologien zur Verfügung stehen.

- **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 in neueren Umgebungen weder normal noch empfohlen. 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 die Auffüllung 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 unter `HKLM\Software\Citrix\VirtualDesktopAgent` einen Registrierungsschlüssel mit dem Namen `ListOfSIDs (REG_SZ)`. 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 (`List OfSIDs`) 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 zur Fehlerbehebung bei der VDA-Registrierung

- Weitere Informationen zu Funktionsebenen finden Sie unter 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

March 27, 2023

Aufrechterhalten der Sitzungsaktivität ist wichtig für die beste Benutzererfahrung. Eine Unterbrechung der Verbindung aufgrund von unzuverlässigen Netzwerken, stark variierender Netzwerklatenz 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 hier beschriebenen 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.

Sie können Benutzer von einer Sitzung abmelden, Sitzungen trennen und Sitzungsvorabstart sowie Sitzungsfortbestehen konfigurieren. Informationen hierzu finden Sie unter 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 Workspace-App-Benutzer können die Controllereinstellung nicht außer Kraft setzen.

Sie können die Sitzungszuverlässigkeit mit Transport Layer Security (TLS) verwenden. Mit TLS werden nur die Daten verschlüsselt, die zwischen dem Benutzergerät und Citrix 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 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 die Citrix Workspace-App 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 die Citrix Workspace-App, die Verbindung mit der Sitzung wiederherzustellen, bis die Wiederverbindung erfolgreich war oder der Benutzer die Wiederverbindung abbricht.

Bei Desktopsitzungen versucht die Citrix Workspace-App 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 derselben Citrix Workspace-App, nachdem 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 die Citrix Workspace-App. Diese übermittelt den Schlüssel zur Wiederverbindung 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 die Citrix Workspace-App 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 der Citrix Workspace-App für Windows über die Datei icaclient.adm. Weitere Informationen finden Sie in der Dokumentation zu Ihrer Version der Citrix Workspace-App 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 die Citrix Workspace-App 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 die Citrix Workspace-App 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.

> **Wichtig:**
>
> 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 inaktive 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 der Citrix Workspace-App 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.

Sitzungsroaming konfigurieren

Zum Konfigurieren des Sitzungsroamings verwenden Sie die folgenden Anspruchsrichtlinienregel-Cmdlets mit der Eigenschaft "SessionReconnection". Optional können Sie auch die Eigenschaft "LeasingBehavior"angeben.

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.

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.

Diese Einstellung gilt nur für VMs mit Desktop-VDAs. Microsoft steuert das Anmeldetimeout auf Maschinen mit Server-VDAs.

Verwenden der Suche in Studio

February 6, 2020

Verwenden Sie die Suchfunktion, um bestimmte Maschinen, Sitzungen, Maschinenkataloge, Anwendungen oder Bereitstellungsgruppen zu finden.

1. Wählen Sie im Studio-Navigationsbereich **Suchen** aus.

Sie können über das Suchfeld keine Suche auf den Registerkarten "Maschinenkataloge"oder "Bereitstellungsgruppen"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.

Klicken Sie alternativ auf das Symbol **Suche erweitern** (zwei nach unten weisende spitze Klammern), um ein Menü mit Sucheigenschaften anzuzeigen. Sie können eine erweiterte Suche unter Erstellung eines Ausdrucks mit den Eigenschaften im Menü durchführen.

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

September 21, 2021

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 weiterer 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.

- 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 Verwalten von Bereitstellungsgruppen.

- Zielgerichtete Anwendung (Zuweisung) von Citrix Richtlinien auf 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** dieses Tag und das Kontrollkästchen **Aktivieren**. Sie können auch einer Bereitstellungsgruppe ein Tag hinzufügen und eine Citrix Richtlinie auf die Gruppe anwenden. Einzelheiten finden Sie unter Erstellen von Richtlinien.

Sie können Tags auf Folgendes anwenden:

- Maschinen
- Anwendungen
- Maschinenkataloge (nur PowerShell; siehe Tags für Maschinenkataloge)
- 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

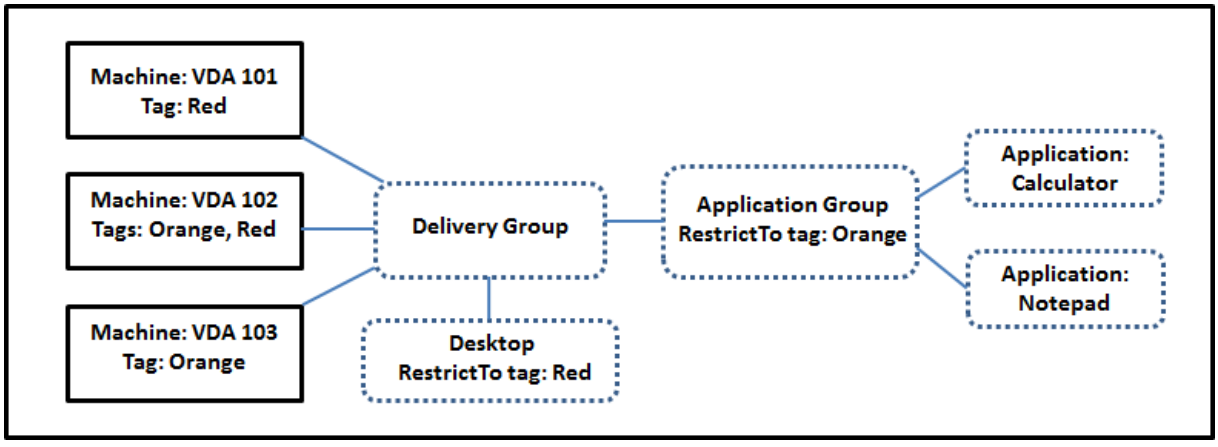
Das Erstellen von Tagbeschränkungen umfasst mehrere Schritte:

- 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: einfache Anordnung

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.

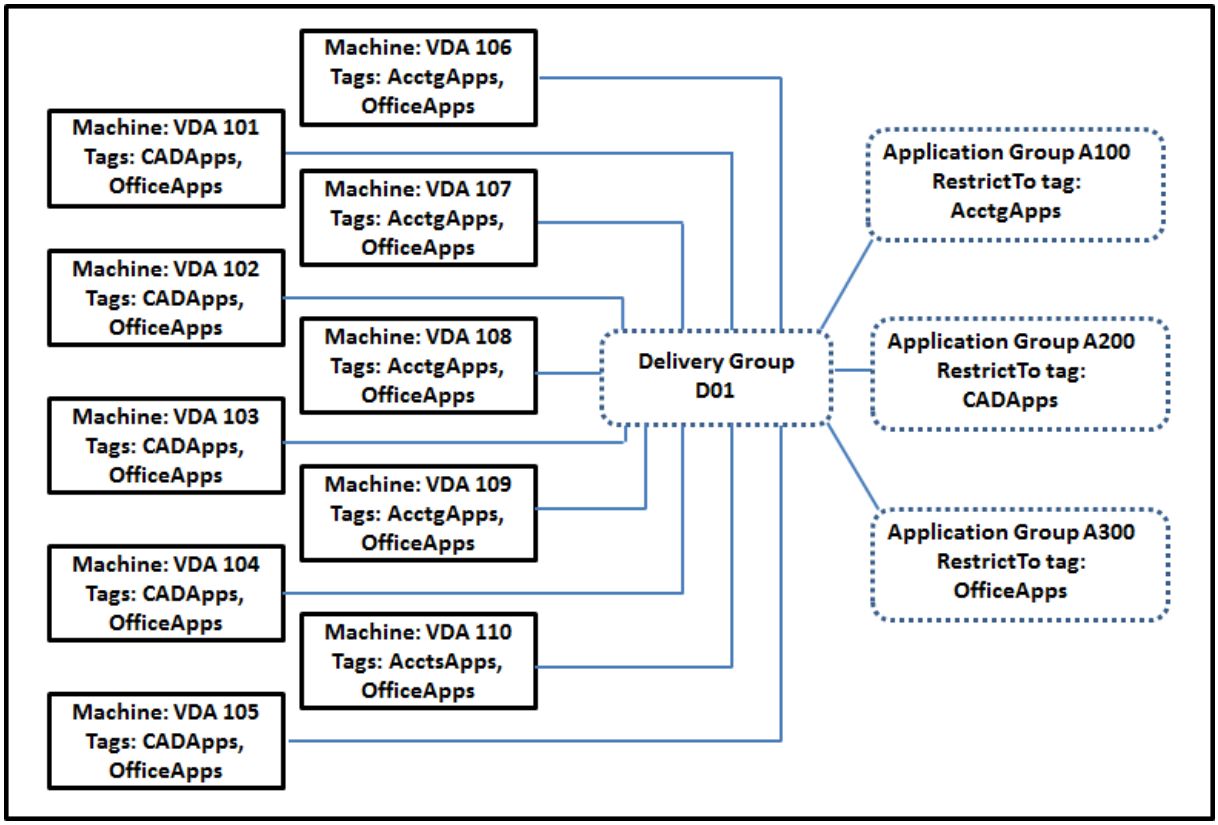
- Die Anwendungsgruppe wurde mit der Tagbeschränkung `Orange` erstellt, sodass alle ihre Anwendungen (Rechner und Editor) nur auf Maschinen gestartet werden können, die das Tag `Orange` haben: VDA 102 und 103.

Maschine VDA 102 hat beide Tags (`Red` und `Orange`) und kann daher für das Starten von Anwendungen und Desktops verwendet werden.

Beispiel 2: komplexere Anordnung

Dieses Beispiel enthält mehrere Anwendungsgruppen mit Tagbeschränkungen. Auf diese Weise können mehr Anwendungen mit weniger Maschinen als bei bloßer Verwendung von Bereitstellungsgruppen bereitgestellt werden.

Unter 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 10 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 10 Maschinen (VDA 101–110) zugreifen.

Es werden nur 10 Maschine mit nur einer 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.

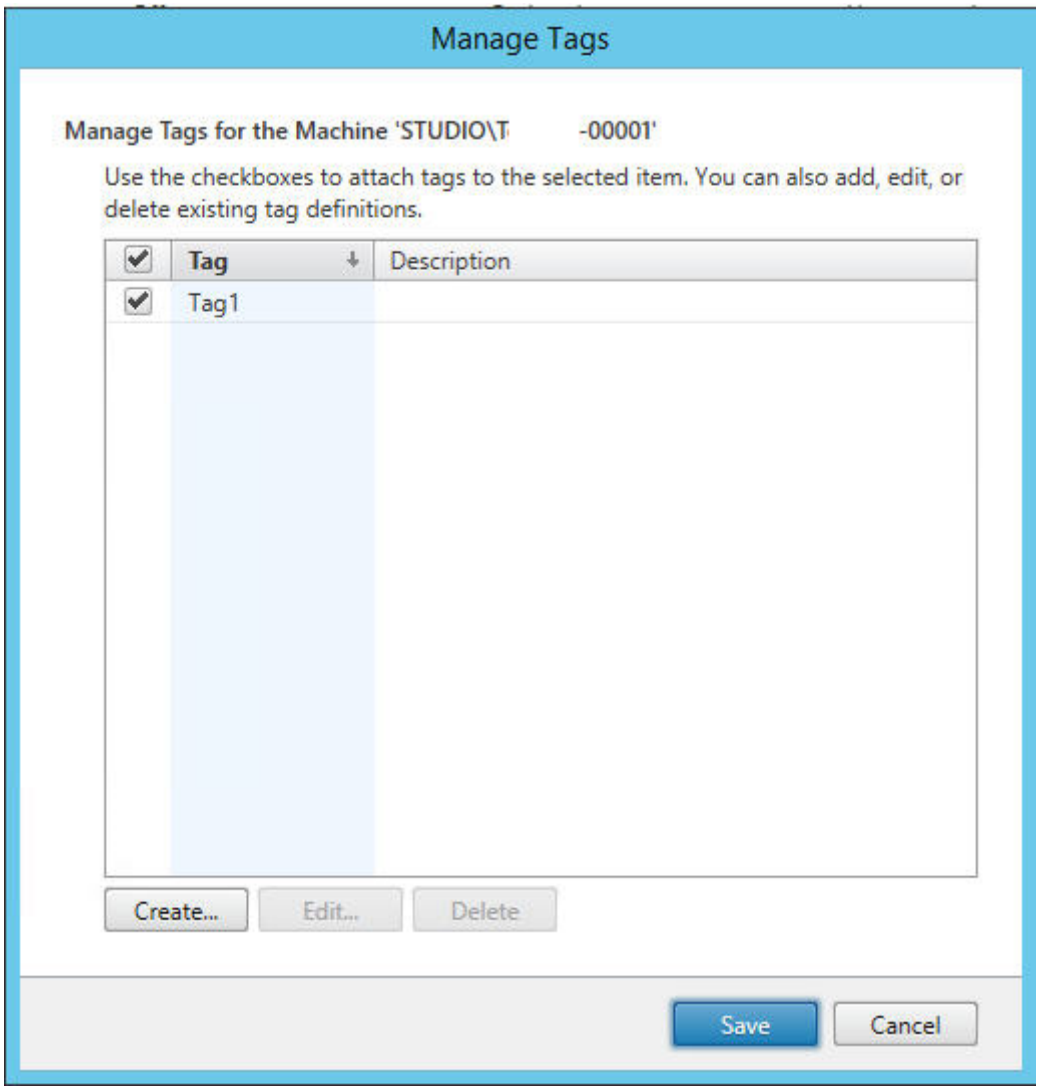
(Ausnahme: Tags für Richtlinienzuweisungen werden über die Aktion **Tags verwalten** in Studio erstellt, bearbeitet und gelöscht. Die Tags werden jedoch beim Erstellen der Richtlinie angewendet (zugewiesen). Weitere Informationen finden Sie unter Erstellen von Richtlinien.)

Tagbeschränkungen konfigurieren Sie beim Erstellen oder Bearbeiten von Desktops in Bereitstellungsgruppen und beim Erstellen und Bearbeiten von Anwendungsgruppen.

Verwenden der Dialogfelder “Tags verwalten”in Studio

Wählen Sie in Studio die Elemente aus, auf die Sie ein Tag anwenden möchten (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. Konsultieren Sie den Artikel Hinweise zum Arbeiten mit Tags.

- **Erstellen von Tags:**

  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. 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 Maschinen hinzuzufügen, werden Sie in Studio gewarnt, dass die Maschinen dadurch evtl. für Starts verfügbar gemacht werden. Wenn dies beabsichtigt ist, fahren Sie fort.

- **Entfernen von Tags:**

  Deaktivieren Sie die Kontrollkästchen neben den entsprechenden Tagnamen. Ein Strich im Kontrollkästchen zeigt an, wenn das Tag auf einige (aber nicht alle) ausgewählten Elemente angewendet wurde. Wenn Sie mehrere Elemente ausgewählt haben und das Kontrollkästchen eines Tags einen Strich enthält, wird bei Deaktivieren des Kontrollkästchens das Tag von allen ausgewählten Maschinen entfernt.

  Wenn Sie versuchen, ein Tag von einer Maschine zu entfernen, für die es als Einschränkung verwendet wird, werden Sie in Studio gewarnt, 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**. Geben Sie einen neuen Namen und/oder eine Beschreibung ein. 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. Bearbeiten Sie zuerst die Anwendungsgruppe entfernen Sie und die Tagbeschränkung oder wählen Sie ein anderes Tag.

Wenn Sie im Dialogfeld **Tags verwalten** fertig sind, klicken Sie auf **Speichern**.

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 Details die Registerkarte Tags.

Verwalten von Tagbeschränkungen

Das Verfahren zum Konfigurieren von Tagbeschränkungen besteht aus mehreren Schritten. Zunächst erstellen Sie 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"die Option **Starts auf Maschinen mit Tag beschränken** und dann aus der Liste das Tag.

- **Tagbeschränkung für eine Anwendungsgruppe ändern/entfernen:**

  Bearbeiten Sie die Gruppe. Wählen Sie auf der Seite "Bereitstellungsgruppen"ein anderes Tag aus der Liste oder entfernen Sie die Tagbeschränkung 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 im Dialogfeld "Desktop hinzufügen"die Option **Starts auf Maschinen mit Tag beschränken** und dann aus dem Menü 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 Liste oder entfernen Sie die Tagbeschränkung durch Deaktivieren der Option **Starts auf Maschinen mit Tag beschränken**.

Hinweise zum Arbeiten mit Tags

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 für eine Anwendungsgruppe oder einen Desktop als Einschränkung verwenden. Dadurch wird die Startauswahl auf Maschinen in den Bereitstellungsgruppen beschränkt, die das Tag haben.

Wenn Sie versuchen, Maschinen ein Tag hinzuzufügen, das als Tagbeschränkung für eine Desktop- oder Anwendungsgruppe verwendet wird, wird in Studio eine Warnung angezeigt. Durch das Hinzufügen des Tags stehen die Maschinen möglicherweise zum Starten zusätzlicher Anwendungen oder Desktops zur Verfügung. Wenn dies beabsichtigt ist, fahren Sie fort. Fall nicht, brechen Sie den Vorgang ab.

Angenommen, Sie erstellen eine Anwendungsgruppe mit der Tagbeschränkung `Red"`. Später fügen Sie der von der Anwendungsgruppe verwendeten Bereitstellungsgruppe mehrere Maschinen hinzu. Wenn Sie versuchen, das Tag `Red` 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.

Konfigurieren von Beispiel 2

Nachfolgend wird erläutert, wie die im zweiten Beispiel 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**. Erstellen Sie ein Tag namens `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. 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**. Erstellen Sie ein Tag namens `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. Schließen Sie das Dialogfeld.

Anwendungsgruppen mit Tagbeschränkungen erstellen

1. Wählen Sie im Studio-Navigationsbereich **Anwendungen** und im Aktionsbereich **Anwendungsgruppe erstellen**.
2. Wählen Sie auf der Seite **Bereitstellungsgruppen** Bereitstellungsgruppe `D01` aus. Wählen Sie **Starts auf Maschinen mit Tag beschränken**. Wählen Sie dann das Tag `AcctgApps` in der Liste 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.

Tags für Maschinenkataloge

Sie können Tags für Maschinenkataloge verwenden. Das Verfahren zum Erstellen eines Tags und der anschließenden Anwendung auf einen Katalog entspricht im Wesentlichen dem zuvor beschriebenen. Das Anwenden von Tags auf Kataloge wird jedoch nur über die PowerShell-Schnittstelle unterstützt. Mit Studio können Sie weder Tags auf einen Katalog anwenden noch aus einem Katalog entfernen. Die Kataloganzeigen in Studio lassen nicht erkennen, ob ein Tag angewendet wurde.

Zusammenfassung: Sie können Studio oder PowerShell verwenden, um ein Tag für einen Katalog zu erstellen oder zu löschen. Verwenden Sie PowerShell, um das Tag auf den Katalog anzuwenden.

Beispiele für die Verwendung von Tags für Kataloge:

- Eine Bereitstellungsgruppe umfasst Maschinen aus mehreren Katalogen, aber Sie möchten einen Vorgang (z. B. einen Neustartzeitplan) nur auf Maschinen eines bestimmten Katalogs anwenden. Das erreichen Sie durch Anwenden eines Tags auf diesen Katalog.
- In einer Anwendungsgruppe möchten Sie Anwendungssitzungen auf Maschinen in einem bestimmten Katalog beschränken. Das erreichen Sie durch Anwenden eines Tags auf diesen Katalog.

Involvierte PowerShell-Cmdlets:

- Sie können Katalogobjekte an Cmdlets wie `Add-BrokerTag` und `Remove-BrokerTag` übergeben.
- `Get-BrokerTagUsage` zeigt an, wie viele Kataloge Tags enthalten.
- `Get-BrokerCatalog` hat die Eigenschaft `Tags`.

Die folgenden Cmdlets fügen beispielsweise dem Katalog `acctg` ein Tag namens `fy2018` hinzu: `Get-BrokerCatalog -Name acctg | Add-BrokerTag fy2018`. (Das Tag wurde zuvor mit Studio oder PowerShell erstellt.)

Anleitungen und Informationen zur Syntax finden Sie in der Hilfe zu PowerShell-Cmdlets.

Weitere Informationen

Blogbeitrag: How to assign desktops to specific servers.

Unterstützung für IPv4/IPv6

January 8, 2021

Dieses Release unterstützt reines IPv4, reines IPv6 und Bereitstellungen mit dualem Stapel, bei denen überlappende IPv4- und IPv6-Netzwerke verwendet werden.

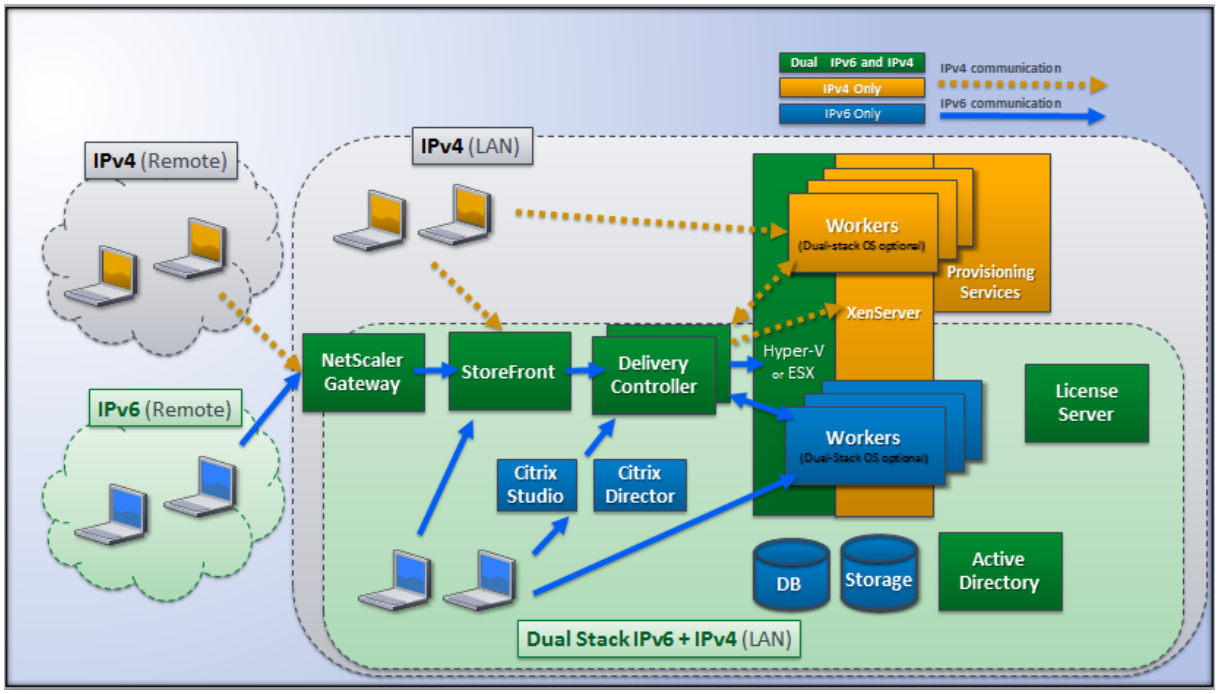
Die IPv6-Kommunikation wird mit zwei verbindungsspezifischen Citrix Richtlinieneinstellungen für Virtual Delivery Agent (VDA) gesteuert:

- 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:

- Citrix Provisioning
- XenServer

- Nicht über die Richtlinieneinstellung **Nur IPv6-Controllerregistrierung verwenden** gesteuerte VDAs
- XenApp-Versionen vor 7.5, XenDesktop-Versionen vor 7 und Director

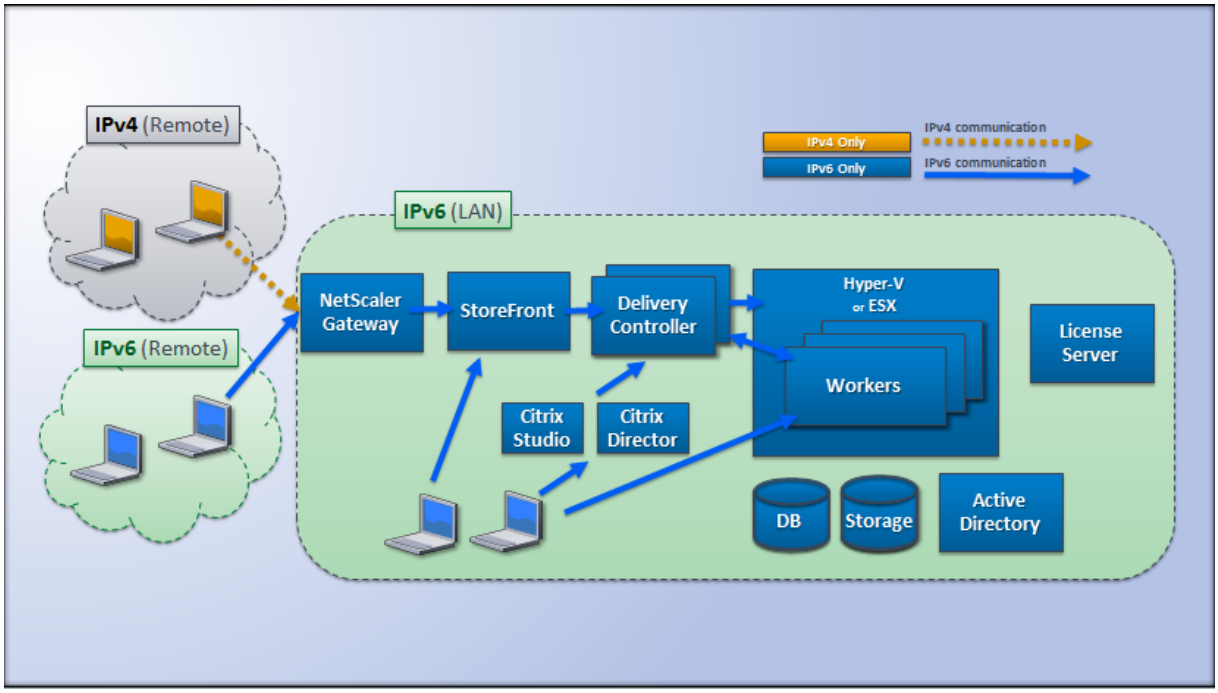
In dieser Bereitstellung gilt:

- 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

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

May 3, 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 Citrix Virtual Apps and Desktops-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 Citrix Virtual Apps and Desktops-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. Citrix Virtual Apps and Desktops-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 Citrix Virtual Apps and Desktops-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 Citrix Provisioning oder 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:

- **Persistent und dediziert:** Beispiele sind Maschinen mit Einzelsitzungs-OS mit statischen 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
- **Persistent und freigegeben:** Beispiele sind Maschinen mit Multisitzungs-OS, die mit den Maschinenerstellungsdiensten erstellt wurden.
- **Bereitgestellt und dediziert:** Beispiele sind Maschinen mit Einzelsitzungs-OS mit statischen Zuweisungen, aber ohne persönliche vDisk, die mit Citrix Provisioning erstellt wurden
- **Bereitgestellt und freigegeben:** Beispiele sind Maschinen mit Einzelsitzungs-OS mit zufälliger Zuweisung, die mit Citrix Provisioning 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 Citrix Virtual Apps-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 Citrix Virtual Apps and Desktops-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.

Konfigurieren Sie die Ordnerumleitung entweder mit den Citrix Richtlinien oder den Active Directory-Gruppenrichtlinienobjekten, jedoch nicht mit beidem. 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 Betrieb-

ssystem 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
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.

Aufzeichnen einer Citrix Diagnostic Facility (CDF)-Trace beim Systemstart

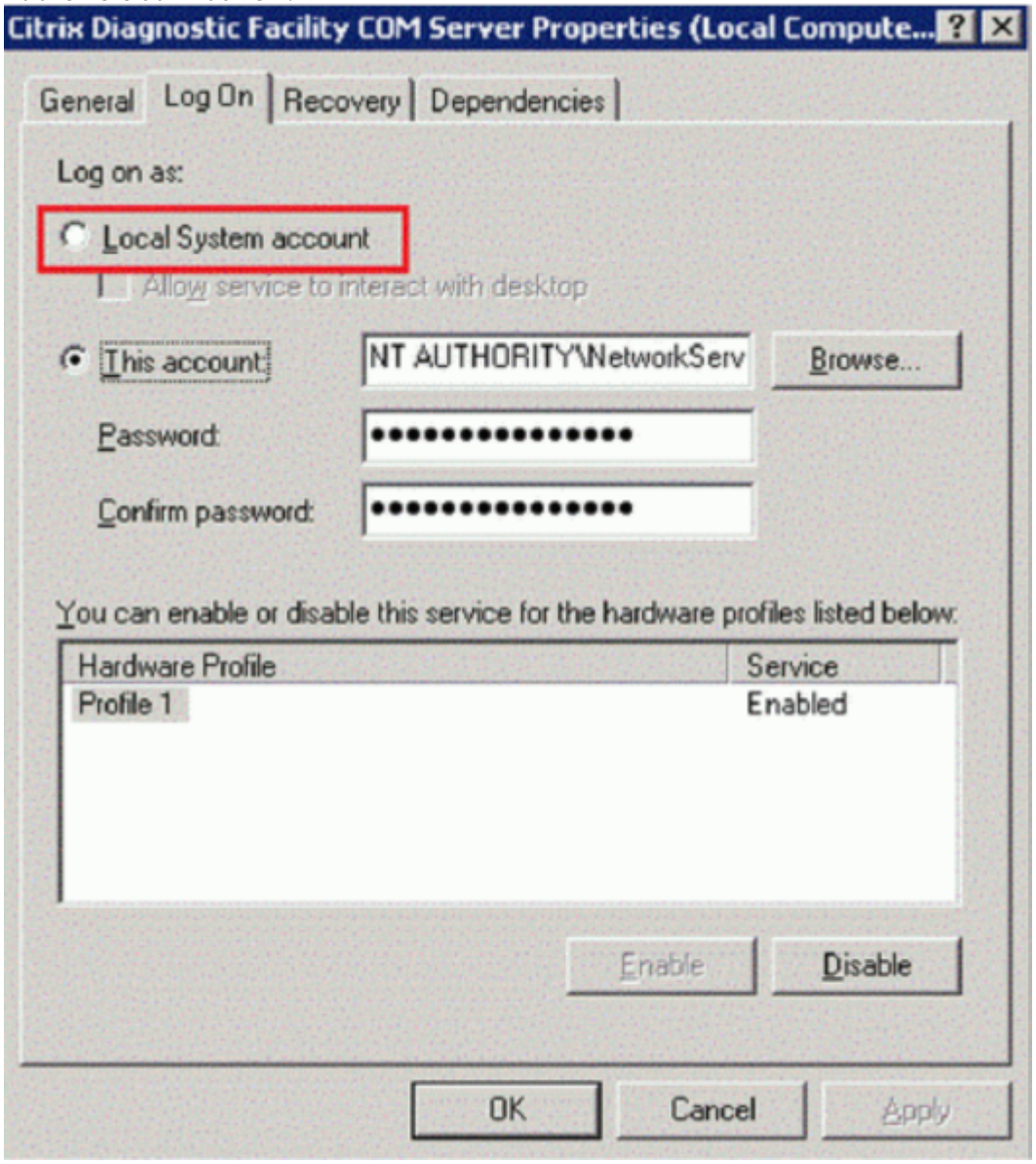
September 21, 2021

Das Hilfsprogramm CDFControl ist ein Ablaufverfolgungscontroller zum Erfassen der CDF-Meldungen der verschiedenen Citrix Ablaufverfolgungsanbieter. Es wurde entwickelt, um komplexe Probleme mit Citrix Systemen zu beheben, die Filterunterstützung zu analysieren und Leistungsdaten zu erfassen. Informationen zum Download von CDFControl finden Sie unter CTX111961.

Verwenden des lokalen Systemkontos

Zum Verwenden des lokalen Systemkontos für den CDF-COM-Serverdienst führen Sie die folgenden Schritte aus:

1. Klicken Sie im **Startmenü** auf **Ausführen**.
2. Geben Sie im Dialogfeld `services.msc` ein und klicken Sie auf **OK**.
3. Wählen Sie den Dienst **Citrix Diagnostics Facility COM Server** und klicken Sie auf **Eigenschaften**.
4. Klicken Sie auf die Registerkarte **Anmelden** und aktivieren Sie das **lokale Systemkonto**. Klicken Sie dann auf **OK**.

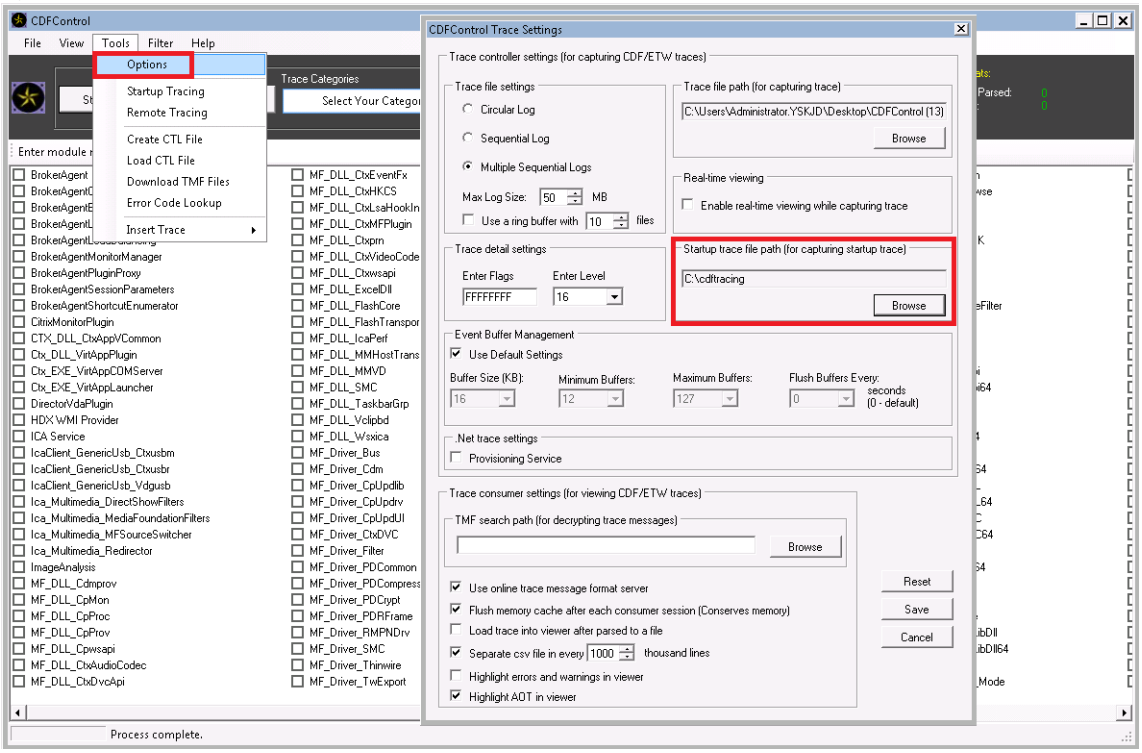


5. Starten Sie den Dienst neu.

Aufzeichnen einer Trace beim Systemstart

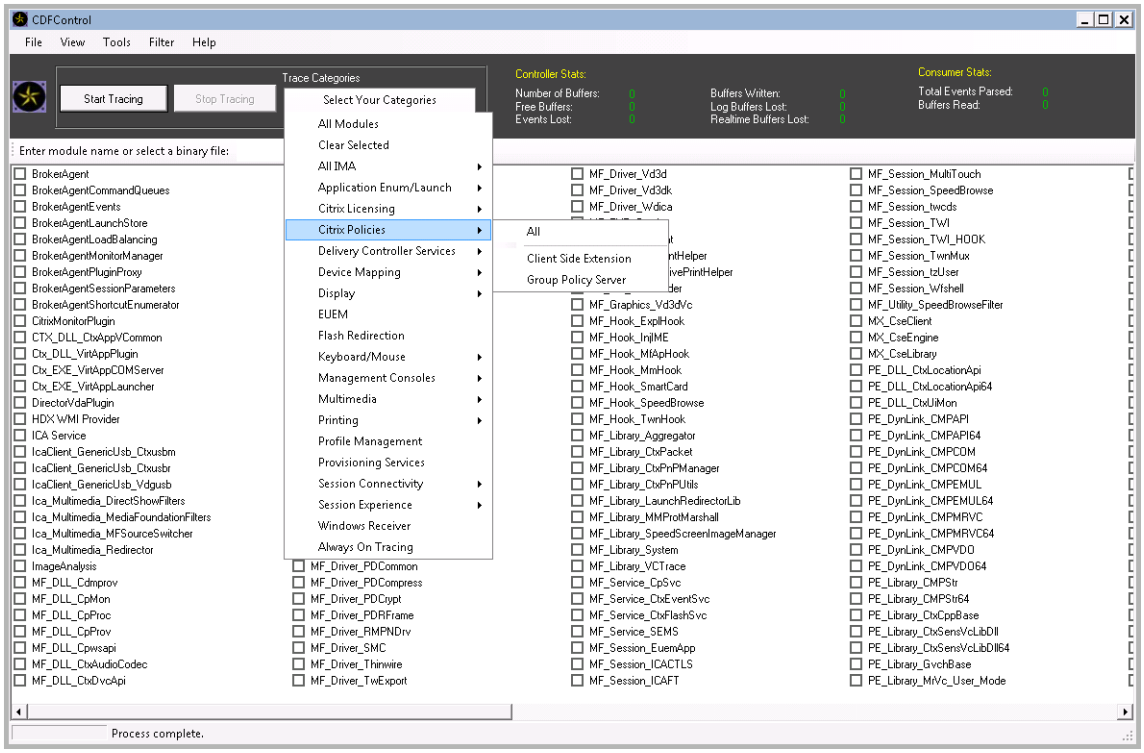
Zum Aufzeichnen einer Trace beim Systemstart führen Sie folgende Schritte aus:

1. Starten Sie **CDFControl** und wählen Sie **Options** im Menü **Tools**.
2. Geben Sie im Abschnitt **Startup trace file path for capturing startup trace** den Pfad für die Systemstart-Tracedatei ein. Klicken Sie auf **Speichern**.



3. Wählen Sie unter **Trace Categories** die vom technischen Support von Citrix empfohlenen Kategorien. In diesem Beispiel wird **Citrix Richtlinien** ausgewählt.

   Die Auswahl **Citrix Richtlinien** wird nur als Beispiel für die Systemstart-Ablaufverfolgung angezeigt. Citrix empfiehlt, dass Sie die Anbieter für das spezifische Problem aktivieren, das Sie beheben möchten.



4. Wählen Sie als Administrator **Startup Tracing** und klicken Sie auf **Enable** im Menü **Tools**.

   Nach Auswahl von **Enable** beginnt die Leiste zu scrollen. Dies hat keinen Einfluss auf das Verfahren. Fahren Sie mit Schritt 5 fort.

5. Schließen Sie das Hilfsprogramm **CDFControl** und starten Sie das System neu, nachdem **Startup Tracing** aktiviert wurde.

6. Starten Sie das Hilfsprogramm **CDFControl**. Nachdem das System neu gestartet wurde und der Fehler angezeigt wird, deaktivieren Sie die Option **Startup Tracing** durch Auswahl von **Disable**.

   Deaktivieren Sie **Startup Tracing** durch Auswahl von “Startup Tracing”im Menü **Tools** und Klicken auf **Disable** (siehe Schritt 4 und 5).

7. Halten Sie den Serverdienst **Citrix Diagnostics Facility COM** an.

8. Erfassen Sie eine Tracedatei (.etl) zur Analyse im angegebenen Dateipfad unter Durchführung von Schritt 1 und 2.

9. Starten Sie den Serverdienst **Citrix Diagnostics Facility COM**.

Citrix Insight Services

May 24, 2024

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 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.cloud.com/privacy-policy

Dieses Release von Citrix Virtual Apps and Desktops unterstützt die nachfolgend aufgeführten Technologien.

- Analyse für Installationen und Upgrades von Citrix Virtual Apps and Desktops
- Citrix-Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP)
- Citrix Call Home
- Citrix Scout

Zusätzlich zu CIS und Citrix Analytics-Daten werden Google Analytics-Daten bei der Installation (oder dem Upgrade) von Studio automatisch und separat erfasst und später hochgeladen. Nach der Installation von Studio können Sie diese Einstellung über den Registrierungsschlüssel "HKLM\Software\Citrix\DesktopStudio\GAEnabled"ändern. Der Wert 1 ermöglicht Sammeln und Upload, 0 deaktiviert Sammeln und Upload.

Analysedaten zu Installationen und Upgrades

Wenn Sie mit dem Produktinstallationsprogramm Citrix Virtual Apps and Desktops-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.

Steuern automatischer Uploads:

- Registrierungseinstellung zur Steuerung des automatischen Uploads von Installations-/Upgradeanalysedaten (Standard = 1):
  - Ort: HKLM:\Software\Citrix\MetaInstall
  - Name: SendExperienceMetrics
  - Wert: 0 = deaktiviert , 1 = aktiviert
- Das folgende PowerShell-Cmdlet deaktiviert den automatischen Upload von Installations-/Upgradeanalysedaten:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\MetaInstall -Name
    SendExperienceMetrics -PropertyType DWORD -Value 0
<!--NeedCopy-->
```

- 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

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 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 dem Erstellen der Site jederzeit beenden. Wählen Sie im Studio-Navigationsbereich den Knoten **Konfiguration**, anschließend die Registerkarte **Produktsupport** und folgen Sie den Anweisungen.

Beim Upgrade einer Citrix Virtual Apps and Desktops-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):

Ort: HKLM: \Software\Citrix\Telemetry\CEIP
Name: Enabled
Wert: 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:

```
1 New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\Telemetry\CEIP -Name
     Enabled -PropertyType DWORD -Value 0
2 <!--NeedCopy-->
```

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. Citrix Provisioning, AppDNA, Citrix Lizenzserver, die Citrix Workspace-App für Windows, den universellen Druckserver und die Sitzungsaufzeichnung. Standardwerte für die Installation und Teilnahme finden Sie in der Dokumentation dieser Komponenten.

Citrix Call Home

Wenn Sie bestimmte Komponenten und Features in Citrix Virtual Apps and Desktops 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 Citrix Virtual Apps and Desktops 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. AOT-Protokolle werden im Ordner C:\Users\CitrixTelemetryService\Appdata\Local\CitrixAOT gespeichert.

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.:

- Von Citrix Virtual Apps and Desktops unter `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix` erstellte Registrierungseinträge
- Informationen zu Windows Management Instrumentation (WMI) unter dem Citrix Namespace.
- Liste der aktuellen Prozesse
- Absturzabbilder von Citrix Prozessen, die unter %PROGRAM DATA%\Citrix\CDF gespeichert wurden
- Informationen zu Installation und Upgrade. Diese können das Protokoll des Metainstallers für das vollständige Produkt, Protokolle über MSI-Fehler, die Ausgabe der MSI-Protokollanalyse, StoreFront-Protokolle, Protokolle der Lizenzkompatibilitätsprüfung und Ergebnisse vorläufiger Site-Upgradetests umfassen.

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.

Wenn Sie Call Home bei Installation einer Komponente aktivieren, können Sie es später deaktivieren.

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 Telemetriedienstes 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 möchten. Es gibt drei Optionen:

Wenn Sie einen Controller installieren, können Sie Informationen nicht mehr über die Call Home-Seite des Installationsassistenten konfigurieren, wenn auf den Server ein Active Directory-Gruppenrichtlinienobjekt mit der Richtlinieneinstellung "Als Dienst anmelden"angewendet wurde. Weitere Informationen finden Sie unter CTX218094.

Wenn Sie einen Controller aktualisieren und bereits bei Call Home registriert sind, werden Sie nicht gefragt, ob teilnehmen möchten.

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:** Diagnosedaten werden automatisch an Citrix hochgeladen. Wenn Sie keine zusätzlichen Cmdlets für einen benutzerdefinierten Zeitplan eingeben, wird der Standardzeitplan verwendet.

  ```
  1  $cred = Get-Credential
  2  Enable-CitrixCallHome -Credential $cred
  3  <!--NeedCopy-->
  ```

  Um sicherzustellen, dass geplante Uploads aktiviert sind, geben Sie `Get-CitrixCallHomeGet -CitrixCallHome` ein. Wenn die Option aktiviert ist, wird `IsEnabled=True` und `IsMasterImage=False` zurückgegeben.

- **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. Wenn die Option aktiviert ist, wird `IsEnabled=True` und `IsMasterImage=True` zurückgegeben.

- **Erstellen eines benutzerdefinierten Zeitplans:** Es kann ein Zeitplan für die tägliche oder wöchentliche Erfassung und Übermittlung von Diagnosedaten erstellt werden.

```
1  $timespan = New-TimeSpan –Hours hours -Minutes minutes
2  Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek day
       -UploadFrequency {
3  Daily|Weekly }
4
5  <!--NeedCopy-->
```

Beispiele:

Das folgende Cmdlet erstellt einen Zeitplan, nach dem Datenpakete jeden Abend um 22:20 Uhr erstellt und hochgeladen werden. Der Parameter für Stunden verwendet das 24-Stunden-Format. Wenn der Wert für den Parameter `UploadFrequency` auf "Daily"festgelegt ist, wird der Parameter `DayOfWeek` ignoriert, wenn er angegeben ist.

```
1  $timespan – New-TimeSpan –Hours 22 –Minutes 20
2  Set-CitrixCallHomeSchedule –TimeOfDay $timespan -UploadFrequency Daily
3  <!--NeedCopy-->
```

Um den Zeitplan zu bestätigen, geben Sie `Get-CitrixCallHomeSchedule` ein. Im vorangegangenen Beispiel wird `StartTime=22:20:00, DayOfWeek=Sunday (ignored), UploadFrequency=Daily` zurückgegeben.

Das folgende Cmdlet erstellt einen Zeitplan, nach dem Datenpakete mittwochabends um 22:20 Uhr erstellt und hochgeladen werden.

```
1  $timespan – New-TimeSpan –Hours 22 –Minutes 20
2  Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek Wed -
       UploadFrequency Weekly
3  <!--NeedCopy-->
```

Um den Zeitplan zu bestätigen, geben Sie `Get-CitrixCallHomeSchedule` ein. Im vorangegangenen Beispiel wird `StartTime=22:20:00, DayOfWeek=Wednesday, UploadFrequency=Weekly` zurückgegeben.

Deaktivieren von Call Home

Sie können Call Home mit einem PowerShell-Cmdlet oder mit Citrix Scout deaktivieren.

AOT-Protokolle werden erfasst und auf dem Datenträger gespeichert, selbst wenn geplante Uploads von Call Home deaktiviert sind. (Wenn geplante Uploads deaktiviert sind, werden AOT-Protokolle

nicht automatisch an Citrix hochgeladen.) Sie können die Erfassung und lokale Speicherung von AOT-Protokollen deaktivieren.

Deaktivieren von Call Home mit PowerShell Nach Ausführen des folgenden Cmdlets werden Diagnosedaten nicht automatisch an Citrix hochgeladen. (Sie können Pakete mit Diagnosedaten weiterhin mit PowerShell-Telemetrie-Cmdlets oder Citrix Scout hochladen.)

```
Disable-CitrixCallHome
```

Geben Sie `Get-CitrixCallHome` ein, um zu bestätigen, dass Call Home deaktiviert werden soll. Wenn die Option deaktiviert ist, wird `IsEnabled=False` und `IsMasterImage=False` zurückgegeben.

Deaktivieren eines Erfassungszeitplans mit Citrix Scout Folgen Sie zum Deaktivieren eines Zeitplans zur Diagnosedatenerfassung mit Citrix Scout den Anweisungen unter Planen der Sammlung. Klicken Sie in Schritt 3 auf **Aus**, um den Zeitplan für die ausgewählten Maschinen zu deaktivieren.

Deaktivieren der Erfassung von AOT-Protokollen Nach Ausführen des folgenden Cmdlets (mit Feld `Enabled` = **`false`**) werden AOT- Protokolle nicht weiter erfasst.

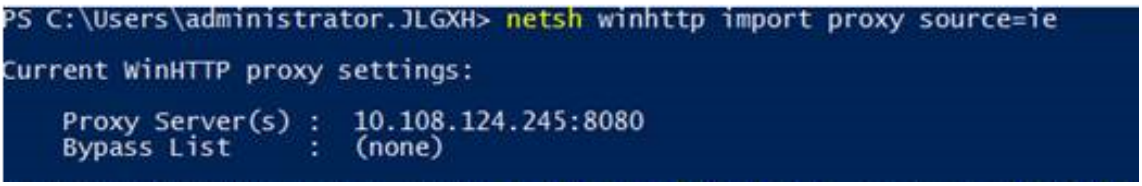
```
Enable-CitrixTrace -Listen‘{ “trace”:{ “enabled”:false,“persistDirectory
”:“C:\Users\Public”,”maxSizeBytes”:1000000, “sliceDurationSeconds”:300
} } ’
```

Der Parameter `Listen` enthält Argumente im JSON-Format.

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.

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.
2. Führen Sie in PowerShell `netsh winhttp import proxy source=ie` aus.



3. Bearbeiten Sie mit einem Text-Editor die Konfigurationsdatei TelemetryService.exe in C:\Programme\Citrix\Telemetry Service. Fügen Sie die in dem roten Feld dargestellten Informationen hinzu.

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 erfassen und nach CIS hochzuladen. (Das Paket wird nicht lokal gespeichert.)
- Verwenden Sie das Cmdlet `Start-CitrixCallHomeUpload`, um Daten manuell zu erfassen und ein Diagnoseinformationspaket lokal zu speichern. Auf diese Weise können Sie eine Vorschau der Daten anzeigen. Später können Sie 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 in CIS:

```
Start-CitrixCallHomeUpload [-Credential] PSCredential [-InputPath
    string] [-Description string] [-IncidentTime string] [-SRNumber
    string] [-Name string] [-UploadHeader string] [-AppendHeaders string
    ] [-Collect string] [<CommonParameters>]
<!--NeedCopy-->
```

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
    strings] [<CommonParameters>]
<!--NeedCopy-->
```

Die folgenden Parameter sind gültig:

- **Credential:** 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:** Informationen über den Upload.
- **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 Datensammelpunktwerte sind:

  - ‘wmi’
  - ‘process’
  - ‘registry
  - ‘crashreport’
  - ‘trace’
  - ‘file’
  - ‘msi’
  - ‘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 eines der folgenden Syntaxmuster:

  - “-Collect “{‘sfb’:{‘account’:’domain\\user1’}}”
  - “-Collect “{‘sfb’:{‘accounts’:[‘domain\\\user1’, ‘domain\\\user2’]}}”

- Allgemeine Parameter: siehe **PowerShell-Hilfe**.

Hochladen von Daten, die zuvor lokal gespeichert waren:

```
Send-CitrixCallHomeBundle -Credential <PSCredentia\> -Path string [<
CommonParameters>]
```

Mit dem Parameter `Path` 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 Citrix Provisioning-VDAs, die um 14:30 Uhr für den Citrix Supportfall 123456 vermerkt wurden. Zusätzlich zu den Call Home-Daten wird die Datei c:\Diagnostics\ExtraData.zip in das Uploadpaket eingeschlossen.

```
1 C:\PS>Start-CitrixCallHomeUpload -InputPath "c:\Diagnostics\ExtraData.
     zip" -Description "Registration failures with Citrix Provisioning
     VDAs" -IncidentTime "14:30" -SRNumber 123456 -Name "
     RegistrationFailure-021812016" -Collect "{
2  'wmi':{
3  'enabled':false }
4   }
5  " -UploadHeader "{
6  'key1':'value1' }
7  " -AppendHeaders "{
```



```
 'key2':'value2' }
 "
<!--NeedCopy-->
```

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
<!--NeedCopy-->
```

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
<!--NeedCopy-->
```

Citrix Scout

January 23, 2023

Einführung

Citrix Scout sammelt Diagnosen und führt Systemintegritätsprüfungen durch. Sie können die Ergebnisse zur vorbeugenden Wartung der Citrix Virtual Apps and Desktops-Bereitstellung verwenden. Citrix bietet eine umfassende, automatisierte Analyse der Diagnoseerfassungen 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 folgende Verfahren:

- **Sammeln:** Eine einmalige Sammlung von Diagnosedaten wird auf den von Ihnen in der Site ausgewählten Maschinen durchgeführt. Anschließend laden Sie die Datei 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 die Datei 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 wird automatisch an Citrix hochgeladen.
- **Systemintegritätsprüfung:** Prüft die Integrität und Verfügbarkeit der Site und ihrer Komponenten. Sie können Integritätsprüfungen an Delivery Controllern, VDAs, StoreFront-Servern und Citrix Lizenzservern ausführen. Wenn Probleme gefunden werden, wird durch Scout ein detaillierter Bericht bereitgestellt. Jedes Mal, wenn Scout gestartet wird, sucht es nach aktualisierten Prüfskripts. Wenn neue Versionen verfügbar sind, lädt Scout diese automatisch herunter, um sie bei der nächsten Prüfung zu verwenden.

Die in diesem Artikel beschriebene grafische Benutzeroberfläche ist die primäre Methode zur Steuerung von Scout. Alternativ können Sie mit PowerShell einmalige oder geplante Diagnosesammlungen und Uploads konfigurieren. Siehe Call Home.

Ort der Ausführung von Scout

- In einer lokalen Bereitstellung führen Sie Scout auf einem Delivery Controller aus, wenn auf einem oder mehreren VDAs, Delivery Controllern, StoreFront-Servern oder Lizenzservern Diagnosedaten gesammelt oder Prüfungen ausgeführt werden sollen. Sie können Scout auch auf einem VDA ausführen, um lokale Diagnosedaten zu sammeln.
- In einer Citrix Cloud-Umgebung mit Citrix Virtual Apps and Desktops Service führen Sie Scout auf einem VDA zum Sammeln lokaler Diagnosedaten aus.

Das Protokoll für Scout wird unter `C:\ProgramData\Citrix\TelemetryService\ScoutUI.log` gespeichert. Diese Datei kann zur Problembehandlung verwendet werden.

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.

Die Sammlung umfasst Folgendes:

- Von Citrix Virtual Apps and Desktops 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
- Citrix Richtlinieninformationen im CSV-Format
- Informationen zu Installation und Upgrade. Die Sammlung kann das Protokoll des Metainstallers für das vollständige Produkt, Protokolle über MSI-Fehler, die Ausgabe der MSI-Protokollanalyse, StoreFront-Protokolle, Protokolle der Lizenzkompatibilitätsprüfung und Ergebnisse vorläufiger Site-Upgradetests umfassen.

Hinweise zu Ablaufverfolgungsdaten

- Die Ablaufverfolgungsdaten werden beim Sammeln komprimiert und erfordern nur wenig Speicherplatz auf der Maschine.
- Der Citrix Telemetriedienst speichert auf jeder Maschine Ablaufverfolgungsdaten in komprimierter Form für maximal acht Tage.
- Ab Citrix Virtual Apps and Desktops 7 1808 werden Tracedateien der Always-On-Ablaufverfolgung standardmäßig auf dem lokalen Datenträger gespeichert. (In früheren Versionen wurden Tracedateien im Arbeitsspeicher abgelegt.) Standardpfad = `C:\Users\CitrixTelemetryService\AppData\Local\CitrixAOT`.
- Ab Citrix Virtual Apps and Desktops 7 1811 werden auf Netzwerkfreigaben gespeicherte AOT-Traces zusammen mit anderen Diagnosedaten erfasst.
- Sie können die maximale Größe (Standard = 10 MB) und Slicedauer mit dem Cmdlet `Enable-CitrixTrace` oder dem Registrierungseintrag `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Telemetry DefaultListen` ändern.
- Traces werden bis zum Erreichen von 10 % des `MaxSize`-Werts an die Datei angehängt.

Eine Liste der Datenpunkte, die Scout erfasst, finden Sie unter Wichtige Call Home-Datenpunkte.

Informationen zu Integritätsprüfungen

Die Daten der Integritätsprüfung werden in Ordnern unter `C:\ProgramData\Citrix\TelemetryService\` gespeichert.

Siteintegritätsprüfungen

Siteintegritätsprüfungen sind im Environment Test Service enthalten, der eine umfassende Bewertung der FlexCast Management Architecture-Dienste bietet. Neben der Dienstverfügbarkeit werden weitere Integritätsindikatoren, etwa die Datenbankverbindungen, überprüft.

Siteintegritätsprüfungen werden auf Delivery Controllern ausgeführt. Abhängig von der Größe der Site können diese Prüfungen bis zu einer Stunde dauern.

Delivery Controller-Konfigurationsprüfungen Im Rahmen der Siteintegritätsprüfungen. Bei der Delivery Controller-Konfigurationsprüfung wird anhand der Citrix Empfehlungen für Citrix Virtual Apps and Desktops-Sites auf folgende Probleme geprüft:

- Ein oder mehrere Delivery Controller befinden sich in einem fehlerhaften Zustand.
- Es gibt nur einen Delivery Controller in der Site.
- Die Delivery Controller liegen in verschiedenen Versionen vor.

Zusätzlich zur Erfüllung der Berechtigungen und Anforderungen für Integritätsprüfungen erfordern Delivery Controller-Konfigurationsprüfungen Folgendes:

- Mindestens ein Controller ist eingeschaltet.
- Der Brokerdienst wird auf einem Controller ausgeführt.
- Eine funktionierende Verbindung vom Controller zur Sitedatenbank.

VDA-Integritätsprüfungen

Bei VDA-Integritätsprüfungen wird die mögliche Ursache häufiger Probleme bei der VDA-Registrierung, beim Sitzungsstart und bei der Zeitzonenumleitung gesucht.

Für die Registrierung auf dem VDA überprüft Scout Folgendes:

- Installation der VDA-Software
- Domänenmitgliedschaft der VDA-Maschine
- Verfügbarkeit der VDA-Kommunikationsports
- VDA-Dienststatus
- Konfiguration der Windows-Firewall
- Kommunikation mit dem Controller
- Zeitsynchronisierung mit dem Controller
- VDA-Registrierungsstatus

Für den Sitzungsstart auf VDAs überprüft Scout Folgendes:

- Verfügbarkeit der Sitzungsstart-Kommunikationsports
- Status der Sitzungsstartdienste
- Windows-Firewallkonfiguration für den Sitzungsstart
- Clientzugriffslizenzen für VDA-Remotedesktopdienste
- VDA-Anwendungsstartpfad

Für die Zeitzonenumleitung auf VDAs überprüft Scout Folgendes:

- Windows-Hotfixinstallation
- Citrix Hotfixinstallation
- Microsoft-Gruppenrichtlinieneinstellungen
- Citrix Gruppenrichtlinieneinstellungen

StoreFront-Integritätsprüfungen

Für StoreFront wird Folgendes überprüft:

- Der Citrix Standarddomänendienst wird ausgeführt.
- Der Citrix Credential Wallet-Dienst wird ausgeführt.
- Es gibt eine Verbindung vom StoreFront-Server zum Active Directory-Port 88.
- Es gibt eine Verbindung vom StoreFront-Server zum Active Directory-Port 389.
- Die Basis-URL hat einen gültigen FQDN.
- Die korrekte IP-Adresse kann aus der Basis-URL abgerufen werden.
- Der IIS-Anwendungspool verwendet .NET 4.0.
- Ob das Zertifikat an den SSL-Port für die Host-URL gebunden ist.
- Ob die Zertifikatkette vollständig ist.
- Ob Zertifikate abgelaufen sind.
- Ob ein Zertifikat bald abläuft (innerhalb von 30 Tagen).

Lizenzserverprüfungen

Für den Lizenzserver wird Folgendes überprüft:

- Lizenzserver-Verbindung vom Delivery Controller
- RAS-Status der Lizenzserver-Firewall
- Status des Citrix Lizenzierungsdiensts
- Status des Lizenzserver-Kulanzzeitraums
- Verbindung der Lizenzserver-Ports
- Ob der Citrix Vendor Daemon (CITRIX) ausgeführt wird
- Ob die Systemuhren synchronisiert sind
- Ob der Citrix Lizenzierungsdienst unter dem lokalen Dienstkonto ausgeführt wird
- Vorhandensein der Datei `CITRIX.opt`
- Datum der Customer Success Services-Berechtigung
- Citrix Lizenzserverupdate
- Ob das Lizenzserverzertifikat im vertrauenswürdigen Stammspeicher des Delivery Controllers ist

Neben der Erfüllung der Berechtigungen und Anforderungen für Integritätsprüfungen muss der Lizenzserver Mitglied einer Domäne sein. Andernfalls wird der Lizenzserver nicht erkannt.

Berechtigungen und Anforderungen

Berechtigungen:

- Sammeln von Diagnosedaten:
  - 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.
- Ausführen von Integritätsprüfungen:
  - Sie müssen Mitglied der Gruppe "Domänenbenutzer"sein.
  - Sie müssen entweder Volladministrator sein oder eine benutzerdefinierte Rolle mit Lesezugriff und Berechtigung zum **Ausführen von Umgebungstests** für die Site haben.
- Verwenden Sie **Als Administrator ausführen**, wenn Sie Scout starten.

Für jede Maschine, auf der Sie Diagnosedaten erfassen oder Integritätsprüfungen ausführen, 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.
- WMI-Zugriff (Windows Management Infrastructure) muss auf der Maschine aktiviert sein.
- Um einen Zeitplan für die Diagnoseerfassung festzulegen, muss auf der Maschine eine kompatible Scout-Version ausgeführt werden.

Verwenden Sie in Benutzernamen, die in Pfadnamen angegeben sind, kein Dollarzeichen ($). Das Dollarzeichen verhindert die Erfassung von Diagnoseinformationen.

Von Scout werden die von Ihnen ausgewählten Maschinen auf Erfüllung dieser Bedingungen geprüft.

Tests zur Überprüfung

Vor Ausführung einer Diagnosesammlung oder Integritätsprüfung wird automatisch jede ausgewählte Maschine überprüft. Diese Prüfung gewährleistet, dass die Anforderungen erfüllt sind. Besteht eine Maschine den Test nicht, wird in Scout eine Meldung mit einem Maßnahmenvorschlag angezeigt.

- **Scout kann diese Maschine nicht erreichen:** Stellen Sie Folgendes sicher:
  - Die Maschine ist eingeschaltet.
  - Die Verbindung mit dem Netzwerk funktioniert ordnungsgemäß. (Dazu gehört u. U. eine Überprüfung der ordnungsgemäßen Konfiguration der Firewall.)

  - Datei- und Druckerfreigabe ist aktiviert. Weitere Informationen finden Sie in der Microsoft Dokumentation.

- **PSRemoting und WinRM aktivieren:** 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.
- **WMI wird nicht auf der Maschine ausgeführt:** Stellen Sie sicher, dass der Windows Management Instrumentation-Zugriff aktiviert ist.
- **WMI-Verbindungen blockiert:** Aktivieren Sie WMI im Windows-Firewalldienst.
- **Aktuellere Version des Citrix Telemetry Service ist erforderlich:** (Die Version wird nur für "Sammeln"und "Ablauf verfolgen und reproduzieren"überprüft.) Aktualisieren Sie den Telemetriedienst auf der Maschine (siehe Installation und Upgrade). Wenn Sie den Dienst nicht aktualisieren, wird die Maschine von den Aktionen **Sammeln** bzw. **Ablauf verfolgen und reproduzieren** ausgeschlossen.

Versionskompatibilität

Diese Version von Scout (3.x) ist für die Ausführung auf Controllern und VDAs unter Citrix Virtual Apps and Desktops (bzw. XenApp und XenDesktop ab Version 7.14) vorgesehen.

Eine ältere Version von Scout steht für XenApp und XenDesktop-Bereitstellungen vor Version 7.14 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 Virtual Apps and Desktops (sowie XenApp und XenDesktop 7.14 bis 7.18)	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)
Integritätsprüfungen	Nein	Ja

Feature	Scout 2.23	Scout 3.0
Datenmaskierung	Nein	Ab 3.17

Installation und Upgrade

Standardmäßig wird Scout automatisch als Teil des Citrix Telemetriediensts installiert bzw. aktualisiert, wenn Sie einen VDA oder Controller installieren oder aktualisieren.

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 Installationsmediums für Citrix Virtual Apps and Desktops aus.

Wenn Sie die Aktion **Sammeln** oder **Ablauf verfolgen und reproduzieren** ausführen, werden Sie benachrichtigt, wenn auf einer Maschine eine ältere Version des Citrix Telemetriediensts ausgeführt wird. Citrix empfiehlt die Verwendung der neuesten unterstützten Version. Wenn Sie den Telemetriedienst nicht aktualisieren, wird die Maschine von den Aktionen **Sammeln** bzw. **Ablauf verfolgen und reproduzieren** ausgeschlossen. Verwenden Sie zum Aktualisieren des Telemetriediensts dasselbe Verfahren wie bei der Installation.

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. Zur Verwendung des Tokens das nächste Mal beim Ausführen von **Sammeln** oder **Ablauf verfolgen und reproduzieren** 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. Alternativ können Sie die IP-Adresse und Portnummer des Proxyservers angeben.

Manuelles Hinzufügen von Maschinen

Nachdem Scout die erkannten Controller und VDAs aufgelistet hat, können Sie weitere Maschinen in der Bereitstellung (StoreFront-Server, Citrix Provisioning-Server usw.) manuell hinzufügen.

Beim Ausführen von Integritätsprüfungen gilt Folgendes:

- Citrix Lizenzserver in der Domäne werden automatisch erkannt. Lizenzserver können nicht manuell hinzugefügt werden.
- Integritätsprüfungen unterstützen derzeit keine Citrix Provisioning-Server.

Klicken Sie auf einer Scout-Seite, auf der die erkannten Maschinen aufgeführt werden, auf **Maschine hinzufügen**. Geben Sie den FQDN der gewünschten Maschine ein und klicken Sie auf **Weiter**. Wiederholen Sie den Vorgang, um nach Bedarf weitere Maschinen hinzuzufügen. (Die Eingabe eines DNS-Alias anstelle eines FQDNs erscheint möglicherweise zwar als gültig, die Integritätsprüfungen können jedoch fehlschlagen.)

Manuell hinzugefügte Maschinen erscheinen in der Maschinenliste immer vor den erkannten Maschinen.

Anhand der roten Löschschaltfläche am rechten Zeilenende lassen sich manuell hinzugefügte Maschinen leicht erkennen. Diese Schaltfläche wird nur für manuell hinzugefügte Maschinen angezeigt. Für erkannte Maschinen wird sie nicht angezeigt.

Zum Entfernen einer manuell hinzugefügten Maschine klicken Sie auf die rote Schaltfläche am rechten Zeilenende. Bestätigen Sie die Löschung. Wiederholen Sie diesen Vorgang nach Bedarf, um weitere manuell hinzugefügte Maschinen zu löschen.

Scout behält alle manuell hinzugefügte Maschinen in der Liste, bis Sie sie entfernen. Wenn Sie Scout schließen und erneut öffnen, werden die manuell hinzugefügten Maschinen weiterhin oben in der Liste aufgeführt.

Bei Verwendung des Features **Ablauf verfolgen und reproduzieren** auf StoreFront-Servern werden keine CDF-Abläufe erfasst. Alle anderen Ablaufverfolgungsinformationen werden jedoch gesammelt.

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.

1. Starten Sie Scout. Wählen Sie im **Startmenü** der Maschine **Citrix > Citrix Scout**. Klicken Sie auf der Startseite auf **Sammeln**.
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**.

   Informationen zum manuellen Hinzufügen weiterer Maschinen (z. B. von StoreFront- oder Citrix Provisioning-Servern) finden Sie unter Manuelles Hinzufügen von Maschinen.

   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**.
3. Sammeln Sie Diagnosedaten. 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 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 darauf klicken, geht die Sammlung verloren.)

Wenn die Sammlung abgeschlossen ist, klicken Sie auf **Weiter**.

4. Sammlung speichern oder hochladen. Wählen Sie, ob die Datei 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. Siehe CTX136396.

   Klicken Sie auf **Fertig**, um zur Scout-Startseite zurückzukehren. Sie brauchen keine weiteren Schritte auszuführen.

5. Authentifizieren Sie sich für Uploads und geben Sie optional den Proxy an. Weitere Informationen 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 das wünschen, wählen Sie diese Option aus 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 des Browsers konfigurieren. Alternativ können Sie 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**.

6. Geben Sie Informationen zum Upload an.

   - 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, die Diagnosesammlung und den Upload der Datei 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 enthalten Tracingberichte der Always-On-Ablaufverfolgung. Durch dieses Verfahren werden CDF-Tracingberichte zur Vereinfachung der Problembehandlung hinzugefügt.

1. Starten Sie Scout. Wählen Sie im **Startmenü** der Maschine **Citrix > Citrix Scout**. Klicken Sie auf der Startseite auf **Ablauf verfolgen und reproduzieren**.
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 Kon-

trollkästchen neben jeder Maschine, auf der Sie Ablaufverfolgungs- und Diagnosedaten sammeln möchten. Klicken Sie dann auf **Weiter**.

Informationen zum manuellen Hinzufügen weiterer Maschinen (z. B. von StoreFront- oder Citrix Provisioning-Servern) finden Sie unter Manuelles Hinzufügen von Maschinen.

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 Diagnose- und Ablaufverfolgungsdaten gesammelt.

Nach Abschluss der Überprüfung klicken Sie auf **Weiter**.

3. Beginnen Sie die Ablaufverfolgung. 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.

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 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 dies tun, geht die Sammlung verloren.)

Wenn die Sammlung abgeschlossen ist, klicken Sie auf **Weiter**.

5. Sammlung speichern oder hochladen. Wählen Sie, ob die Datei an Citrix hochgeladen oder lokal 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 für Citrix Insight Services.

   Klicken Sie auf **Fertig**, um zur Scout-Startseite zurückzukehren. Sie brauchen keine weiteren Schritte auszuführen.

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 das wünschen, wählen Sie diese Option aus 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**. Sie können Scout zur Verwendung der Internet-Proxyeinstellungen des Browsers konfigurieren. Alternativ können Sie 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**.

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

> Hinweis:
>
> Sie können derzeit Sammlungen planen, aber keine Integritätsprüfungen.

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.

1. Starten Sie Scout. Wählen Sie im Startmenü der Maschine **Citrix > Citrix Scout**. Wählen Sie **Zeitplan**.
2. Maschinen auswählen. Alle VDAs und Controller der Site werden aufgelistet. Sie können die Anzeige nach Maschinennamen filtern.

Wenn Sie VDAs und Controller über die grafische Oberfläche installiert haben und einen Call Home-Zeitplan festlegen (siehe Citrix Call Home), zeigt Scout diese Einstellungen standardmäßig an. Sie können mit dieser Version von Scout einen neuen Zeitplan einrichten oder einen zuvor konfigurierten Zeitplan ändern.

Sie aktivieren/deaktivieren bei der Installation von Komponenten Call Home zwar für einzelne Maschinen, ein in Scout festgelegter Zeitplan gilt jedoch für alle Maschinen, die Sie auswählen.

Aktivieren Sie das Kontrollkästchen neben jeder Maschine, auf der Sie Diagnosedaten sammeln möchten, und klicken Sie auf **Weiter**.

Informationen zum manuellen Hinzufügen weiterer Maschinen (z. B. von StoreFront- oder Citrix Provisioning-Servern) finden Sie unter Manuelles Hinzufügen von Maschinen.

Scout überprüft automatisch jede ausgewählte Maschine auf Erfüllung der Kriterien für Tests zur Überprüfung. 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 Diagnose- und 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**.

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. Geben Sie die Uhrzeit ein, zu der die Sammlung beginnen soll.
   - Zum Konfigurieren eines täglichen Zeitplans für die ausgewählten Maschinen klicken Sie auf **Täglich**. Geben Sie die Uhrzeit ein, zu der die Sammlung 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**.

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**. Sie können Scout zur Verwendung der Internet-Proxyeinstellungen des Browsers konfigurieren. Alternativ können Sie 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.

Durchführen von Integritätsprüfungen

Die Integritätsprüfung umfasst die Auswahl von Maschinen, das Starten der Prüfung und das anschließende Prüfen des Ergebnisberichts.

1. Starten Sie Scout. Wählen Sie im **Startmenü** der Maschine **Citrix > Citrix Scout**. Wählen Sie **Integritätsprüfung**.
2. Maschinen auswählen. Auf der Seite **Maschinen wählen** werden alle in der Site erkannten VDAs, Delivery Controller und Lizenzserver 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**.

   Informationen zum Hinzufügen anderer Komponenten (z. B. von StoreFront-Servern) finden Sie unter Manuelles Hinzufügen von Maschinen. Citrix Provisioning-Server und Citrix Lizenzserver können nicht manuell hinzugefügt werden.

   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 der Maschine 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). Integritätsprüfungen werden für diese Maschine nicht ausgeführt.

Nach Abschluss der Überprüfung klicken Sie auf **Weiter**.

3. Führen Sie die Integritätsprüfungen auf den ausgewählten Maschinen aus. In der Zusammenfassung werden die Maschinen aufgelistet, auf denen die Prüfungen ausgeführt werden (d. h. die Maschinen, die Sie ausgewählt haben und die den Test bestanden haben). Klicken Sie auf **Überprüfung starten**.

   Während und nach der Prüfung:

   - In der Spalte **Status** wird der aktuelle Status der Prüfung für die Maschinen angezeigt.
   - Um alle laufenden Prüfungen zu stoppen, klicken Sie unten rechts auf der Seite auf **Überprüfung stoppen**. (Sie können die Integritätsprüfung nur für alle ausgewählten Maschinen, nicht aber für einzelne Maschinen stoppen.) Daten von Maschinen, für die die Prüfungen abgeschlossen wurden, werden beibehalten.
   - Wenn die Überprüfung aller ausgewählten Maschinen abgeschlossen ist, ändert sich die Schaltfläche **Überprüfung stoppen** in der unteren rechten Ecke in **Fertig**.
   - Schlägt eine Überprüfung fehl, können Sie in der Spalte **Aktion** auf **Wiederholen** klicken.
   - Wenn eine Überprüfung abgeschlossen wird und kein Problem gefunden wurde, bleibt die Spalte **Aktion** leer.
   - Wird bei einer Überprüfung ein Problem festgestellt, klicken Sie auf **Details anzeigen**, um die Ergebnisse anzuzeigen.
   - Wenn die Überprüfung für alle ausgewählten Maschinen abgeschlossen ist, klicken Sie nicht auf **Zurück**. (Wenn Sie dies tun, gehen die Prüfergebnisse verloren.)

4. Klicken Sie nach Abschließen der Überprüfungen auf **Fertig**, um zur Scout-Startseite zurückzukehren.

Ergebnisse der Integritätsprüfung

Berichte von Citrix Prüfungen enthalten Folgendes:

- Uhrzeit und Datum der Erstellung des Ergebnisberichts
- Überprüfte Maschinen
- Bedingungen, auf die auf den Zielmaschinen geprüft wurde

Überwachung

September 21, 2021

Administratoren und Helpdeskmitarbeiter können Citrix Virtual Apps and Desktops-Sites mit einer Reihe von Features und Tools überwachen. Sie können mit diesen Tools 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.

Konfigurationsprotokollierung

Mit der Konfigurationsprotokollierung können 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 Maschinen mit einzelner Sitzung

- Fehlgeschlagene Maschinen mit mehreren Sitzungen

Weitere Informationen zum Aktivieren und Konfigurieren der Konfigurationsprotokollierung finden Sie im Artikel Konfigurationsprotokollierung. Im Artikel Director wird beschrieben, wie protokollierte Informationen über dieses Tool angezeigt werden.

Ereignisprotokolle

Dienste in Citrix Virtual Apps and Desktops protokollieren auftretende Ereignisse. Ereignisprotokolle können zur Überwachung und Problembehandlung verwendet werden.

Weitere Informationen finden Sie unter Ereignisprotokolle. Artikel zu einzelnen Features enthalten auch Informationen zu Ereignissen.

Konfigurationsprotokollierung

September 21, 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 anhand von Datumsbereichen und Ergebnissen 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 jedem Controller 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 auf Englisch erstelltes Protokoll wird unabhängig vom Gebietsschema des Lesers auf 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).

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 **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 **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 **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. 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 **Änderungen der Sitekonfiguration ohne Datenbankzugriff**. Konfigurationsänderungen und administrative Aktivitäten sind dann zulässig, selbst wenn kein Zugriff auf die Konfigurationsprotokollierungsdatenbank besteht. Dies ist die Standardeinstellung.

Ändern des Speicherorts für die Konfigurationsprotokollierungsdatenbank

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. Informationen zu gültigen Formaten finden Sie unter Datenbankadressformate.
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 Bereich auswählen, werden im unteren Bereich die Low-Level-Operationen angezeigt.

Schlägt eine Operation vor der Beendigung fehl, kann die Protokollierung in der Datenbank evtl. nicht abgeschlossen werden. Beispielsweise hat ein Startdatensatz dann keinen entsprechenden Stoppdatensatz. 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. Sie haben folgende Möglichkeiten:

- Sortieren der Anzeige nach Spaltenüberschrift.
- Filtern der Anzeige, indem Sie ein Tagesintervall angeben oder Text in das Feld **Suchen** eingeben. Um nach dem Suchen zur Standardanzeige zurückzukehren, löschen Sie den Text im Feld **Suchen**.

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 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 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 die Anmeldung einem Benutzer in der Datenbank zu. SQL Server erstellt automatisch einen Benutzer in der Datenbank mit dem gleichen Namen.

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 wird. 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

April 1, 2021

Die folgenden Artikel enthalten Informationen zu den Ereignissen, die von Diensten in Citrix Virtual Apps and Desktops protokolliert werden können.

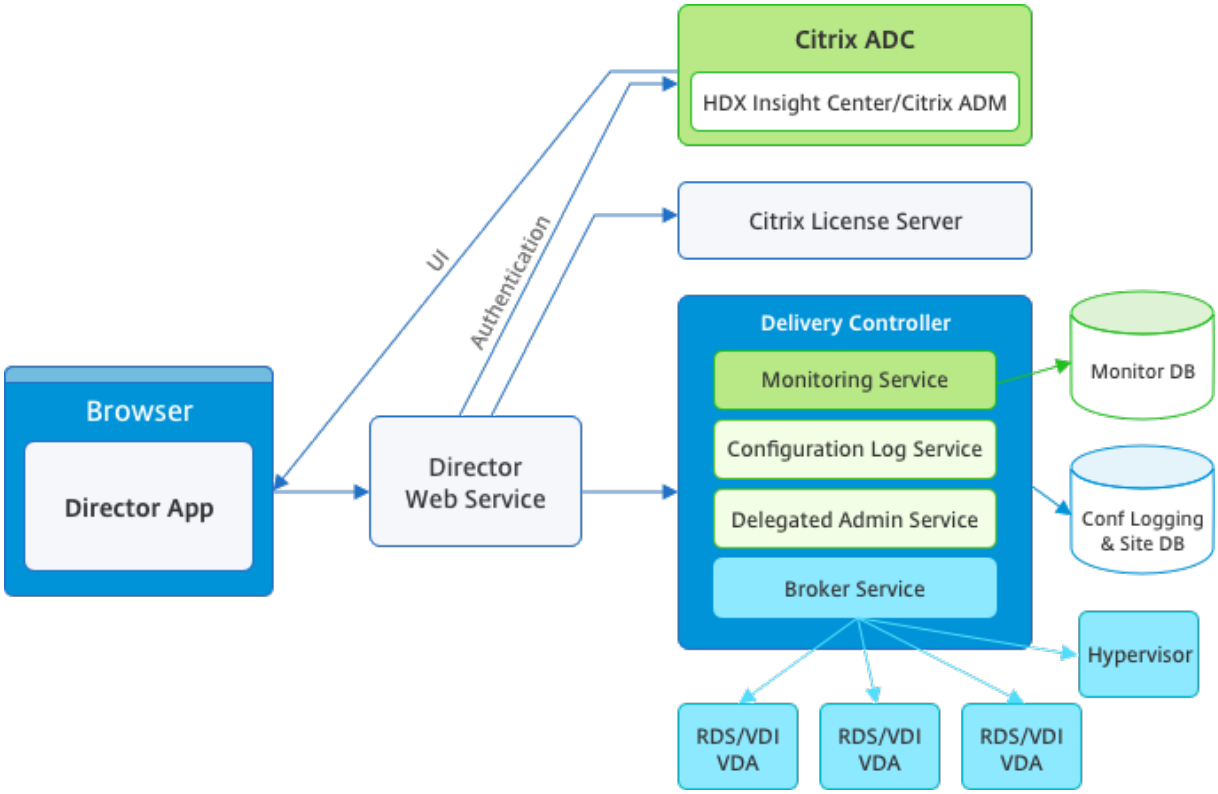
Die Informationen sind nicht erschöpfend. Weitere Informationen zu Ereignissen enthalten die Artikel zu den einzelnen Features.

- Citrix Brokerdienstereignisse
- Citrix FMA Service SDK-Ereignisse
- Citrix Konfigurationsdienstereignisse
- Citrix Delegated Administration Service-Ereignisse

Director

May 24, 2024

Director ist eine Konsole zur Überwachung und Problembehandlung für Citrix Virtual Apps and Desktops.



Director hat auf Folgendes Zugriff:

- Echtzeitdaten vom Brokeragent über eine einheitliche Konsole, die mit Analytics, Leistungsverwaltung und Netzwerkinspektion integriert ist.
  - Analytics umfasst eine Leistungsverwaltung zum Sicherstellen von Integrität und Kapazität, sowie historische Trends und Netzwerkanalysedaten (von Citrix ADM) zum Identifizieren von Engpässen, die auf dem Netzwerk in der Citrix Virtual Apps und Desktops-Umgebung beruhen.
- In der Überwachungsdatenbank gespeicherte historische Daten für den Zugriff auf die Datenbank für die Konfigurationsprotokollierung.
- ICA-Daten vom Citrix Gateway unter Verwendung von Citrix ADM.
  - Übersicht über die Endbenutzererfahrung für virtuelle Anwendungen, Desktops und Benutzer für Citrix Virtual Apps oder Desktops.
  - Korrelation von Netzwerkdaten mit Anwendungsdaten und Echtzeitmetrik für effektive Problembehandlung.
  - Integration mit dem Überwachungstool von Citrix Virtual Desktops 7 Director.

Director hat ein Dashboard zur Problembehandlung, das die Echtzeitzustandsüberwachung der Citrix Virtual Apps- oder Virtual Desktops-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.

> Hinweis:
>
> Aufgrund der Schwachstellen gegenüber den spekulativen ausführungsseitigen Channelangriffen Meltdown und Spectre empfiehlt Citrix die Installation relevanter Patches. Diese Patches können die Leistung von SQL Server beeinträchtigen. Weitere Informationen finden Sie im Microsoft-Supportartikel Protect SQL Server from attacks on Spectre and Meltdown side-channelvulnerabilities. Citrix empfiehlt, dass Sie die Skalierung testen und Workloads planen, bevor Sie die Patches in Ihren Produktionsumgebungen bereitstellen.

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. Informationen zur Installation und Konfiguration von Director finden Sie unter Installieren und Konfigurieren von Director.

Anmelden bei Director

Die Director-Website ist unter https oder `http://<Server FQDN>/Director`.

Wenn eine der Sites einer Bereitstellung mit mehreren Sites ausfällt, dauert die Anmeldung für Director etwas länger, während Verbindungsversuche mit dieser Site laufen.

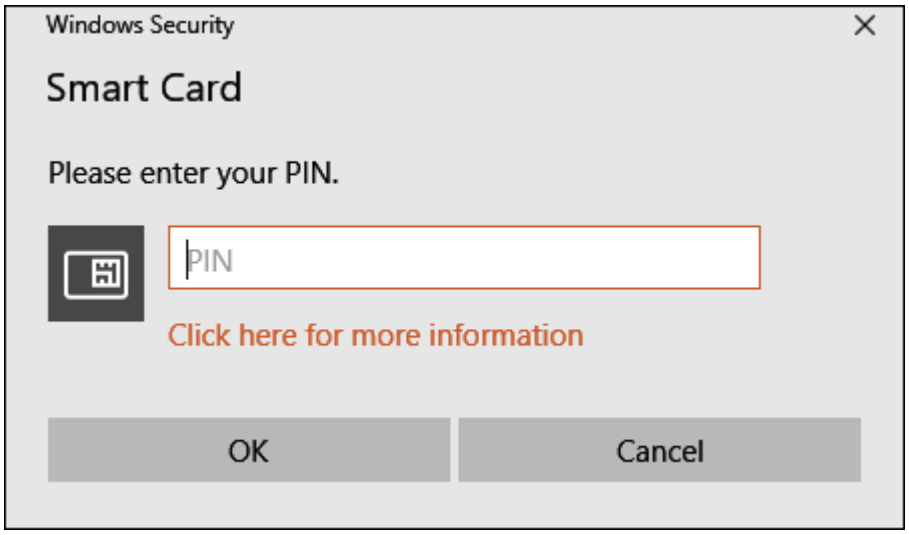
Verwenden von Director mit PIV-Smartcardauthentifizierung

Director unterstützt jetzt die Smartcardauthentifizierung auf PIV-Basis (Personal Identity Verification). Das Feature ist für Unternehmen und Behörden nützlich, die eine Authentifizierung per Smartcard für die Zugriffssteuerung verwenden.
Die Smartcardauthentifizierung erfordert eine spezifische Konfiguration auf dem Director-Server und in Active Directory. Die Konfigurationsschritte werden unter Konfigurieren der PIV-Smartcardauthentifizierung beschrieben.

> Hinweis:
>
> Die Smartcardauthentifizierung wird nur für Benutzer aus derselben Active Directory-Domäne unterstützt.

Nachdem Sie die erforderliche Konfiguration durchgeführt haben, können Sie sich mit einer Smartcard bei Director anmelden:

1. Geben Sie Ihre Smartcard in den Smartcardleser ein.
2. Öffnen Sie einen Browser und rufen Sie die Director-URL "`https://<directorfqdn>/Director`"auf.
3. Wählen Sie ein gültiges Benutzerzertifikat aus der angezeigten Liste aus.
4. Geben Sie Ihr Smartcardtoken ein.



5. Nach der Authentifizierung können Sie auf Director zugreifen, ohne zusätzliche Anmeldeinformationen auf der Anmeldeseite von Director eingeben zu müssen.

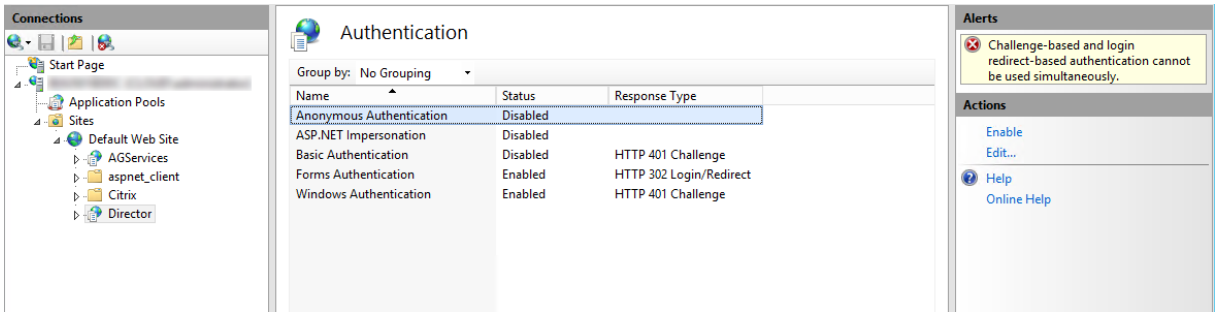
Verwenden von Director mit der integrierten Windows-Authentifizierung

Mit der integrierten Windows-Authentifizierung (IWA) 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.

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.

Weitere Informationen zu den verschiedenen Rollen und ihren Berechtigungen in Director finden Sie unter Delegierte Administration und Director

Erfassung von Nutzungsdaten durch Google Analytics

Director erfasst unter Einsatz von Google Analytics anonyme Nutzungsdaten nach der Installation. Es werden Statistiken über die Nutzung der Trends-Seiten sowie Analysedaten zu OData API-Aufrufen erfasst. Die Analytics-Sammlung entspricht den Datenschutzrichtlinien von Citrix. Die Datenerfassung ist standardmäßig aktiviert, wenn Sie Director installieren.

Um die Google Analytics-Datenerfassung zu deaktivieren, bearbeiten Sie wie weiter unten beschrieben den Registrierungsschlüssel auf der Maschine, auf der Director installiert ist. Wenn der Registrierungsschlüssel noch nicht vorhanden ist, erstellen Sie ihn und legen Sie den gewünschten Wert fest. Aktualisieren Sie die Director-Instanz nach Änderung des Registrierungsschlüsselwerts.
Achtung: Die unsachgemäße Verwendung des Registrierungs-Editors kann zu schwerwiegenden Problemen führen, die möglicherweise 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. Citrix empfiehlt, dass Sie die Windows-Registrierung sichern, bevor Sie sie ändern.

Speicherort: HKEY_LOCAL_MACHINE\Software\Citrix\Director

Name: DisableGoogleAnalytics

Wert: 0 = aktiviert (Standard), 1 = deaktiviert

Sie können das folgende PowerShell-Cmdlet zum Deaktivieren der Datenerfassung durch Google Analytics verwenden:

```
1 New-Item HKLM:\SOFTWARE\Citrix -Name Director
2 New-ItemProperty HKLM:\SOFTWARE\Citrix\Director -Name
     DisableGoogleAnalytics -PropertyType DWORD -Value 1
```


Leitfaden zu neuen Features

Director enthält einen produktinternen Leitfaden, der Pendo zur Erläuterung der neuen Features in der aktuellen Director-Version verwendet. Anhand dieser Kurzübersicht und produktinternen Meldungen sehen Sie, was am Produkt neu ist.

Um das Feature zu deaktivieren, bearbeiten Sie wie weiter unten beschrieben den Registrierungsschlüssel auf der Maschine, auf der Director installiert ist. Wenn der Registrierungsschlüssel noch nicht vorhanden ist, erstellen Sie ihn und legen Sie den gewünschten Wert fest. Aktualisieren Sie die Director-Instanz nach Änderung des Registrierungsschlüsselwerts.

Achtung: Die unsachgemäße Verwendung des Registrierungs-Editors kann zu schwerwiegenden Problemen führen, die möglicherweise 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. Citrix empfiehlt, dass Sie die Windows-Registrierung sichern, bevor Sie sie ändern.

Speicherort: HKEY_LOCAL_MACHINE\Software\Citrix\Director

Name: DisableGuidedHelp

Wert: 0 = aktiviert (Standard), 1 = deaktiviert

Sie können das folgende PowerShell-Cmdlet verwenden, um den produktinternen Leitfaden zu deaktivieren:

```
1 New-Item HKLM:\SOFTWARE\Citrix -Name Director
2 New-ItemProperty HKLM:\SOFTWARE\Citrix\Director -Name DisableGuidedHelp
      -PropertyType DWORD -Value 1
```

Installation und Konfiguration

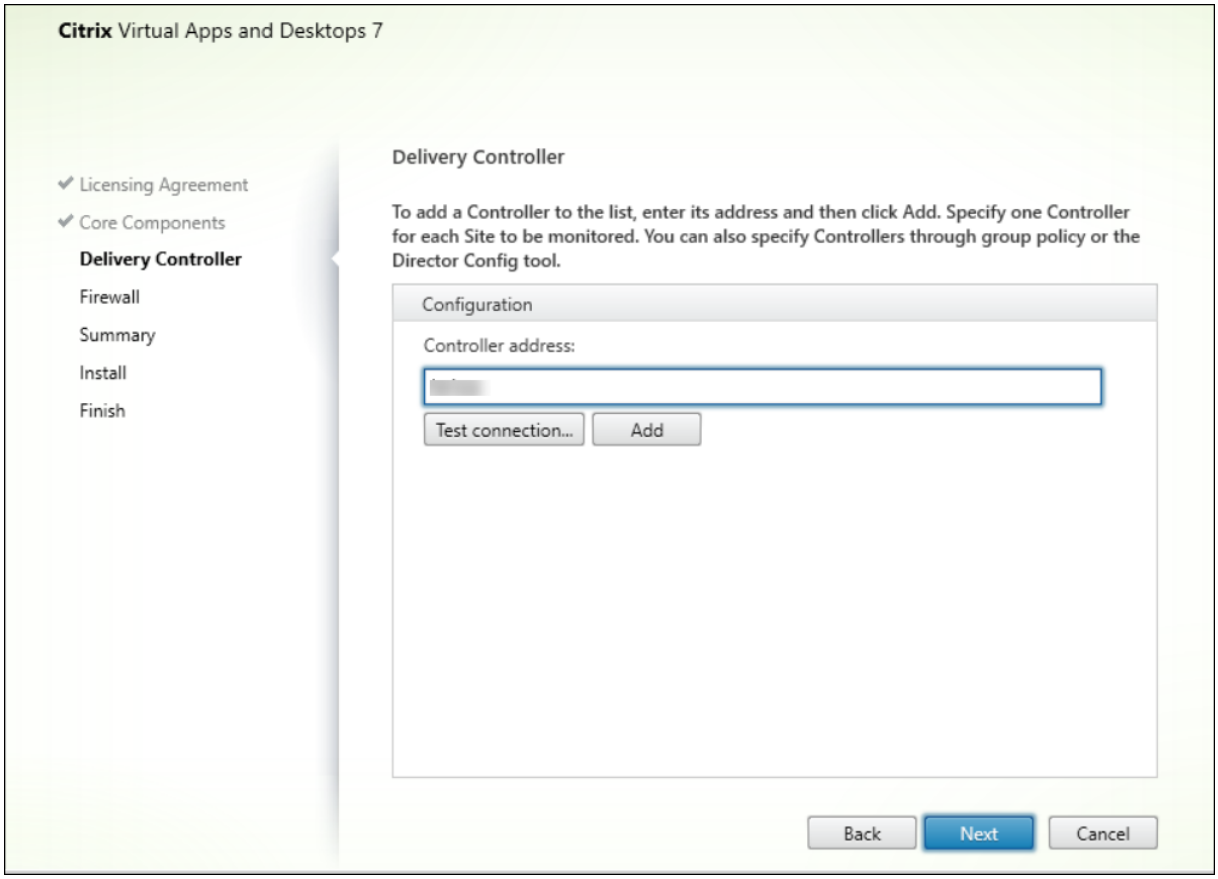
March 9, 2022

Installieren von Director

Installieren Sie Director mit dem ISO-Produktinstallationsprogramm für Citrix Virtual Apps and Desktops. Dieses prüft, ob die Voraussetzungen erfüllt sind, installiert fehlende Komponenten, richtet die Director-Website ein und führt die Grundkonfiguration durch. 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 Virtual Apps-Bereitstellungen vor Version 6.5 und

Virtual Desktops-Bereitstellungen vor Version 7.
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.

Bereitstellen und Konfigurieren von Director

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.

> 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)
- Konfigurierte delegierte Administratorrollen (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.

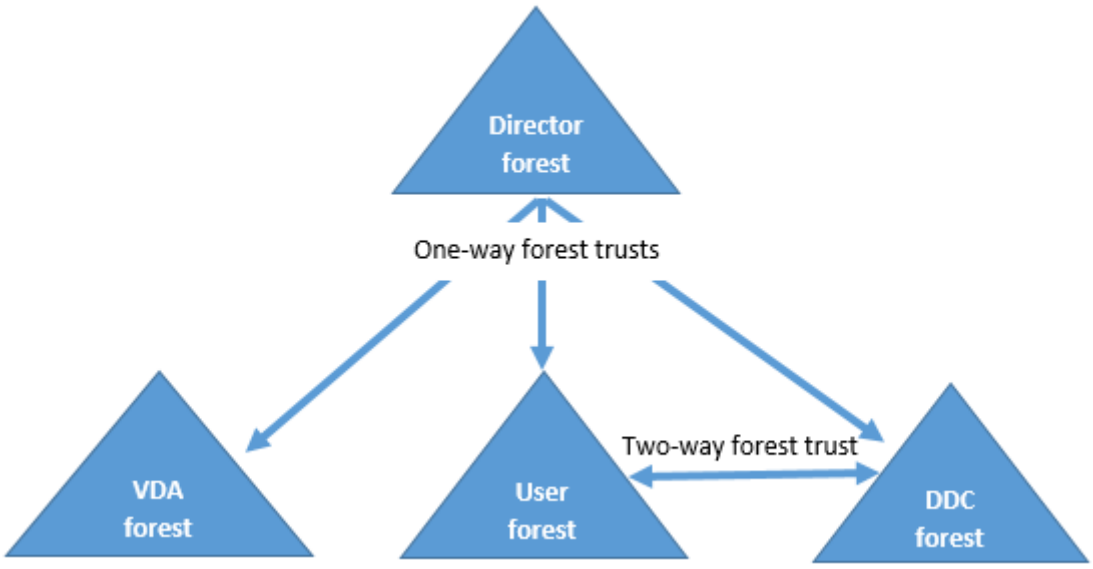
Erweiterte Konfiguration

March 9, 2022

Director unterstützt Umgebungen mit mehreren Gesamtstrukturen, in denen Benutzer, Delivery Controller (DC), 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 Umgebungen 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 Delivery Controllern 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.
5. Klicken Sie auf **Hinzufügen**, um eine neue Einstellung hinzuzufügen.

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 folgende Anwendungseinstellung auf der Director-Website in der IIS-Verwaltungskonsole:

```
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:

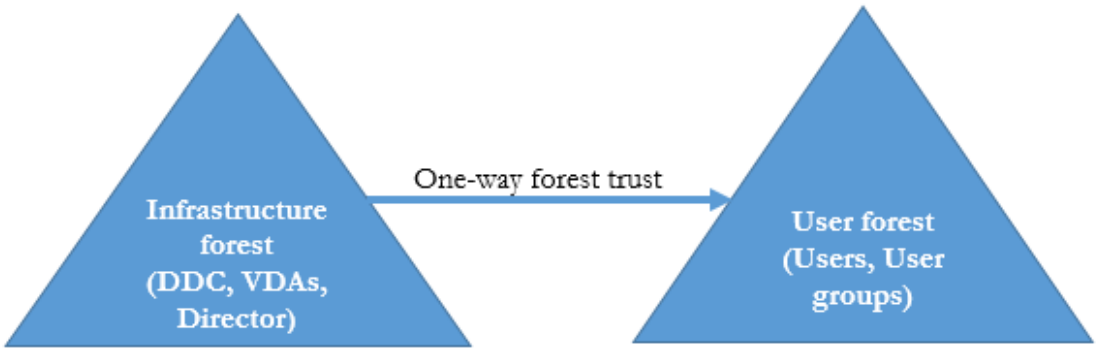
```
Connector.ActiveDirectory.Domains = (user),(server),\<domain1\>,\<
    domain2\>
```

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.

Konfiguration einer domänenlokalen Gruppe

Die meisten Citrix Service Provider (CSPs) haben ähnliche Umgebungen, bei denen die VDAs, der oder die Delivery Controller und Director in einer Infrastruktur-Gesamtstruktur sind und die Benutzer-/Gruppeneinträge in der Kunden-Gesamtstruktur. Von der Infrastruktur-Gesamtstruktur ausgehend besteht zur Kunden-Gesamtstruktur eine unidirektionale Vertrauensstellung.

CSP-Administratoren erstellen in der Regel eine domänenlokale Gruppe in der Infrastruktur-Gesamtstruktur und fügen dieser die Benutzer oder Gruppen der Kunden-Gesamtstruktur hinzu.



Director kann eine solche Konfiguration mit mehrere Gesamtstrukturen unterstützen und die Sitzungen von mithilfe domänenlokaler Gruppen konfigurierten Benutzern überwachen.

1. Fügen Sie die folgenden Anwendungseinstellungen auf der Director-Website in der IIS-Verwaltungskonsole hinzu:

   ```
   Connector.ActiveDirectory.DomainLocalGroupSearch= true Connector.
       ActiveDirectory

   DomainLocalGroupSearchDomains= \<domain1\>,\<domain2\>
   ```

   <domain1><domain2> sind Namen der Gesamtstrukturen, in denen die domänenlokale Gruppe angesiedelt ist.

2. Weisen Sie die lokale Gruppe der Domäne den Bereitstellungsgruppen in Citrix Studio zu.
3. Starten Sie IIS neu und melden Sie sich erneut bei Director an, damit die Änderungen wirksam werden. Director kann dann die Sitzungen der Benutzer überwachen und anzeigen.

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
<!--NeedCopy-->
```

SiteAController und SiteBController sind die Adressen von Delivery Controllern aus zwei verschiedenen Sites.

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 auf dem VDA gesammelt und 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

> Wichtig:
>
> Zum Deaktivieren der Ansicht ausgeführter Anwendungen empfiehlt Citrix, dass beide Änderun-

> gen durchgeführt werden, damit die Daten im Aktivitätsmanager nicht angezeigt werden.

Konfigurieren der PIV-Smartcardauthentifizierung

June 27, 2024

In diesem Artikel wird die zum Aktivieren der Smartcardauthentifizierung auf dem Director-Server und in Active Directory erforderliche Konfiguration behandelt.

> Hinweis:
> Die Smartcardauthentifizierung wird nur für Benutzer aus derselben Active Directory-Domäne unterstützt.

Konfiguration des Director-Servers

Führen Sie die folgenden Konfigurationsschritte auf dem Director-Server aus:

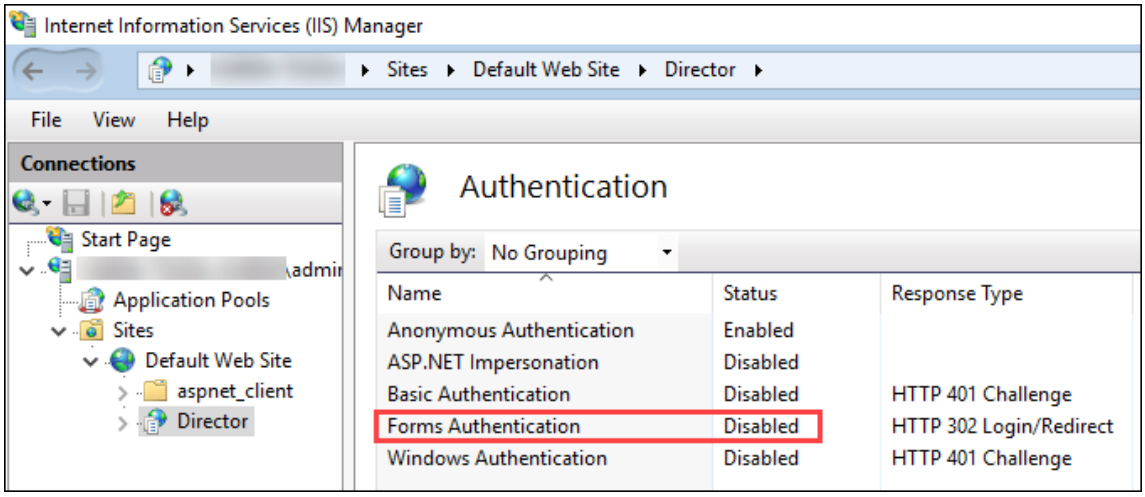
1. Installieren und aktivieren Sie die Clientzertifikatzuordnung-Authentifizierung. Folgen Sie den Anweisungen im Abschnitt **Client Certificate Mapping authentication using Active Directory** des Microsoft-Dokuments Client Certificate Mapping Authentication.
2. Deaktivieren Sie die Formularauthentifizierung in der Director-Site.

   Starten Sie IIS-Manager.

   Rufen Sie **Sites** > **Standardwebsite** > **Director** auf.

   Wählen Sie **Authentifizierung**.

   Klicken Sie mit der rechten Maustaste auf **Formularauthentifizierung** und wählen Sie **Deaktivieren**.



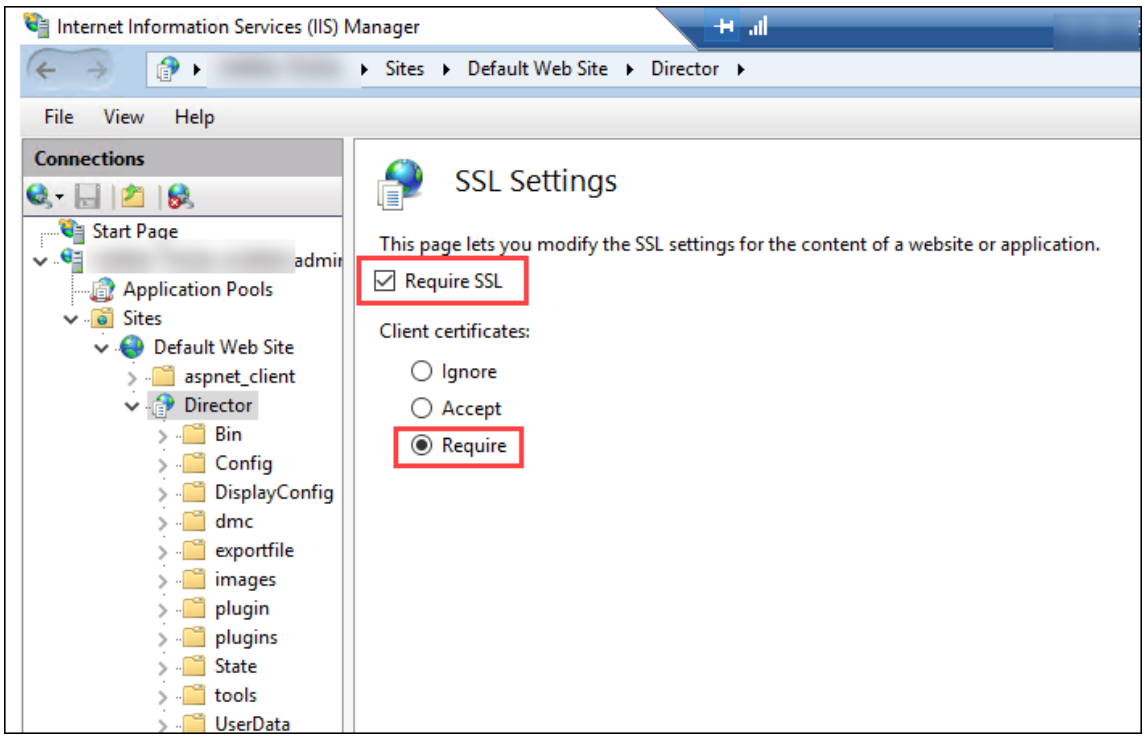
3. Konfigurieren Sie die Director-URL für das sicherere HTTPS-Protokoll (anstelle von HTTP) für die Clientzertifikatauthentifizierung.

   a) Starten Sie IIS-Manager.

   b) Rufen Sie **Sites** > **Standardwebsite** > **Director** auf.

   c) Wählen Sie **SSL-Einstellungen**.

   d) Wählen Sie **SSL erforderlich** und **Clientzertifikate** > **Erforderlich**.



4. Aktualisieren Sie web.config. Öffnen Sie die Datei web.config (in c:\inetpub\wwwroot\Director) in einem Texteditor.

Fügen Sie unter dem Element <system.webServer> das folgende Snippet als erstes untergeordnetes Element hinzu:

```
<defaultDocument>
   <files>
       <add value="LogOn.aspx"/>
   </files>
</defaultDocument>
```

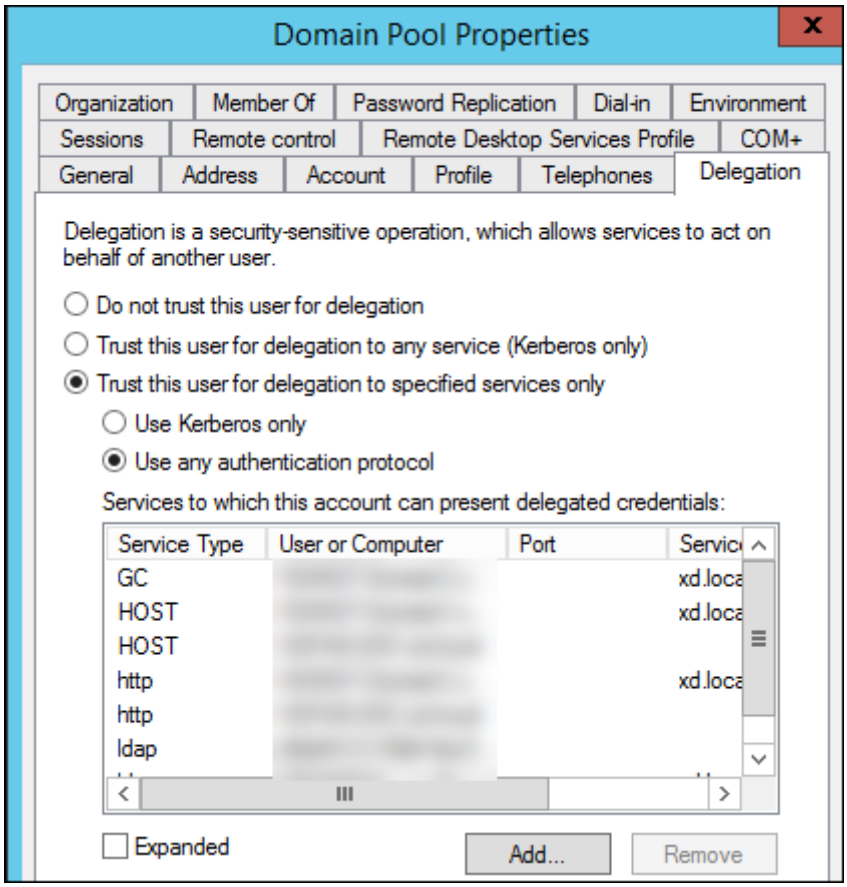
Active Directory-Konfiguration

Standardmäßig wird die Director-Anwendung mit der Identitätseigenschaft **Application Pool** ausgeführt. Die Smartcardauthentifizierung erfordert Delegierung, wofür die Director-Anwendungsidentität

Trusted Computing Base-Privilegien auf dem Servicehost haben muss.

Citrix empfiehlt die Erstellung eines eigenen Dienstkontos für Application Pool-Identität. Erstellen Sie das Dienstkonto und weisen Sie TCB-Privilegien zu (siehe Microsoft-Artikel Protocol Transition with Constrained Delegation Technical Supplement).

Weisen Sie das neu erstellte Dienstkonto dem Director-Anwendungspool zu. Die folgende Abbildung zeigt das Dialogfeld "Eigenschaften"des Beispieldienstkontos, "Domain Pool".

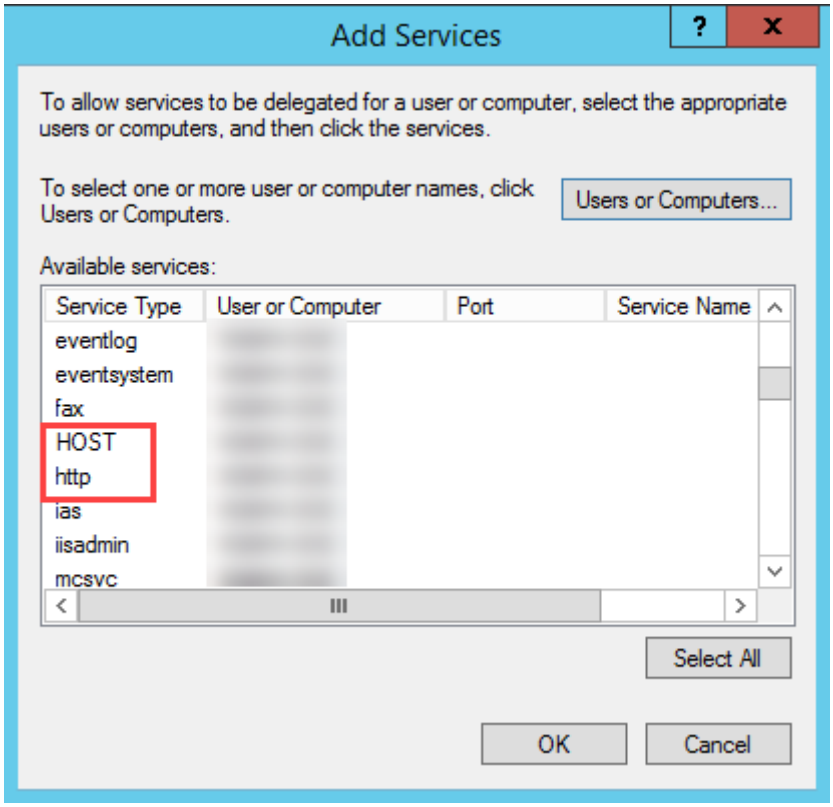


Konfigurieren Sie die folgenden Dienste für dieses Konto:

- Delivery Controller: HOST, http
- Director: HOST, http
- Active Directory: GC, LDAP

Führen Sie hierfür folgende Schritte aus:

1. Klicken Sie im Dialogfeld "Benutzerkontoeigenschaften"auf **Hinzufügen**.
2. Klicken Sie im Dialogfeld **Dienste hinzufügen** auf "Benutzer"oder "Computer".
3. Wählen Sie den Delivery Controller-Hostnamen.
4. Wählen Sie in der Liste **Verfügbare Dienste** den Diensttyp **HOST und HTTP**.



Fügen Sie auf ähnliche Weise Diensttypen für **Director**- und **Active Directory**-Hosts hinzu.

Firefox-Konfiguration

Installieren Sie zur Verwendung von Firefox den auf OpenSC 0.17.0 verfügbaren PIV-Treiber. Anweisungen zu Installation und Konfiguration finden Sie unter Installing OpenSC PKCS#11 Module in Firefox, Step by Step.
Informationen zur Verwendung der Authentifizierung per Smartcard in Director finden Sie unter Verwendung von Director mit Authentifizierung mit PIV-Smartcards.

Konfigurieren der Netzwerkanalyse

March 4, 2024

> **Hinweis:**
> Die Verfügbarkeit dieser Funktion richtet sich nach der Lizenzierung und den Administratorberechtigungen.

Director ermöglicht in Kombination mit Citrix ADM die Netzwerkanalyse und Leistungsverwaltung:

- Die Netzwerkanalyse nutzt HDX Insight-Berichte aus Citrix ADM 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:

- In der Trendansicht werden Anmeldedaten für HDX-Verbindungen für VDAs vor Version 7 nicht gesammelt. Für frühere VDAs werden die Diagrammdaten als 0 angezeigt.

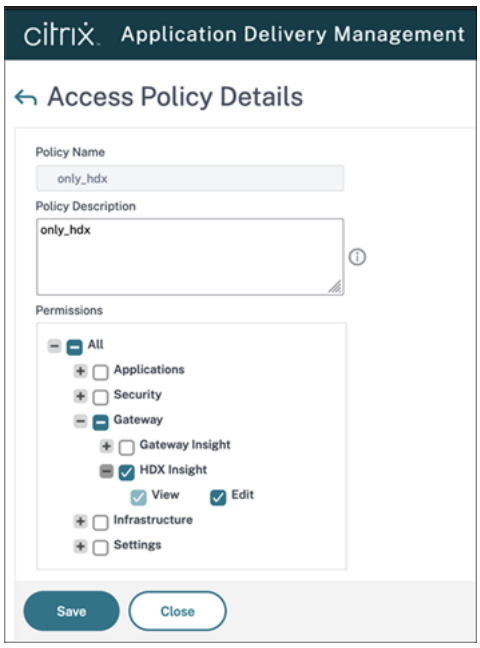
Um die Netzwerkanalyse zu aktivieren, müssen Sie Citrix ADM in Director installieren und konfigurieren. Director erfordert Citrix ADM Version 11.1 Build 49.16 oder höher. MAS ist ein virtuelles Gerät, das unter Citrix XenServer ausgeführt wird. Mit der Netzwerkanalyse sammelt Director Daten zur Bereitstellung.

Weitere Informationen finden Sie in der Dokumentation zu Citrix ADM.

> **Hinweis:**
> Citrix NetScaler Insight Center wird seit 15. Mai 2018 nicht mehr gewartet. Weitere Informationen finden Sie in der Citrix Produktmatrix. Integrieren Sie Director und Citrix ADM für die Netzwerkanalyse. Informationen zum Migrieren von NetScaler Insight Center zu Citrix ADM finden Sie unter Migrate from NetScaler Insight Center to Citrix ADM.

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 Citrix ADM, den Benutzernamen, das Kennwort und den oder HTTPS-Verbindungstyp (HTTPS is HTTP vorzuziehen) ein und wählen Sie die Citrix ADM-Integration.
3. Melden Sie sich zum Prüfen der Änderungen ab und wieder an.

> **Hinweis:**
>
> Aus Sicherheitsgründen wird empfohlen, eine benutzerdefinierte Rolle für die ADM-Integration mit Director zu erstellen, die ausreichende Berechtigungen für den Zugriff auf HDX Insight hat.



Weitere Informationen finden Sie unter Zugriffsrichtlinien konfigurieren.

Delegierte Administration und Director

September 21, 2021

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, 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 Maschinen mit Einzelsitzungs-OS verwenden. Kann nicht auf das Dashboard, Trends, Warnungen oder Filteransichten zugreifen. Kann keine Energieoptionen auf Maschinen mit Multisitzungs-OS verwenden.
Maschinenkatalogadministrator	Kann nur auf die Seite “Maschinendetails” zugreifen (maschinenbasierte Suche).
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:

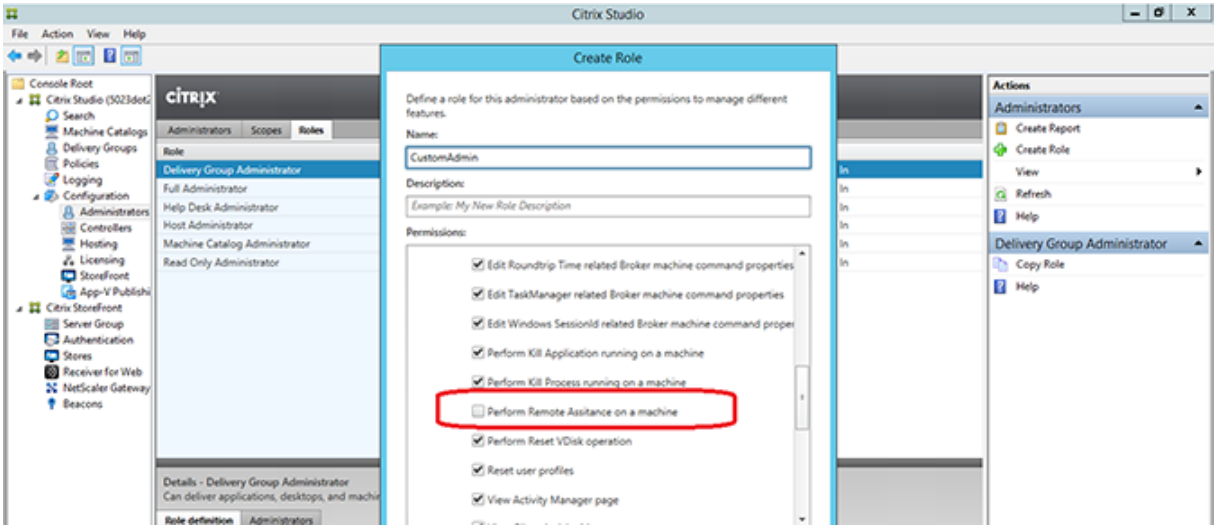
- Delivery Controller-Berechtigung zur Anmeldung bei Director –mindestens Lesezugriff im Administratormodus
- Berechtigungen für Bereitstellungsgruppen zum Anzeigen der zu diesen gehörigen Daten in Director –mindestens Lesezugriff

Alternativ können Sie eine benutzerdefinierte Rolle erstellen, indem Sie eine vorhandene Rolle kopieren und dieser zusätzliche Berechtigungen für die verschiedenen Ansichten erteilen. Sie können 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

January 24, 2022

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.

Grenzwerte für Anwendungspoolrecycling

Sie können die folgenden Grenzwerte für das Anwendungspoolrecycling festlegen:

- Virtuelles Arbeitsspeicherlimit: 4.294.967.295
- Privates Arbeitsspeicherlimit: Die Größe des physischen Speichers des StoreFront-Servers
- Anforderungslimit: 4.000.000.000

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 Citrix ADC mit TLS und nicht IPsec schützen.

Informationen zum Schützen der Kommunikation zwischen Director und Citrix Virtual Apps and Desktops-Servern (für die Überwachung und Berichte) finden Sie unter Data Access Security.

Informationen zum Schützen der Kommunikation zwischen Director und Citrix ADC (für Citrix 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.

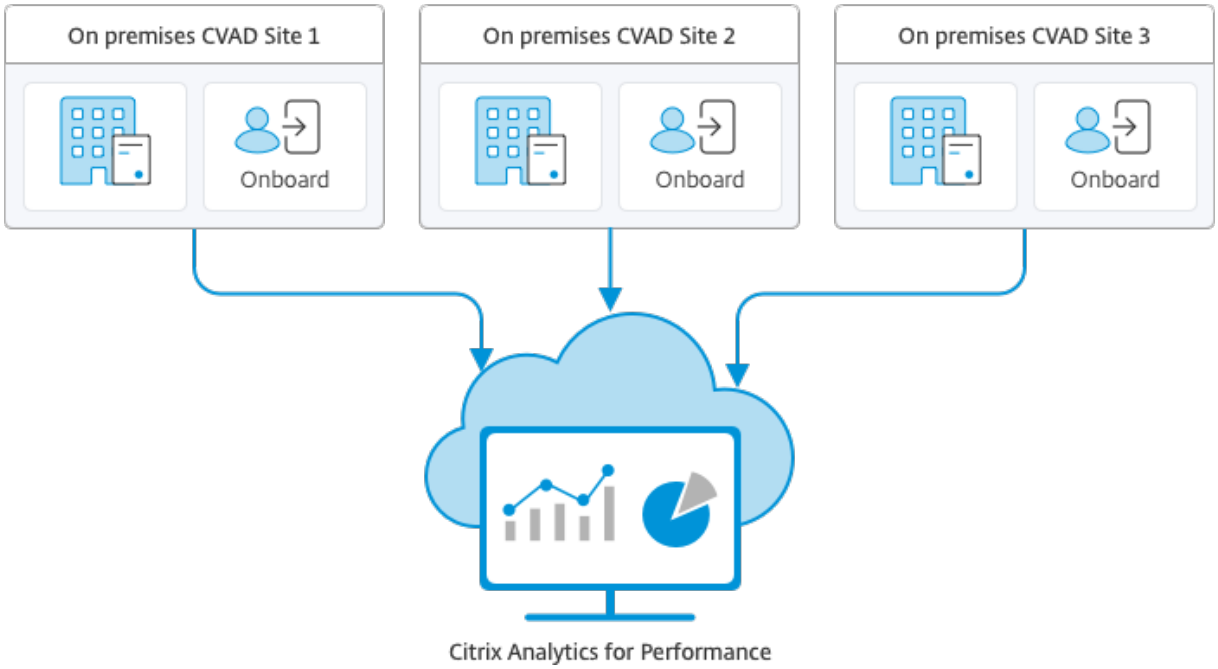
On-Premises-Sites mit Citrix Analytics for Performance konfigurieren

June 27, 2024

Citrix Analytics for Performance (Leistungsanalyse) ist die umfassende Lösung zur Leistungsüberwachung des Citrix Analytics Cloud Service. Die Leistungsanalyse bietet Metriken zur besseren Beurteilung und Analyse der Leistung. Mit der Leistungsanalyse können Sie die Nutzungs- und Leistungskennzahlen von Citrix Virtual Apps and Desktops-Sites in Ihrer Organisation überwachen und anzeigen.

Weitere Informationen zur Leistungsanalyse finden Sie unter Leistungsanalyse.

Sie können Leistungsdaten von Ihrer Site an Citrix Analytics for Performance in Citrix Cloud senden, um die erweiterten Leistungsanalysefunktionen zu nutzen. Zur Anzeige und Nutzung der Leistungsanalyse müssen Sie zunächst auf der Registerkarte **Analytics** in **Director** die on-premises Sites mit Citrix Analytics for Performance konfigurieren. Dieses Feature erfordert Director ab Version 1909 und Delivery Controller und VDAs ab Version 1906.



Beim sicheren Datenzugriff der Leistungsanalyse werden keine Daten von Citrix Cloud an die On-Premises-Umgebung übertragen.

Voraussetzungen

Für das Konfigurieren von Citrix Analytics for Performance in Director müssen keine neuen Komponenten installiert werden. Vergewissern Sie sich, dass die folgenden Anforderungen erfüllt sind:

- Delivery Controller und Director liegen in Version 1912 CU2 oder höher vor. Weitere Informationen finden Sie in der Featurekompatibilitätsmatrix.

> **Hinweis:**
>
> - Das Konfigurieren Ihrer On-Premises-Site mit Citrix Analytics for Performance von Director aus schlägt möglicherweise fehl, wenn der Delivery Controller eine Version von Microsoft .NET Framework vor 4.8 ausführt. Aktualisieren Sie als Workaround das .NET Framework für den Delivery Controller auf Version 4.8. LCM-9255.
> - Wenn Sie eine On-Premises-Site, auf der Citrix Virtual Apps and Desktops Version 2012 ausgeführt wird, mit Citrix Analytics für Leistung über Director konfigurieren, schlägt die Konfiguration möglicherweise nach ein paar Stunden oder nach einem Neustart des Citrix Überwachungsdiensts auf dem Delivery Controller fehl. Auf der Registerkarte "Analytics"wird in diesem Fall der Status "Nicht verbunden"angezeigt. Erstellen Sie als Workaround einen Verschlüsselungsordner in der Registrierung auf dem Delivery Controller. Ort: HKEY_LOCAL_MACHINE\Software\Citrix\XDservices\Monitor. Ordnername:

> Encryption. Vergewissern Sie sich, dass das CitrixMonitor-Konto über Vollzugriff auf den Verschlüsselungsordner verfügt. Starten Sie den Citrix Monitordienst neu.DIR-14324

- Nur Volladministratoren können auf die Registerkarte **Analytics** zugreifen und die Konfiguration ausführen.
- Alle Delivery Controller und die Maschinen mit installiertem Director haben einen ausgehenden Internetzugriff, damit Leistungsmetriken durch die Leistungsanalyse erfasst werden können. Vor allem die folgenden URLs müssen erreichbar sein:
  - Citrix Schlüsselregistrierung: `https://*.citrixnetworkapi.net/`
  - Citrix Cloud: `https://*.citrixworkspacesapi.net/`
  - Citrix Analytics: `https://*.cloud.com/`
  - Microsoft Azure: `https://*.windows.net/`

    Falls Delivery Controller und Director-Maschinen in einem Intranet sind und der ausgehende Internetzugriff über einen Proxyserver erfolgt, muss Folgendes gelten:
- Der Proxyserver die oben aufgeführten URLs zulassen.
- Fügen Sie die folgende Konfiguration in den Dateien web.config und citrix.monitor.exe.config von Director hinzu. Vergewissern Sie sich, dass Sie diese Konfiguration in den **Konfigurations-Tags** hinzufügen:

```
<system.net>
    <defaultProxy>
        <proxy  usesystemdefault = "false"  proxyaddress = "http
            ://<your_proxyserver_address>:80" bypassonlocal = "
            true"  />
    </defaultProxy>
</system.net>  -  Die web.config-Datei für Director ist auf der
    Maschine mit Director im Verzeichnis `C:\inetpub\wwwroot\
    Director\web.config`.  -  Die Datei citrix.monitor.exe.config
    ist im Verzeichnis `C:\Program Files\Citrix\Monitor\Service\
    Citrix.Monitor.exe.Config` auf der Maschine mit dem Delivery
    Controller.
```

  Diese Einstellung wird von Microsoft in IIS bereitgestellt. Weitere Informationen finden Sie unter `https://docs.microsoft.com/en-us/dotnet/framework/network-programming/proxy-configuration`.

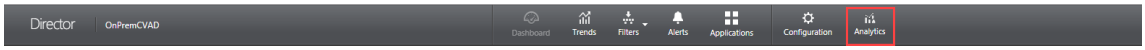
  Das Feld **defaultproxy** in der Konfigurationsdatei steuert den ausgehenden Zugriff von Director und den Überwachungsdienst. Für die Konfiguration und Kommunikation mit der Leistungsanalyse muss das Feld **defaultproxy** auf **true** gesetzt sein. Es ist möglich, dass die geltenden Richtlinien dieses Feld auf “false”setzen. In diesem Fall müssen Sie das Feld manuell auf “true”setzen. Erstellen Sie ein Backup der Konfigurationsdateien, bevor Sie die Änderungen machen. Starten Sie den Überwachungsdienst auf dem Delivery Controller neu, damit die Änderungen umgesetzt werden.

- Sie haben einen aktiven Citrix Cloud-Anspruch auf Citrix Analytics for Performance.
- Ihr Citrix Cloud-Konto ist ein Administratorkonto mit Berechtigungen für die Produktregistrierung. Weitere Hinweise zu Administratorrechten finden Sie unter Ändern von Administratorberechtigungen.

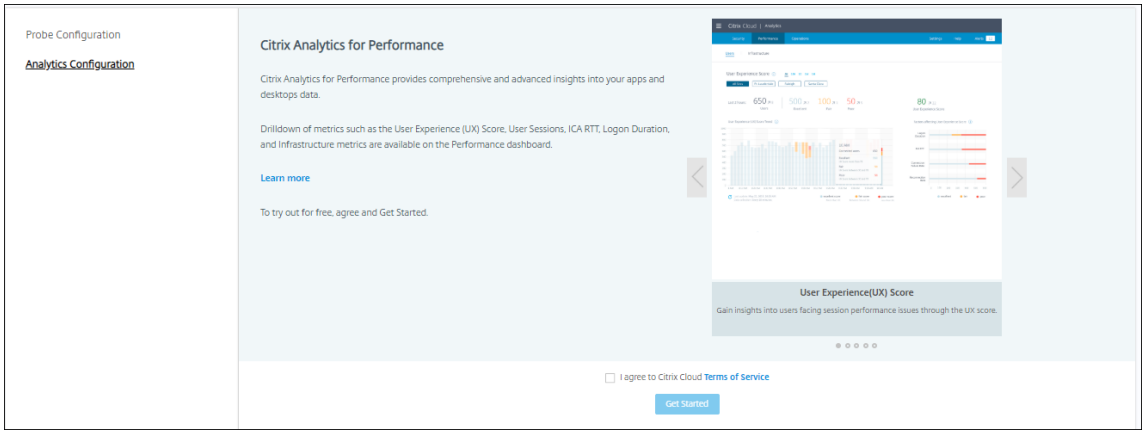
Konfigurationsschritte

Nachdem Sie die Voraussetzungen überprüft haben, gehen Sie folgendermaßen vor:

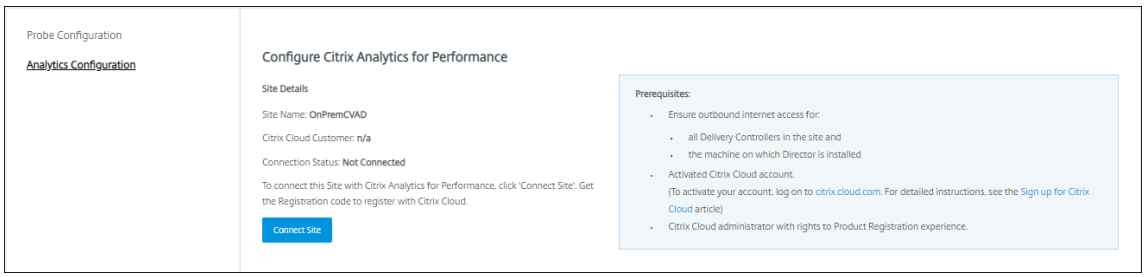
1. Melden Sie sich bei Director als Volladministrator an und wählen Sie die Site aus, für die Sie die Leistungsanalyse konfigurieren möchten.
2. Klicken Sie auf die Registerkarte **Analytics**. Die Seite **Konfiguration** wird angezeigt.



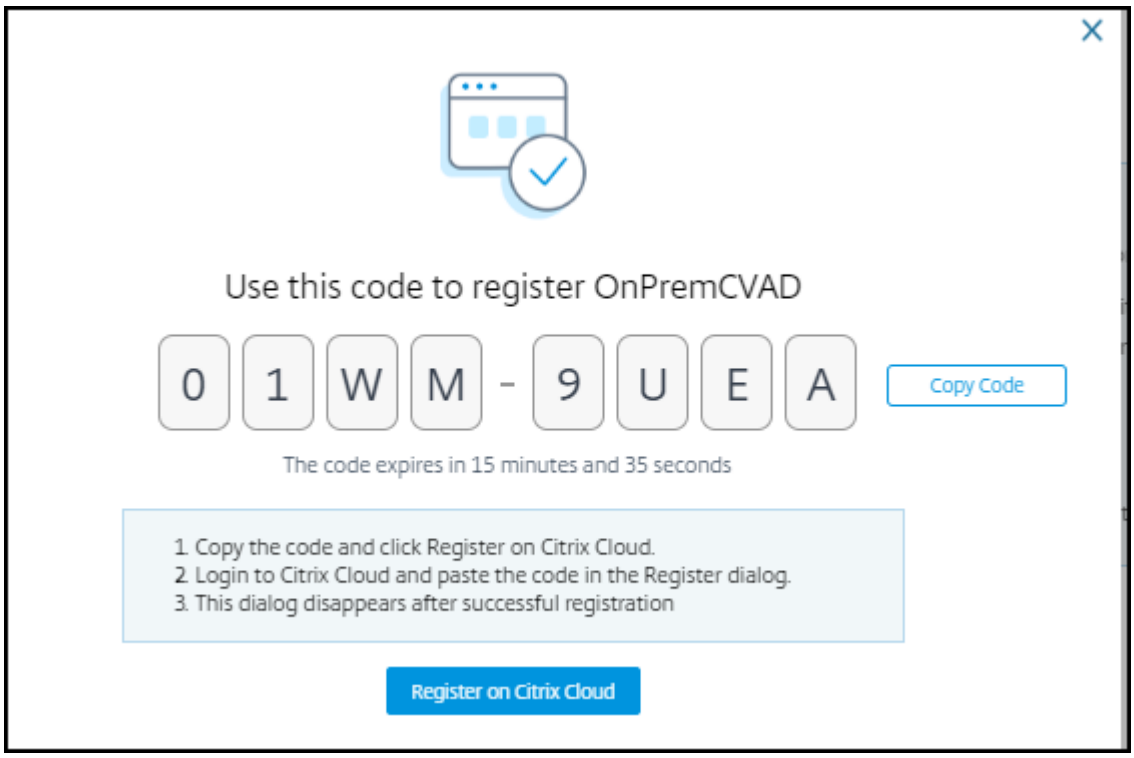
3. Lesen Sie die Anweisungen, bestätigen Sie die Nutzungsbedingungen und klicken Sie auf **Erste Schritte**.



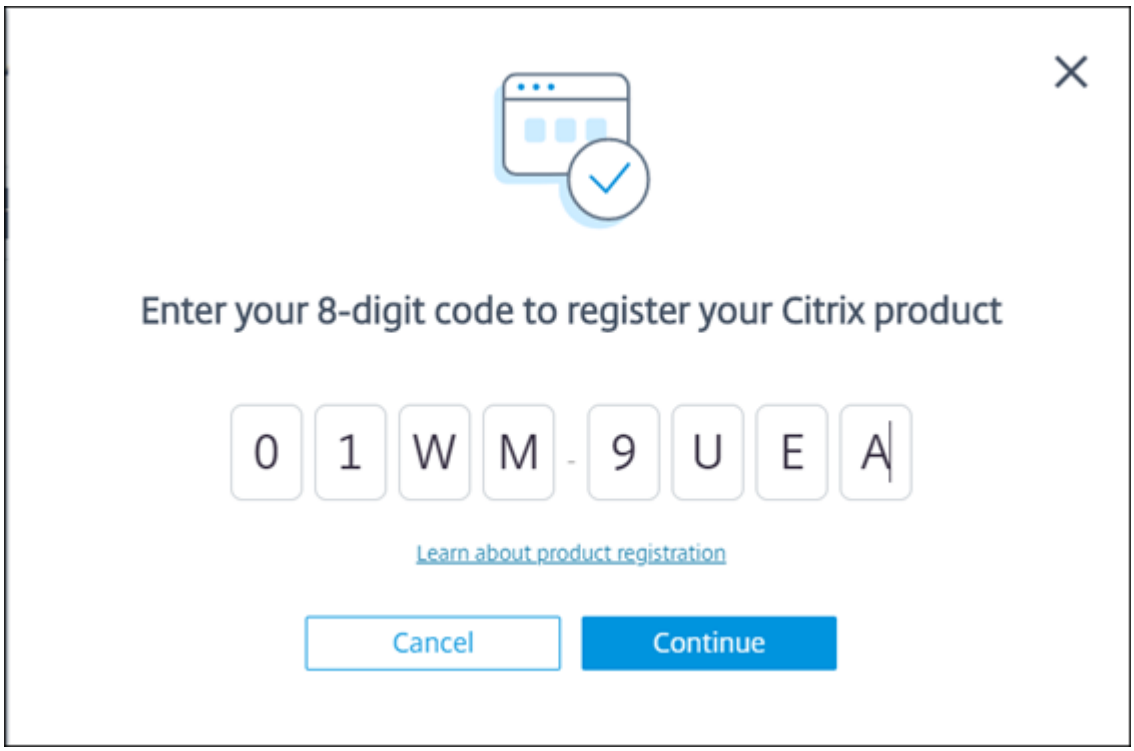
4. Vergewissern Sie sich, dass alle Voraussetzungen erfüllt sind. Überprüfen Sie die Details zur Site.
5. Klicken Sie auf **Site verbinden**, um die Konfiguration zu starten.



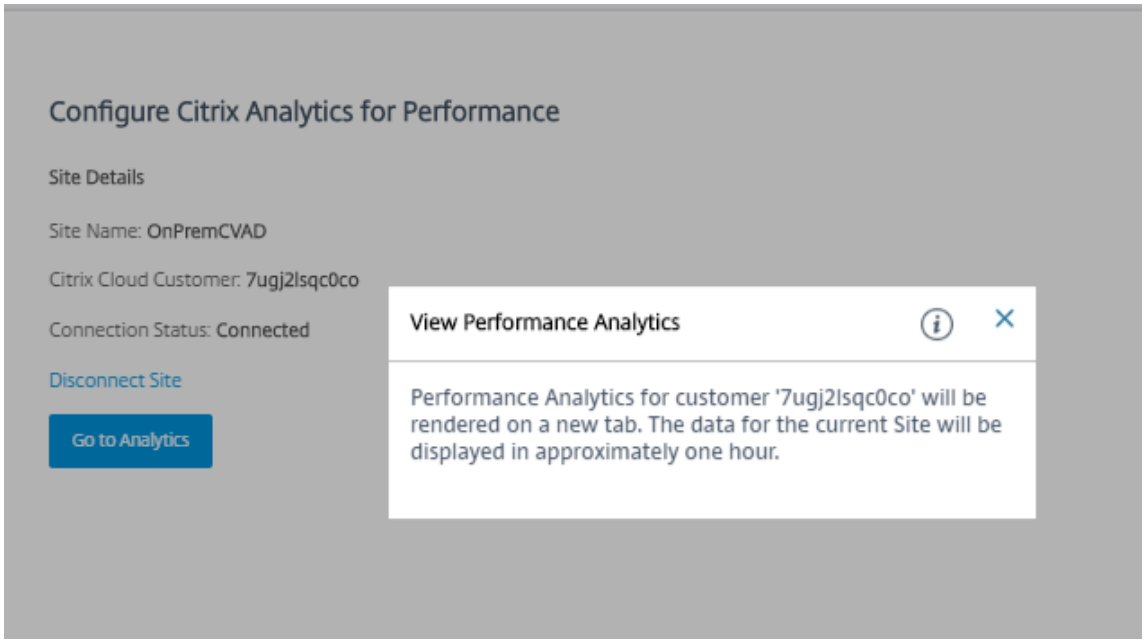
6. Zur Registrierung der Site bei Citrix Cloud wird ein 8-stelliger Registrierungscode generiert.



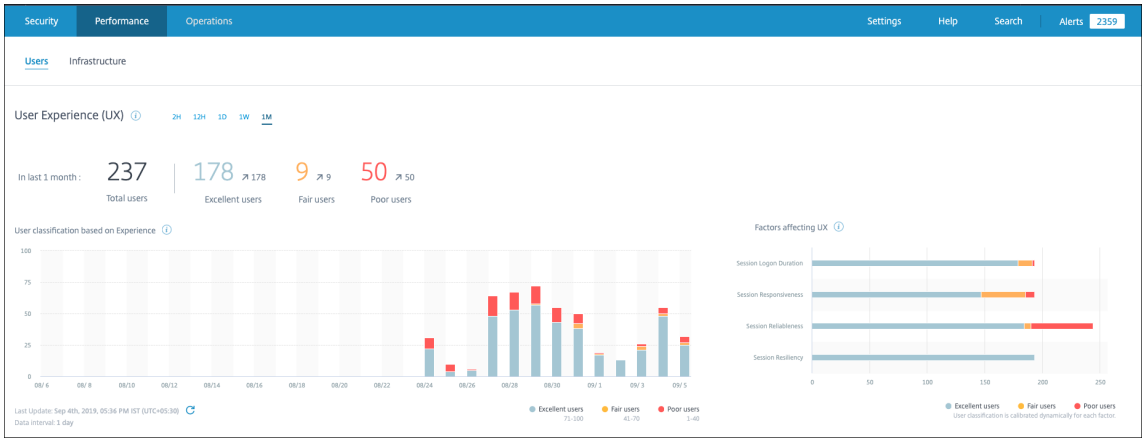
7. Klicken Sie auf **Code kopieren** und dann auf **Bei Citrix Cloud registrieren**.
8. Sie werden zur Registrierungs-URL in Citrix Cloud weitergeleitet. Melden Sie sich mit Ihren Citrix Cloud-Anmeldeinformationen an und wählen Sie Ihren Kunden aus.
9. Fügen Sie den kopierten Registrierungscode in Citrix Cloud auf der Seite "Produktregistrierungen"ein. Klicken Sie auf **Weiter**, um sich zu registrieren. Überprüfen Sie die Registrierungsdetails und klicken Sie auf **Registrieren**.



10. Ihre On-Premises-Site wird bei Citrix Cloud registriert. Klicken Sie in **Director** auf der Registerkarte **Analytics** auf **Gehe zu Analytics**.



11. Die Leistungsanalyse wird in einer neuen Browserregisterkarte geöffnet.



Bei Ablauf Ihrer Citrix Cloud-Sitzung werden Sie eventuell zur Anmeldeseite von Citrix.com oder My Citrix umgeleitet.

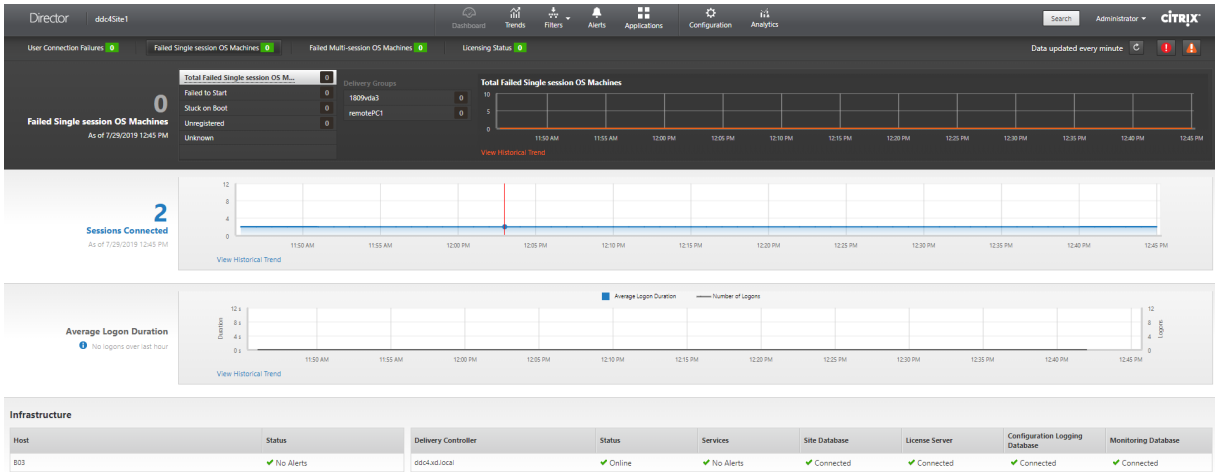
12. Um mehrere Sites für die Leistungsanalyse zu registrieren, wiederholen Sie für jede Site die vorherigen Konfigurationsschritte in Director. Die Metriken für alle konfigurierten Sites werden im Leistungsanalyse-Dashboard angezeigt.
13. Klicken Sie auf **Site trennen**, um Ihre Site von Citrix Cloud zu trennen. Diese Option löscht die vorhandene Konfiguration.

> **Hinweise:**
>
> Beim ersten Konfigurieren einer Site kann die Verarbeitung der Site-Ereignisse rund eine Stunde dauern, sodass Metriken verzögert im Leistungsanalyse-Dashboard angezeigt werden. Danach werden die Ereignisse in regelmäßigen Abständen aktualisiert.
>
> Nach der Trennung wird die Datenübertragung vom alten Konto für einige Zeit fortgesetzt, bis die Ereignisse aus dem neuen Konto übertragen werden. Nach Beendigung der Datenübertragung sind die Analysedaten für das alte Konto noch eine Stunde im Leistungsanalyse-Dashboard zu sehen.
>
> Sobald der Anspruch auf den Citrix Analytics-Dienst erlischt, werden Site-Metriken noch für maximal einen Tag an die Leistungsanalyse gesendet.

Siteanalyse

March 15, 2022

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 Maschinen mit Einzelsitzungs-OS und fehlgeschlagene Maschinen mit Multisitzungs-OS	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 Maschinen mit Multisitzungs-OS wird auch das Erreichen der maximalen Last angegeben.

Bereich	Beschreibung
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. Der unter **Delivery Controller** > **Details** > **Produktedition** angezeigte Lizenzstatus **PLT** bedeutet **Premium** und nicht **Platinum**.
Verbundene Sitzungen	Verbunden Sitzungen in allen Bereitstellungsgruppen in den letzten 60 Minuten.
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.

Bereich	Beschreibung
Infrastruktur	Liste der zu der Siteinfrastruktur gehörigen Hosts und Controller. Auf Citrix Hypervisor 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 im Abschnitt "XenCenter Performance Alerts"der Dokumentation zu Citrix Hypervisor.

> **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.
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**.

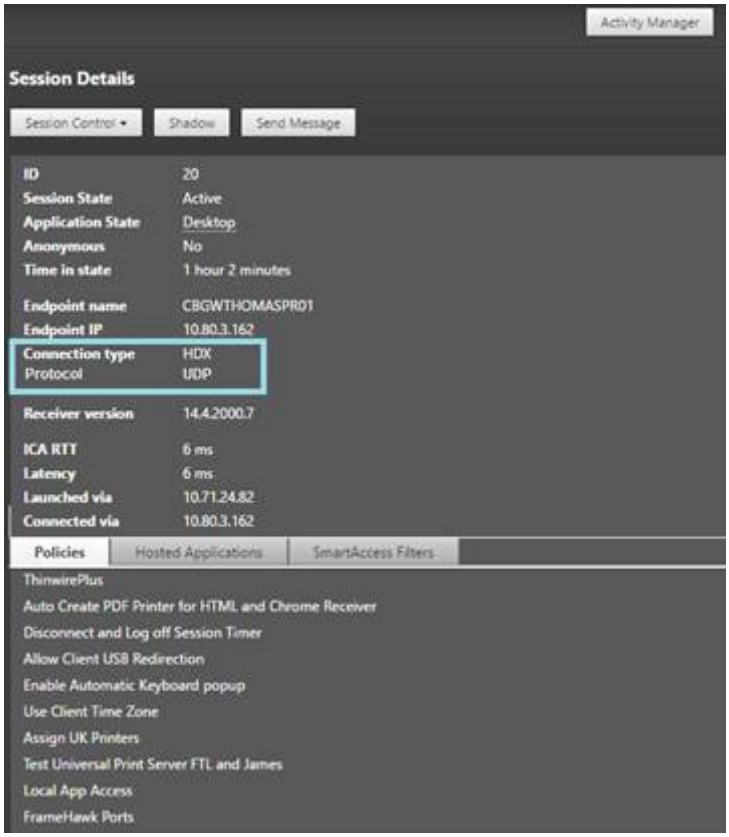
> **Hinweis:**
> Wenn auf dem Benutzergerät eine ältere Virtual Delivery Agent-Version ausgeführt wird, z. B. eine VDA-Version vor 7 oder ein VDA für Linux, kann Director keine vollständigen Sitzungsinformationen anzeigen. Stattdessen wird gemeldet, dass die Informationen nicht verfügbar sind.

Einschränkung für Desktopzuweisungsregeln:
Citrix Studio ermöglicht die Zuordnung mehrerer Desktopzuweisungsregeln (DAR) für verschiedene Benutzer oder Benutzergruppen zu einem VDA in einer Bereitstellungsgruppe. In StoreFront wird der zugewiesene Desktop unter dem zugehörigen **Anzeigenamen** gemäß der Desktopzuordnungsregel für den angemeldeten Benutzer angezeigt. Director unterstützt keine Desktopzuordnungsregeln und zeigt den zugewiesenen Desktop unabhängig vom angemeldeten Benutzer unter dem Namen der Bereitstellungsgruppe an. Sie können daher keinen bestimmten Desktop einer Maschine in Director zuordnen.
Mit folgendem PowerShell-Befehl können Sie den in StoreFront angezeigten, zugewiesenen Desktop dem in Director angezeigten Bereitstellungsgruppennamen zuordnen:

```
Get-BrokerDesktopGroup | Where-Object {
  \$\_.Uid -eq \(Get-BrokerAssignmentPolicyRule | Where-Object {
  \$\_.PublishedName -eq \"\<Name on StoreFront\>\"  }
 ).DesktopGroupUid  }
  | Select-Object -Property Name, Uid
```

Sitzungstransportprotokoll

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.

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	1000.000
CSV	100.000 (10.000.000 auf Registerkarte **Sitzungen**)	UI.ExportCsvDrilldownLimit	10.000.000

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 die Felder “UI.ExportPdfDrilldownLimit”, “UI.ExportExcelDrilldownLimit”bzw. “UI.ExportCsvDrilldownLimit”nach Bedarf.

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 sind für Maschinen mit Einzelsitzungs-OS verfügbar, aber möglicherweise nicht für Maschinen mit Multisitzungs-OS.

> **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.

Befehl	Funktion
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.

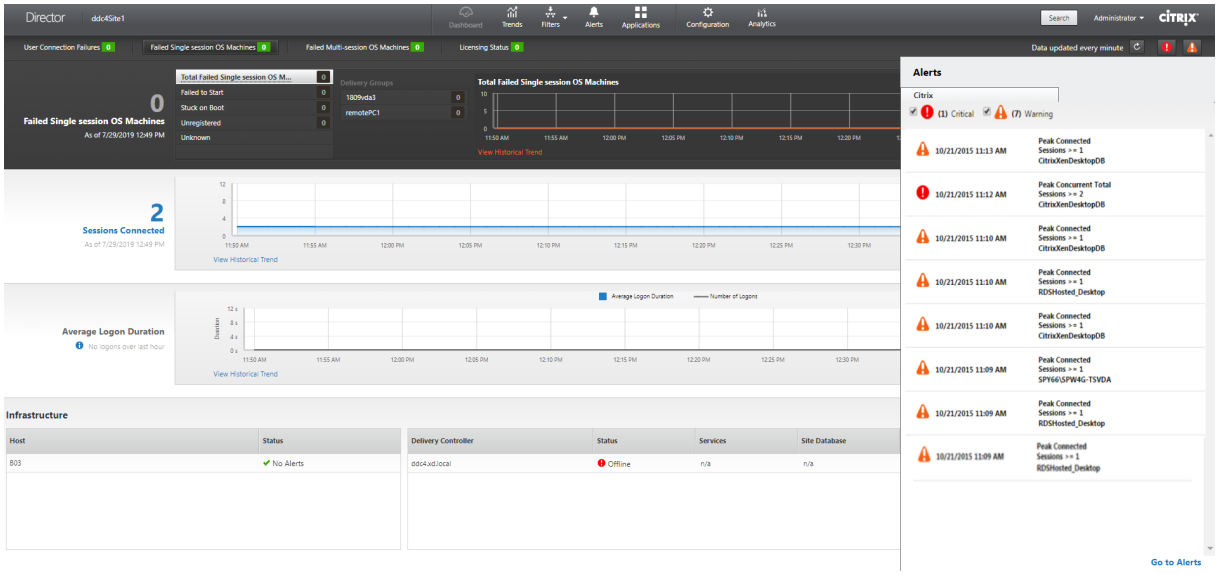
Anwendungsanalyse

Auf der Registerkarte **Anwendungen** werden konsolidierte Anwendungsdaten zur effizienten Analyse und Verwaltung der Anwendungsleistung angezeigt. Sie erhalten hier wertvolle Einblicke in die Integrität und Nutzung aller in der Site veröffentlichten Anwendungen. Die Ansicht enthält Anwendungstestergebnisse, die Zahl der Instanzen pro Anwendung und ähnliche Kennzahlen sowie Informationen zu Fehlern bei veröffentlichten Anwendungen. Weitere Informationen finden Sie unter Problembehandlung bei Anwendungen im Abschnitt **Anwendungsanalyse**.

Warnungen und Benachrichtigungen

May 10, 2023

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 **Premium**-Lizenz zur Verfügung. Die Anzeige von Warnungen wird jede Minute automatisch aktualisiert und kann bei Bedarf auch manuell aktualisiert werden.

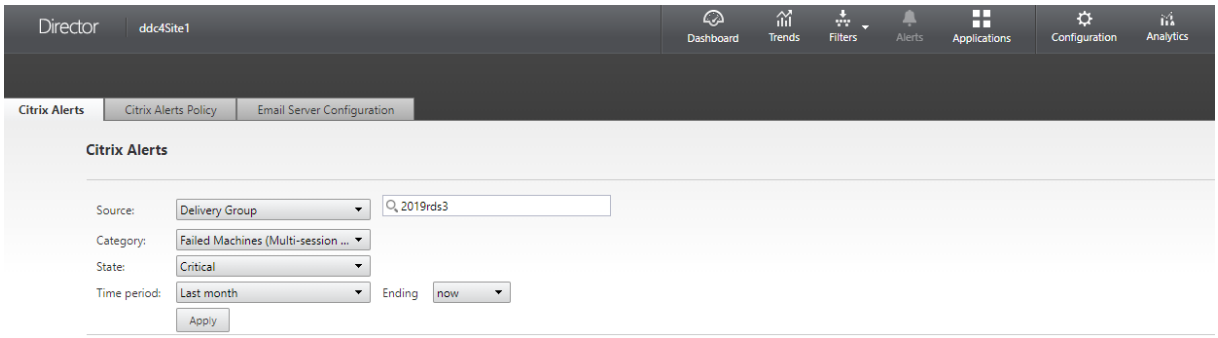


Eine Warnung (gelbes Dreieck) zeigt an, dass der Schwellenwert einer Bedingung erreicht oder überschritten wurde.

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 Maschinen mit Multisitzungs-OS für eine bestimmte Bereitstellungsgruppe im vergangenen Monat oder alle Warnungen für einen bestimmten Benutzer anzeigen. Weitere Informationen finden Sie unter Exportieren von Berichten.



Citrix Warnungen

Citrix Warnungen in Director stammen von Citrix Komponenten. Sie können Citrix Warnungen in Director über **Warnungen** > **Citrix Benachrichtigungsrichtlinie** konfigurieren. Im Rahmen der Konfig-

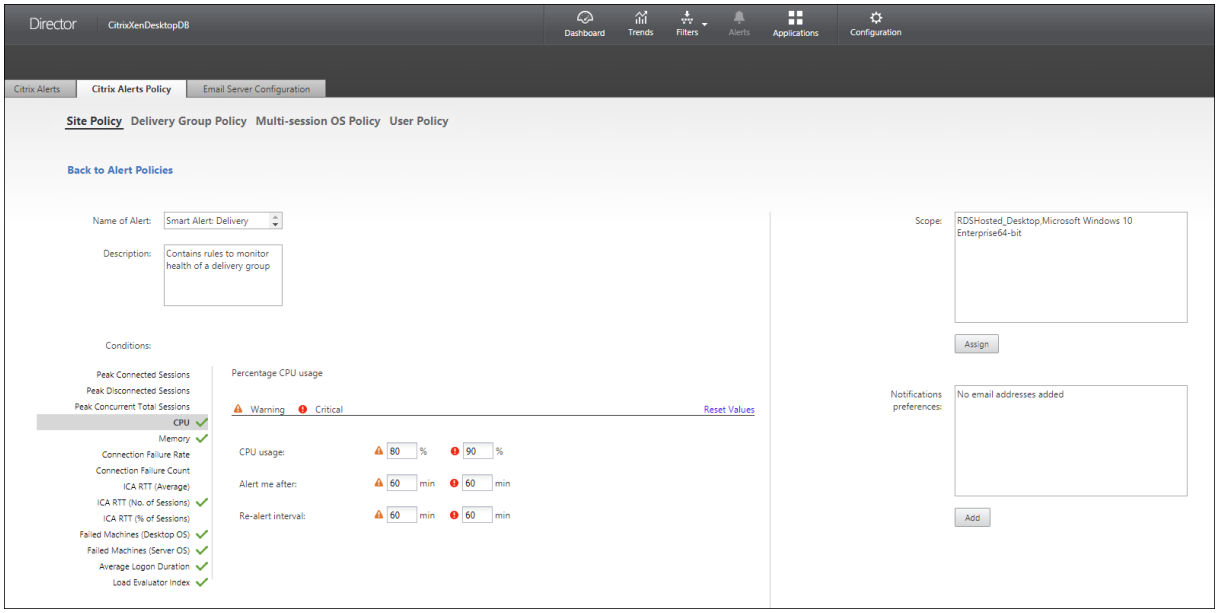
uration können Sie den Versand von Benachrichtigungen per E-Mail an Personen und Gruppen festlegen, wenn die Schwellenwerte überschritten werden. Weitere Informationen zum Einrichten von Citrix Warnungen finden Sie unter Erstellen von Benachrichtigungsrichtlinien.

Intelligente Benachrichtigungsrichtlinien

Eine Reihe integrierter Benachrichtigungsrichtlinien mit vordefinierten Schwellenwerten ist für Bereitstellungsgruppen und Multisitzungs-OS-VDAs verfügbar. Für dieses Feature sind Director und Delivery Controller ab Version 7.18 erforderlich. Sie können die Schwellenwertparameter der integrierten Benachrichtigungsrichtlinien unter **Warnungen** > **Citrix Benachrichtigungsrichtlinie** ändern.
Diese Richtlinien werden erstellt, wenn mindestens ein Warnungsziel –eine Bereitstellungsgruppe oder ein Multisitzungs-OS-VDA –in der Site vorhanden ist. Außerdem werden integrierte Benachrichtigungsrichtlinien automatisch neuen Bereitstellungsgruppen und Multisitzungs-OS-VDAs hinzugefügt.

Wenn Sie Director und Ihre Site aktualisieren, werden die Benachrichtigungsrichtlinien der älteren Director-Instanz übernommen. Integrierte Benachrichtigungsrichtlinien werden nur erstellt, wenn die Überwachungsdatenbank keine entsprechenden Warnmeldungsregeln enthält.

Informationen zu den Schwellenwerten der integrierten Benachrichtigungsrichtlinien finden Sie unter Bedingungen für Benachrichtigungsrichtlinien.



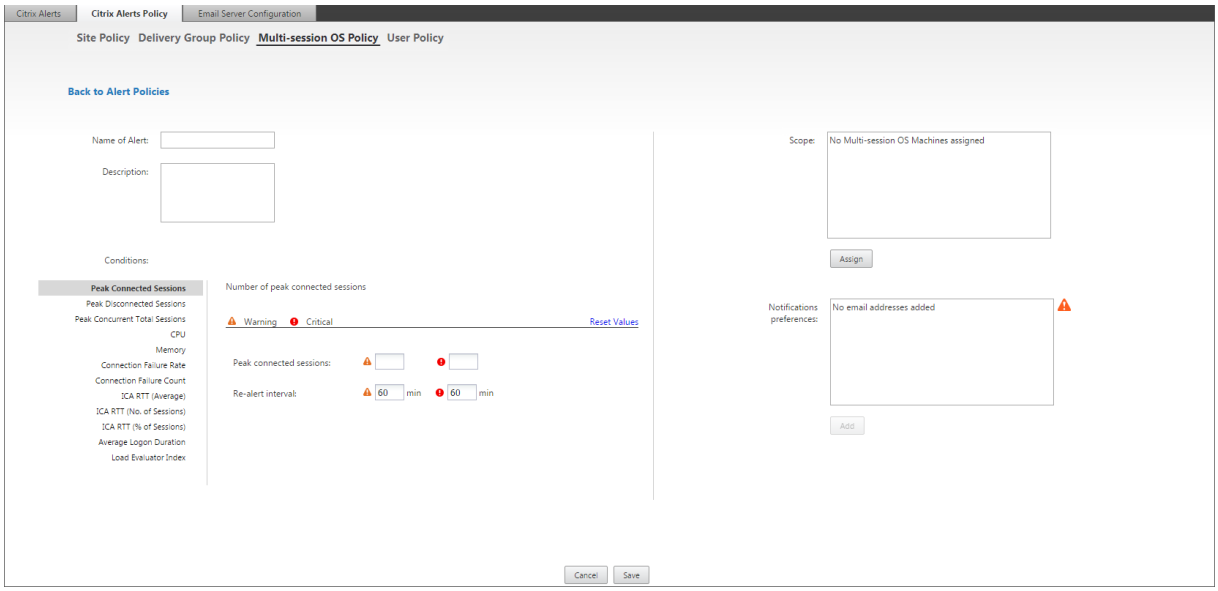
SCOM-Warnungen

Warnungen von Microsoft System Center 2012 Operations Manager (SCOM) enthalten detaillierte Angaben zu Datencenterintegrität und Leistung in Director. Weitere Informationen finden Sie unter

Konfigurieren der SCOM-Integration.

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 “Multisitzungs-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 Benachrichti-

gungsrichtlinien müssen Sie auf der Registerkarte **E-Mail-Serverkonfiguration** einen E-Mail-Server angeben.

7. Klicken Sie auf **Speichern**.

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

Nachfolgend werden die Warnmeldungskategorien, empfohlene Maßnahmen zur Problembehandlung und Bedingungen für integrierte Richtlinien (sofern definiert) aufgeführt. Die integrierten Benachrichtigungsrichtlinien sind für Warnungsintervalle von 60 Minuten definiert.

Max. 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, falls erforderlich, neue Maschinen hinzu.

Max. 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, falls erforderlich, ab.

Max. gleichzeitiger Sitzungen insgesamt

- 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, falls erforderlich, ab.

CPU

Der Prozentsatz der CPU-Auslastung umfasst die gesamte Auslastung auf dem VDA, einschließlich Prozesse. Detaillierte Informationen zur CPU-Auslastung durch einzelne Prozesse erhalten Sie auf der Seite **Maschinendetails** des jeweiligen VDAs.

- Rufen Sie hierzu **Maschinendetails > Historische Auslastung anzeigen > Top-10-Prozesse** auf. Die Prozessüberwachungsrichtlinie muss aktiviert sein, damit die Ressourcennutzung auf Prozessebene erfasst wird.
- Beenden Sie, falls erforderlich, den Prozess.
- Beim 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 Einstellungen der Überwachungsrichtlinie.

Bedingungen für intelligente Benachrichtigungsrichtlinien:

- **Bereich:** Bereitstellungsgruppe, Multisitzungs-OS
- **Schwellenwerte:** Warnung - 80 %, Kritisch - 90 %

Speicher

Der Prozentsatz der Speicherauslastung umfasst die gesamte Auslastung auf dem VDA, einschließlich Prozesse. Detaillierte Informationen zur Speicherauslastung durch einzelne Prozesse erhalten Sie auf der Seite **Maschinendetails** des jeweiligen VDAs.

- Rufen Sie hierzu **Maschinendetails > Historische Auslastung anzeigen > Top-10-Prozesse** auf. Die Prozessüberwachungsrichtlinie muss aktiviert sein, damit die Ressourcennutzung auf Prozessebene erfasst wird.
- Beenden Sie, falls erforderlich, den Prozess.
- Beim 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.

Bedingungen für intelligente Benachrichtigungsrichtlinien:

- **Bereich:** Bereitstellungsgruppe, Multisitzungs-OS
- **Schwellenwerte:** Warnung - 80 %, Kritisch - 90 %

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.

ICA RTT (Durchschnitt)

Durchschnittliche ICA-Roundtripzeit.

- Überprüfen Sie die Aufschlüsselung der ICA-Roundtripzeit in Citrix ADM, um die Ursache zu finden. Weitere Informationen finden Sie in der Dokumentation von Citrix ADM.
- Wenn Citrix ADM 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 Anwendungen oder Desktops handelt.

ICA RTT (Anzahl an Sitzungen)

Anzahl der Sitzungen, die den Schwellenwert für die ICA-Roundtripzeit überschreiten

- Überprüfen Sie in Citrix ADM, wie viele Sitzungen eine hohe ICA-Roundtripzeit haben. Weitere Informationen finden Sie in der Dokumentation von Citrix ADM.
- Wenn Citrix ADM nicht verfügbar ist, suchen Sie die Ursache zusammen mit dem Netzwerkteam.

  Bedingungen für intelligente Benachrichtigungsrichtlinien:

  - **Bereich:** Bereitstellungsgruppe, Multisitzungs-OS
  - **Schwellenwerte:** Warnung - 300 ms für 5 oder mehr Sitzungen, Kritisch - 400 ms für 10 oder mehr Sitzungen

ICA RTT (% der Sitzungen)

Prozentanteil der Sitzungen, die die durchschnittliche ICA-Roundtripzeit überschreiten

- Überprüfen Sie in Citrix ADM, wie viele Sitzungen eine hohe ICA-Roundtripzeit haben. Weitere Informationen finden Sie in der Dokumentation von Citrix ADM.
- Wenn Citrix ADM 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.

Fehlerhafte Maschinen (Einzelsitzungs-OS)

Anzahl fehlerhafter Maschinen mit Einzelsitzungs-OS. 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.

  Bedingungen für intelligente Benachrichtigungsrichtlinien:

  - **Bereich:** Bereitstellungsgruppe
  - **Schwellenwerte:** Warnung - 1, Kritisch - 2

Fehlgeschlagene Computer (Multisitzungs-OS)

Anzahl fehlerhafter Maschinen mit Multisitzungs-OS. 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.

  Bedingungen für intelligente Benachrichtigungsrichtlinien:

  - **Bereich:** Bereitstellungsgruppe, Multisitzungs-OS
  - **Schwellenwerte:** Warnung - 1, Kritisch - 2

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.

  Bedingungen für intelligente Benachrichtigungsrichtlinien:

  - **Bereich:** Bereitstellungsgruppe, Multisitzungs-OS
  - **Schwellenwerte:** Warnung - 45 Sekunden, Kritisch - 60 Sekunden

Anmeldedauer (Benutzer)

Dauer der Anmeldungen des angegebenen Benutzers in der letzten Stunde.

Lastauswertungsprogrammindex

Wert des Lastauswertungsprogrammindex der letzten 5 Minuten.

- Suchen Sie in Director nach Maschinen mit Multisitzungs-OS, die mit Spitzenlast ausgeführt werden. Zeigen Sie das Dashboard (Fehler) und die Trendansicht für den Lastauswertungsprogrammindex an.

  Bedingungen für intelligente Benachrichtigungsrichtlinien:

  - **Bereich:** Bereitstellungsgruppe, Multisitzungs-OS
  - **Schwellenwerte:** Warnung - 80 %, Kritisch - 90 %

Überwachen von Hypervisorwarnungen

In Director werden Warnungen zur Überwachung des Hypervisorstatus angezeigt. Warnungen von Citrix Hypervisor und VMware vSphere helfen bei der Überwachung von Hypervisorparametern und -zuständen. Der Hypervisor-Verbindungsstatus wird ebenfalls überwacht und eine Warnung generiert, wenn der Hostcluster bzw. -pool neu gestartet wird oder nicht verfügbar ist.

Um Hypervisorwarnungen zu erhalten, muss in Citrix Studio eine Hostingverbindung erstellt werden. Weitere Informationen finden Sie unter Verbindungen und Ressourcen. Nur diese Verbindungen werden auf Hypervisorwarnungen überwacht. In der folgenden Tabelle werden die verschiedenen Parameter und Zustände von Hypervisorwarnungen beschrieben.

Warnung	Unterstützte Hypervisors	Ausgelöst durch	Bedingung	Konfiguration
CPU-Nutzung	Citrix Hypervisor, VMware vSphere	Hypervisor	Schwellenwert der CPU-Auslastung erreicht oder überschritten	Warnschwellenwerte müssen im Hypervisor konfiguriert werden.
Speichernutzung	Citrix Hypervisor, VMware vSphere	Hypervisor	Schwellenwert der Speicherauslastung erreicht oder überschritten	Warnschwellenwerte müssen im Hypervisor konfiguriert werden.
Netzwerknutzung	Citrix Hypervisor, VMware vSphere	Hypervisor	Schwellenwert der Netzwerkauslastung erreicht oder überschritten	Warnschwellenwerte müssen im Hypervisor konfiguriert werden.
Datenträgernutzung	VMware vSphere	Hypervisor	Schwellenwert der Datenträgerauslastung erreicht oder überschritten	Warnschwellenwerte müssen im Hypervisor konfiguriert werden.

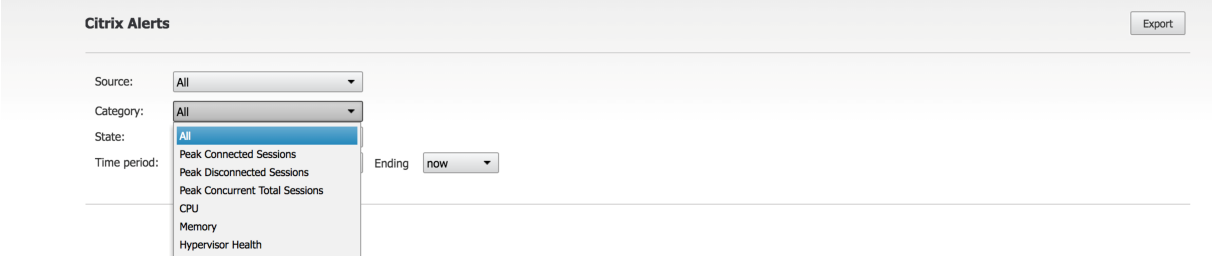
Warnung	Unterstützte Hypervisors	Ausgelöst durch	Bedingung	Konfiguration
Hostverbindung oder Energiezustand	VMware vSphere	Hypervisor	Hypervisorhost neu gestartet oder nicht verfügbar	In VMware vSphere sind die Warnungen vorkonfiguriert. Es ist keine zusätzliche Konfiguration erforderlich.
Hypervisorverbindung nicht verfügbar	Citrix Hypervisor, VMware vSphere	Delivery Controller	Die Verbindung mit dem Hypervisor (Pool oder Cluster) ist getrennt, heruntergefahren oder wird neu gestartet. Diese Warnung wird stündlich generiert, solange die Verbindung nicht verfügbar ist.	Warnungen für den Delivery Controller sind vorkonfiguriert. Es ist keine zusätzliche Konfiguration erforderlich.

> Hinweis:
>
> Weitere Informationen zum Konfigurieren von Warnungen finden Sie unter Citrix XenCenter Alerts oder in der Dokumentation von VMware vCenter Alerts.

E-Mail-Benachrichtigungseinstellungen können unter **Citrix Benachrichtigungsrichtlinie > Siterichtlinie > Hypervisorzustand** konfiguriert werden. Die Schwellenwertbedingungen für Hypervisorwarnrichtlinien können nur über den Hypervisor, nicht aber über Director konfiguriert, bearbeitet, deaktiviert und gelöscht werden. Die Konfiguration der E-Mail-Einstellungen und das Verwerfen von Warnungen ist in Director möglich.

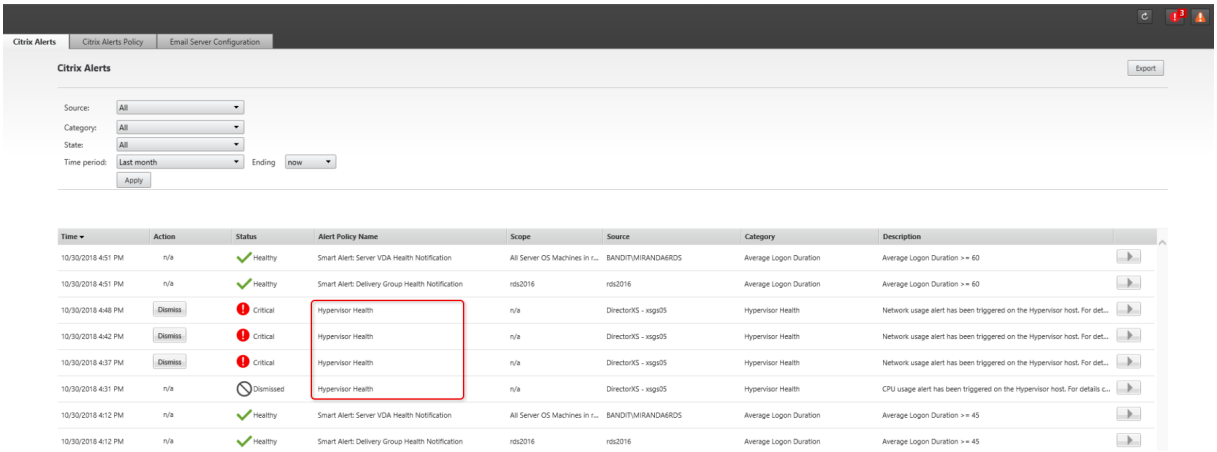
> Wichtig:
>
> - Vom Hypervisor ausgelöste Warnungen werden abgerufen und in Director angezeigt. Änderungen im Lebenszyklus/Status der Hypervisorwarnungen werden jedoch nicht in Direc-

> tor wiedergegeben.
> - Warnungen, die fehlerfrei, verworfen oder in der Hypervisorkonsole deaktiviert sind, werden weiterhin in Director angezeigt und müssen explizit geschlossen werden.
> - Warnungen, die in Director geschlossen werden, werden nicht automatisch in der Hypervisorkonsole geschlossen.



Es gibt die neue Warnungskategorie **Hypervisorzustand**, mit der die Hypervisorwarnungen herausgefiltert werden können. Die Warnungen werden angezeigt, wenn die Schwellenwerte erreicht (oder überschritten) werden. Es gibt folgende Arten von Hypervisorwarnungen:

- Kritisch: Der kritische Schwellenwert der Hypervisorwarnungsrichtlinie wurde erreicht oder überschritten.
- Warnung: Der Warnschwellenwert der Hypervisorwarnungsrichtlinie wurde erreicht oder überschritten.
- Verworfen: Die Warnung wird nicht mehr als aktive Warnung angezeigt.



Für dieses Feature ist Delivery Controller ab Version 7 1811 erforderlich. Wenn Sie eine ältere Director-Version für Sites ab Version 7 1811 verwenden, wird nur die Zahl der Hypervisorwarnungen angezeigt. Sie müssen Director aktualisieren, um den Warnungstext anzuzeigen.

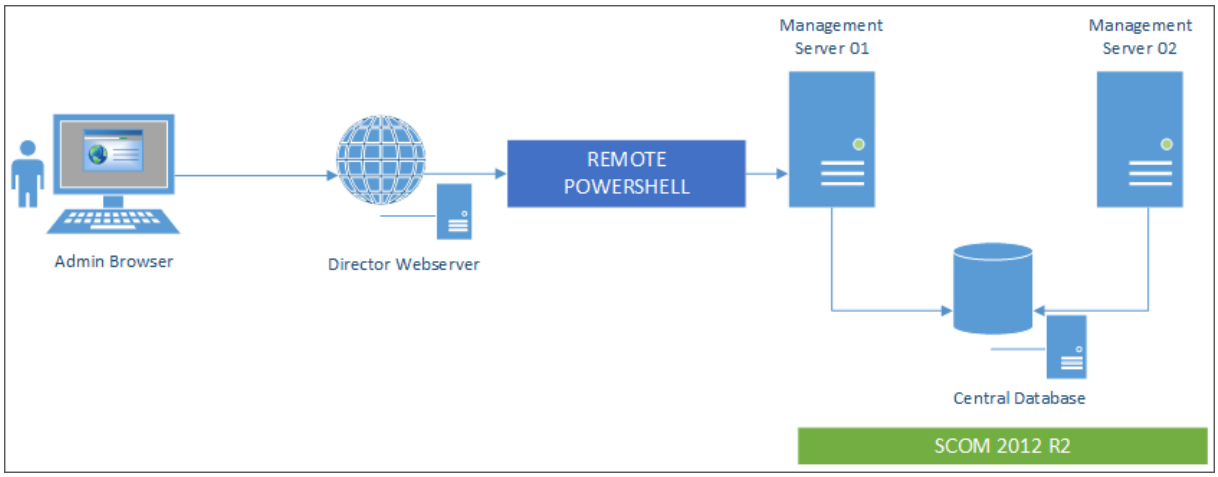
Konfigurieren der Integration von SCOM-Warnungen

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.

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 außerdem, nicht mehr als 10 Director-Administratoren pro SCOM-Verwaltungsserver zu konfigurieren, um eine optimale Leistung sicherzustellen.

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:
   - Abrufen der aktuellen TrustedHosts-Liste

     Get-Item WSMAN:\localhost\Client\TrustedHosts
   - Fügen Sie den SCOM-Verwaltungsserver der Liste "TrustedHosts"hinzu. <Old Values> steht für die von dem Cmdlet "Get-Item"zurückgegebenen vorhandenen Einträge.

     Set-Item WSMAN:localhostClientTrustedHosts -Value "<FQDN SCOM Management Server>,<Old Values>"
3. Konfigurieren Sie SCOM mit dem Tool DirectorConfig.

   C:\inetpub\wwwroot\Director\tools\DirectorConfig.exe /configscom

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:

```
> -  If there are multiple management servers configured and the
primary management server is not available, the Director
administrator cannot connect to the secondary management server
. The primary management server is the server configured in the
 Director web.config file, that is the same server as the one
specified with the DirectorConfig tool in step 3 above. The
secondary management servers are peer management servers of the
 primary server.
```



```
2 > -  While filtering alerts, the Director administrator cannot
      search for the alert source. This requires an operator level
      permission.
```

a) Zum Ändern einer Benutzerrolle klicken Sie mit der rechten Maustaste auf die Rolle und dann auf **Eigenschaften**.

b) 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”}

```
1 PS:
2
3 ```Set -Item WSMan:\localhost\Shell\MaxConcurrentUsers 20<!--
    NeedCopy-->
```

b) Ändern von MaxShellsPerUser:

Befehlszeilenschnittstelle (CLI):

```
winrm set winrm/config/winrs @{ MaxShellsPerUser="20"} <!--
NeedCopy-->
```

PS:

“‘Set-Item WSMan:\localhost\Shell\MaxShellsPerUser 20

```
1 1.  Ändern von MaxMemoryPerShellMB:
2
3     Befehlszeilenschnittstelle (CLI):
4
5     ```winrm set winrm/config/winrs @{
6  MaxMemoryPerShellMB="1024" }
7  <!--NeedCopy-->
```

```
1 PS:
```

```
Set-Item WSMan:\localhost\Shell\MaxMemoryPerShellMB 1024<!--
NeedCopy-->
```


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.

Filtern von Daten zur Problembehandlung

September 21, 2021

Wenn Sie auf Zahlen im Dashboard klicken oder im Menü Filter einen vordefinierten Filter auswählen, wird die Ansicht "Filter"mit Daten für die ausgewählte Maschine oder den Fehlertyp geöffnet.

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 Maschinen mit Einzelsitzungs-OS oder mit Multisitzungs-OS aus. Diese Ansicht zeigt die Anzahl der konfigurierten Computer. Die Registerkarte "Maschinen mit Multisitzungs-OS"enthält auch den Lastauswertungsindex, der die Verteilung der Leistungsindikatoren angibt, und Quickinfos zur Sitzungsanzahl, die Sie aufrufen können, wenn Sie mit der Maus 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 Serverbetriebssysteme und für Einzelsitzungs-OS. Die Sitzungsleerlaufzeiten stehen für Anwendungsinstanzen auf Multisitzungs-OS-VDAs zur Verfügung.

> **Hinweis:**
>
> Wenn Sie Desktopsitzungen auf VDAs unter Windows 10 1809 gestartet haben, werden Microsoft Edge und Office im Aktivitätsmanager in Director möglicherweise als aktiv ausgeführt angezeigt, obwohl sie im Hintergrund ausgeführt werden.

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. Klicken Sie auf **Exportieren**, um die Daten im CSV-Format zu exportieren. Daten von bis zu 100.000 Datensätzen können exportiert werden. Das Feature ist für Delivery Controller ab Version 1808 verfügbar.

9. 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.
10. 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.
11. 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.
12. 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. 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.

> **Hinweis:**
> Citrix Studio ermöglicht die Zuordnung mehrerer Desktopzuordnungsregeln (DAR) für verschiedene Benutzer oder Benutzergruppen zu einem VDA in einer Bereitstellungsgruppe. In StoreFront wird der zugewiesene Desktop unter dem zugehörigen Anzeigenamen gemäß der Desktopzuordnungsregel für den angemeldeten Benutzer angezeigt. Director unterstützt keine Desktopzuordnungsregeln und zeigt den zugewiesenen Desktop unabhängig vom angemeldeten Benutzer unter dem Namen der Bereitstellungsgruppe an. Sie können daher keinen bestimmten Desktop einer Maschine in Director zuordnen. Verwenden Sie folgenden PowerShell-Befehl, um den in StoreFront angezeigten, zugewiesenen Desktop dem in Director angezeigten Bereitstellungsgruppennamen zuzuordnen:

```
Get-BrokerDesktopGroup | Where-Object {
  $\_.Uid -eq (Get-BrokerAssignmentPolicyRule | Where-Object {
  $\_.PublishedName -eq "<Name on StoreFront>"  }
 ).DesktopGroupUid  }
  | Select-Object -Property Name, Uid
<!--NeedCopy-->
```


Siteübergreifendes Überwachen von Verlaufstrends

September 21, 2021

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 Drilldownfeature ermöglicht 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 Premium-Lizenz zur Verfügung.
- Trendberichte über den letzten Monat (31 Tage) stehen in Sites mit Advanced-Lizenz zur Verfügung.
- Trendberichte über die letzten 7 Tage stehen in Editionen mit einer anderen Lizenz als Advanced und Premium 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.
> - Der für den Überwachungsdienst festgelegte Beibehaltungszeitraum der Bereinigung steuert die Verfügbarkeit der Trenddaten. Informationen zu den Standardwerten finden Sie unter Datengranularität und -beibehaltung. In Sites mit Premium-Lizenz kann der gewünschte Beibehaltungszeitraum in Tagen festgelegt werden.
> - Die folgenden IIS-Manager-Parameter steuern den Bereich der verfügbaren Enddaten, die angepasst werden können. Die Verfügbarkeit der Daten für einen ausgewählten Zeitraum hängt jedoch von dem für die jeweilige Kennzahl festgelegten Beibehaltungszeitraum ab.

Parameter	Standardwerte
UI.TrendsLast2HoursRange	3
UI.TrendsLast24HoursRange	32
UI.TrendsLast7DaysRange	32
UI.TrendsLastMonthRange	365

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.

In der Spalte **Automatische Sitzungswiederverbindung** wird die Anzahl der automatischen Wiederverbindungen einer Sitzung angezeigt. Die automatische Wiederverbindung ist aktiviert, wenn die Richtlinie "Sitzungszuverlässigkeit"oder "Client automatisch wieder verbinden"aktiviert ist. Bei einer Netzwerkunterbrechung am Endpunkt werden die folgenden Richtlinien wirksam:

- Sitzungszuverlässigkeit wird (standardmäßig für 3 Minuten) wirksam und Citrix Receiver bzw. die Citrix Workspace-App versucht, eine Verbindung mit dem VDA herzustellen.
- Die automatische Wiederverbindung von Clients wird zwischen 3 und 5 Minuten wirksam und der Client versucht, eine Verbindung mit dem VDA herzustellen.

Beide Wiederverbindungen werden erfasst und dem Benutzer angezeigt. Diese Informationen werden maximal 5 Minuten nach der Wiederverbindung auf der Director-Benutzeroberfläche angezeigt.

Die Informationen zur automatischen Wiederverbindung ermöglichen die Anzeige und Problembehandlung von Netzwerkverbindungen mit Unterbrechungen und die Analyse von Netzwerken mit nahtloser Erfahrung. Sie können die Anzahl der Wiederverbindungen über Filter pro Bereitstellungsgruppe oder Zeitraum anzeigen. Ein Drilldown bietet zusätzliche Informationen wie Sitzungszuverlässigkeit oder automatische Wiederverbindung von Clients, Zeitstempel, IP-Adresse und Name des Endpunkts, auf dem die Workspace-App installiert ist. Standardmäßig werden Protokolle nach Zeitstempel in absteigender Reihenfolge sortiert. Das Feature ist für die Citrix Workspace-App für Windows, die Citrix Workspace-App für Mac, Citrix Receiver für Windows und Citrix Receiver für Mac verfügbar. Dieses Feature erfordert Delivery Controller Version 7 1906 oder höher und VDAs ab Version 1906. Weitere Hinweise zur Wiederverbindung von Sitzungen finden Sie unter Sitzungen. Weitere Informationen zu Richtlinien finden Sie unter Einstellungen der Richtlinie "Automatische Wiederverbindung von Clients" und Einstellungen der Richtlinie "Sitzungszuverlässigkeit".

Manchmal werden die Daten für die automatische Wiederverbindung möglicherweise aus folgenden Gründen nicht in Director angezeigt:

- Die Workspace-App sendet keine Daten zur automatischen Wiederverbindung an den VDA.
- Der VDA sendet keine Daten an den Überwachungsdienst.
- VDA-Nutzlasten werden von Delivery Controllern verworfen, da sie möglicherweise nicht die entsprechenden Sitzungen haben.

> Hinweis:
>
> Es kann vorkommen, dass eine Client-IP-Adresse nicht richtig abgerufen wird, wenn bestimmte NSG-Richtlinien festgelegt sind.

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 "Fehler"für Maschinen mit Einzelsitzungs-OS bzw. Multisitzungs-OS 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"können Sie ein Diagramm anzeigen, das ausführliche Informationen zur Last enthält, die auf die Multisitzungs-OS-Maschinen verteilt ist. Als Filteroptionen für dieses Diagramm stehen Bereitstellungsgruppe oder Multisitzungs-OS-Maschine in einer Bereitstellungsgruppe, Multisitzungs-OS-Maschine (nur wenn Multisitzungs-OS-Maschine in einer Bereitstellungsgruppe ausgewählt ist) 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 Einzelsitzungs-OS und Multisitzungs-OS: In der Ansicht "Trends"wird die Nutzung von Einzelsitzungs-OS 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 Nutzung von Multisitzungs-OS 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 "Maschinen mit Betriebssystemen für Einzelsitzungen"oder "Maschinen mit Betriebssystemen für mehrere Sitzungen", um einen Überblick über die Nutzung der VMs in Echtzeit zu erhalten, sodass Sie den Kapazitätsbedarf der Site schnell einschätzen können.
Verfügbarkeit von Betriebssystemen für Einzelsitzungen: Zeigt den aktuellen Zustand von Maschinen mit Einzelsitzungs-OS (VDIs) nach Verfügbarkeit für die gesamte Site oder für eine bestimmte Bereitstellungsgruppe an.
Verfügbarkeit von Betriebssystemen für mehrere Sitzungen: Zeigt den aktuellen Zustand von Maschinen mit Multisitzungs-OS nach Verfügbarkeit für die gesamte Site oder für bestimmte Bereitstellungsgruppen an.

> **Hinweis:**
> Unter "Verfügbar"werden auch Maschinen im Wartungsmodus angezeigt.

Anzeigen der Ressourcennutzung: Zur Vereinfachung der Kapazitätsplanung wählen Sie auf der Registerkarte "Ressourcenauslastung"die Option "Maschinen mit Einzelsitzungs-OS"oder "Maschinen mit Multisitzungs-OS", 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.

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 Richtlinie ist standardmäßig auf "Nicht zugelassen" festgelegt. Standardmäßig werden alle Daten zur Ressourcenauslastung gesammelt. Dies kann mit der 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 Citrix ADM. 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. VDAs für Einzelsitzungs-OS unter Windows Vista und höher und VDAs für Multisitzungs-OS unter Windows Server 2008 und höher werden unterstützt.
Weitere Informationen finden Sie unter Überwachen historischer Anwendungsstörungen.

Standardmäßig werden nur Anwendungsausfälle von Multisitzungs-OS-VDAs angezeigt. Sie können die Überwachung von Anwendungsstörungen über die Überwachungsrichtlinien steuern. Weitere Informationen finden Sie unter Einstellungen der Überwachungsrichtlinie.

Anzeigen der Ergebnisse von Anwendungstests: Auf der Registerkarte "Anwendungstestergebnisse"werden die Ergebnisse von Anwendungstests angezeigt, die auf der Seite "Konfiguration" konfiguriert wurden. Es wird hier wird die Startphase angegeben, bei der ein Anwendungsstart fehlgeschlagen ist.

Für dieses Feature sind Delivery Controller und VDAs ab **Version 7.18** erforderlich. Weitere Informationen finden Sie unter Anwendungtests.

Erstellen benutzerdefinierter Berichte: Über die Registerkarte "Benutzerdefinierte Berichte"kön-

nen 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 und herunterladen** 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.

> **Hinweis:**
> Die Spaltennamen in der Vorschau und dem Exportbericht nach OData-Abfrage werden auf Englisch angezeigt.

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.

> **Hinweis:**
>
> - 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 Lastauswertungsprogrammindex** der neuen Bereitstellungsgruppe Metriken angezeigt, die aus den alten und neuen Bereitstellungsgruppen konsolidiert wurden.

Problembehandlung bei Bereitstellungen

February 6, 2020

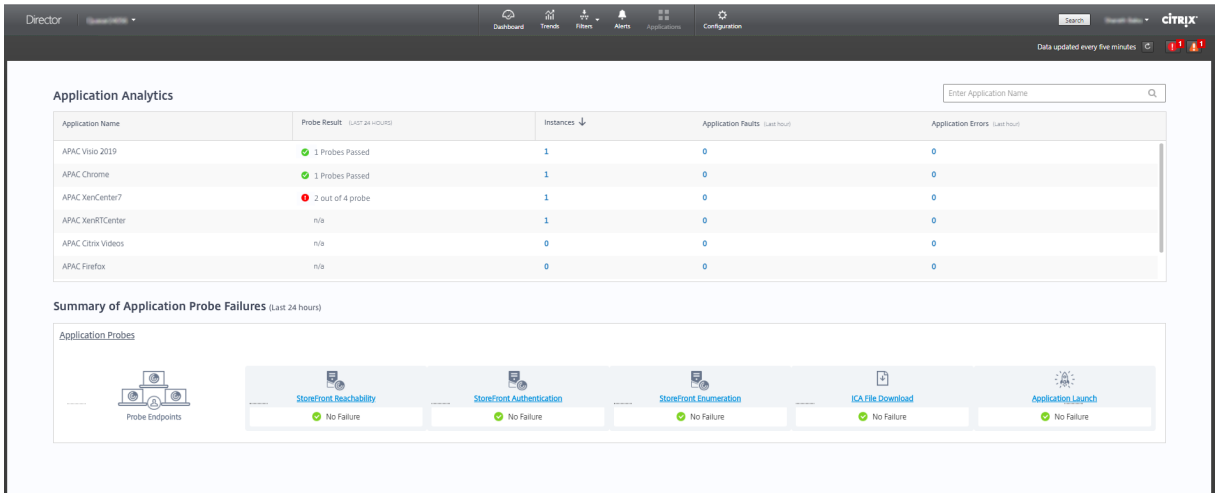
Helpdesk-Administratoren können einen Benutzer, der ein Problem meldet, suchen und Details zu Sitzungen und Anwendungen des Benutzers anzeigen. Sie können auch Maschinen und Endpunkte suchen, bei denen Probleme gemeldet wurden. Probleme können durch die Überwachung relevanter Metriken und das Ergreifen entsprechender Maßnahmen schnell gelöst werden. Mögliche Maßnahmen sind das Beenden einer Anwendung bzw. eines Prozesses, die/der nicht mehr reagiert, das Spiegeln von Vorgängen auf der Maschine des Benutzers, das Abmelden einer nicht mehr reagierenden Sitzung, das Neustarten der Maschine, das Versetzen der Maschine in den Wartungsmodus und das Zurücksetzen des Benutzerprofils.

Problembehandlung bei Anwendungen

September 21, 2021

Anwendungsanalyse

In der Ansicht **Anwendungen** werden konsolidierte Anwendungsdaten zur effizienten Analyse und Verwaltung der Anwendungsleistung angezeigt. Sie erhalten hier wertvolle Einblicke in die Integrität und Nutzung aller in der Site veröffentlichten Anwendungen. In der Standardansicht können die wichtigsten ausgeführten Anwendungen identifiziert werden.
Für dieses Feature sind Delivery Controller ab Version 7.16 und VDAs ab Version 7.15 erforderlich.



In der Spalte **Testergebnis** wird das Ergebnis der Anwendungstests der letzten 24 Stunden angezeigt. Klicken Sie auf einen Ergebnislink, um auf der Seite **Trends** > **Anwendungstestergebnisse** weitere Details aufzurufen. Weitere Informationen zum Konfigurieren von Anwendungstests finden Sie unter Anwendungstests.

In der Spalte **Instanzen** wird die Verwendung der Anwendungen angezeigt. Sie zeigt die Zahl der aktuell ausgeführten Anwendungsinstanzen (verbundene und getrennte Instanzen). Zur weiteren Problembehandlung klicken Sie auf das Feld **Instanzen**, um die entsprechende Filterseite **Anwendungsinstanzen** anzuzeigen. Hier können Sie Anwendungsinstanzen zum Abmelden oder Trennen der Verbindung auswählen.

> **Hinweis:**
>
> Anwendungsinstanzen, die unter "Anwendungsgruppen"erstellt wurden, werden für Administratoren mit benutzerdefiniertem Bereich in Director nicht angezeigt. Zur Anzeige aller Anwendungsinstanzen sind vollständige Administratorrechte erforderlich. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX256001.

Den Status veröffentlichter Anwendungen in der Site können Sie über die Spalten **Anwendungsausfälle** und **Anwendungsfehler** überwachen. In diesen Spalten wird die aggregierte Zahl der Fehler und Ausfälle beim Starten der jeweiligen Anwendung in der letzten Stunde angezeigt. Klicken Sie auf das Feld **Anwendungsausfälle** oder **Anwendungsfehler**, um auf der Seite **Trends** > **Anwendungsstörungen** Fehlerangaben für die ausgewählte Anwendung anzuzeigen.

Die Richtlinien für die Überwachung auf Anwendungsfehler bestimmen die Verfügbarkeit und Anzeige von Ausfällen und Fehlern. Weitere Informationen zu diesen Richtlinien und zu deren Bearbeitung finden Sie unter Richtlinien für die Überwachung auf Anwendungsfehler im Artikel "Einstellungen der Überwachungsrichtlinie".

Überwachen von Anwendungen in Echtzeit

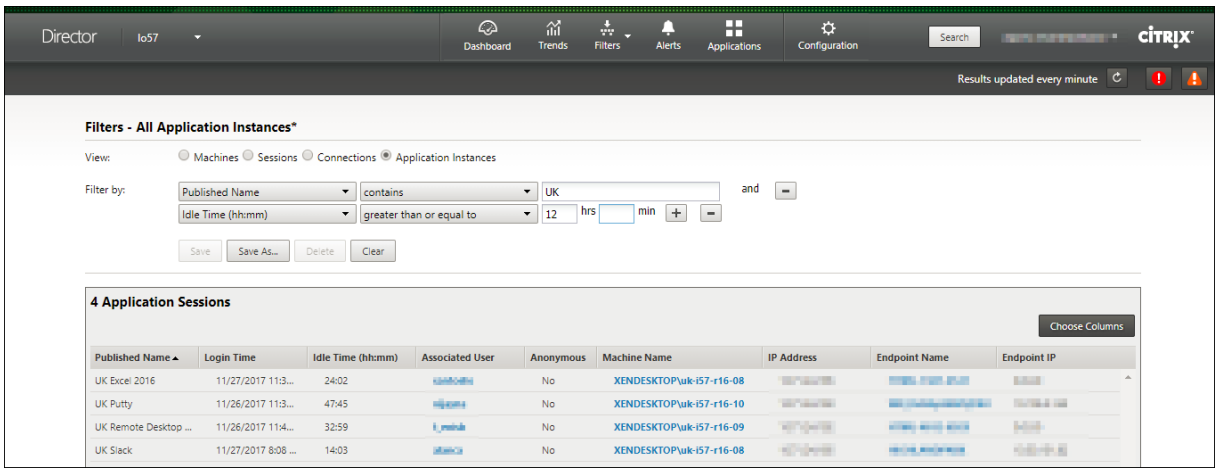
Zur Problembehandlung bei Anwendungen und Sitzungen können Sie anhand von Leerlaufkennzahlen feststellen, welche Instanzen über ein bestimmtes Zeitlimit hinaus inaktiv bleiben.

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 Citrix Virtual Apps and Desktops-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 Einzelsitzungs-OS. Die Leerlaufzeit wird für Anwendungsinstanzen auf Multisitzungs-OS-VDAs angezeigt, die mindestens 10 Minuten im Leerlauf sind.

> **Hinweis:**
> Die Kennzahlen für Anwendungsinstanzen stehen in Sites mit allen Lizenztypen zur Verfügung.

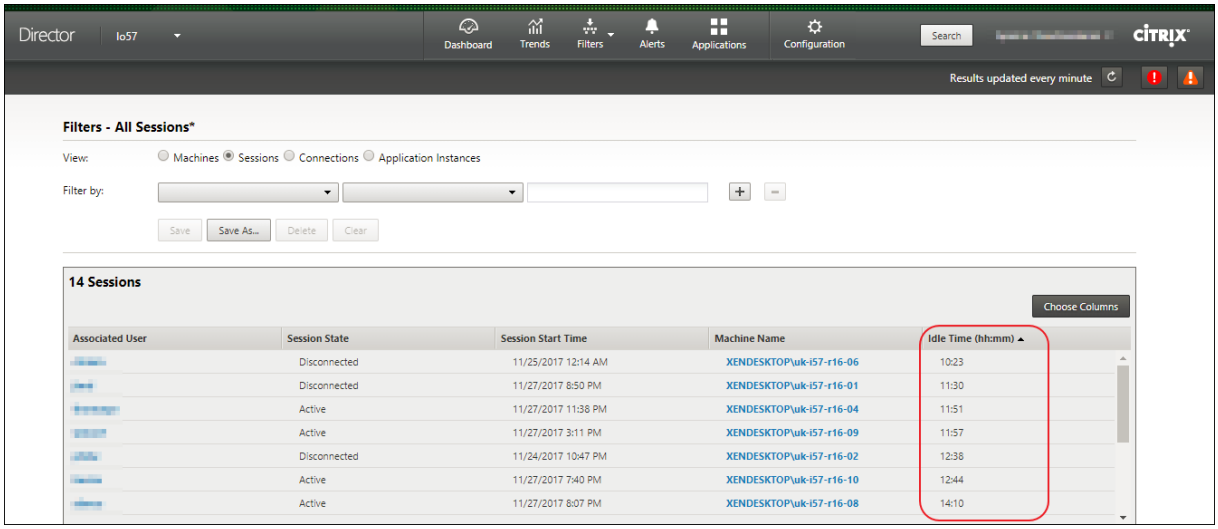
Anhand dieser Informationen können Sie Instanzen suchen, die länger als vorgegeben im Leerlauf sind und diese abmelden oder trennen. Wählen Sie hierfür **Filter > Anwendungsinstanzen** und wählen Sie einen vorhandenen Filter oder **Alle Anwendungsinstanzen** und erstellen Sie Ihren eigenen Filter.



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 Multisitzungs-OS-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 VDA für Einzelsitzungs-OS gestartet wurde
- oder auf einem VDA einer Version bis 7.12 ausgeführt wird

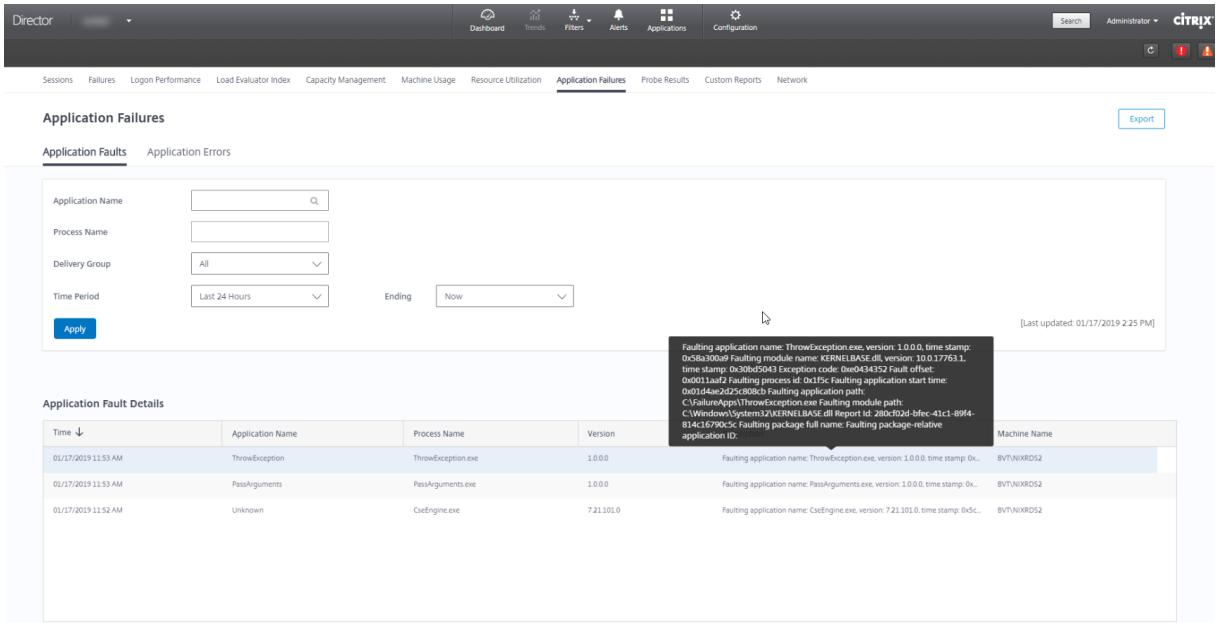
Überwachen historischer Anwendungsstörungen

Auf der Registerkarte **Trends** > **Anwendungsstörungen** werden Fehler bei den veröffentlichten Anwendungen auf den VDAs angezeigt.

Anwendungsstörungstrends für Sites mit Premium- oder Advanced-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 Premium- und anderen Lizenzen auf einen Tag festgelegt. Sie können diese Einstellung mit folgendem PowerShell-Befehl ändern:

```
PowerShell command Set-MonitorConfiguration -<setting name> <value>
<!--NeedCopy-->
```

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

Auf der Seite **Trends** > **Anwendungstestergebnisse** werden die Ergebnisse der Anwendungtests der letzten 24 Stunden und der letzten 7 Tage angezeigt. Weitere Informationen zum Konfigurieren von Anwendungstests finden Sie unter Anwendungstests.

Anwendungstests

January 8, 2021

Das Anwendungtestfeature automatisiert die Überprüfung der Integrität der in einer Site veröffentlichten Citrix Virtual Apps. Das Ergebnis der Anwendungstests steht in Director zur Verfügung.

Anforderungen:

- Auf dem Delivery Controller wird Version 7.18 oder höher ausgeführt.
- Endpunktmaschinen mit Testagents sind Windows-Maschinen mit Citrix Receiver für Windows 4.8 oder höher oder der Citrix Workspace-App für Windows (früher Citrix Receiver für Windows) 1808 oder höher. Die Workspace-App für Unified Windows Platform (UWP) wird nicht unterstützt.
- Director und StoreFront unterstützen die standardmäßige formularbasierte Authentifizierung.

Zum Ausführen von Anwendungstests erforderliche Benutzerkonten/Berechtigungen:

- Eindeutiger StoreFront-Benutzer auf jeder Endpunktmaschine. Der StoreFront-Benutzer muss kein Administrator sein.
- Benutzerkonten mit Windows-Administratorberechtigung zum Installieren und Konfigurieren von Citrix Probe Agent auf den Endpunktmaschinen
- Ein Volladministratorkonto oder eine benutzerdefinierte Rolle mit den folgenden Berechtigungen. Die Wiederverwendung bestehender Benutzerkonten für Anwendungstests kann zur Abmeldung von deren aktiven Sitzungen führen.
  - Bereitstellungsgruppenberechtigungen:
    - Nur Lesen
  - Director-Berechtigungen:
    - E-Mail-Serverkonfiguration erstellen\bearbeiten\entfernen (sofern der E-Mail-Server noch nicht konfiguriert ist)
    - Testkonfigurationen erstellen\bearbeiten\entfernen
    - Konfigurationsseite anzeigen
    - Trendseite anzeigen

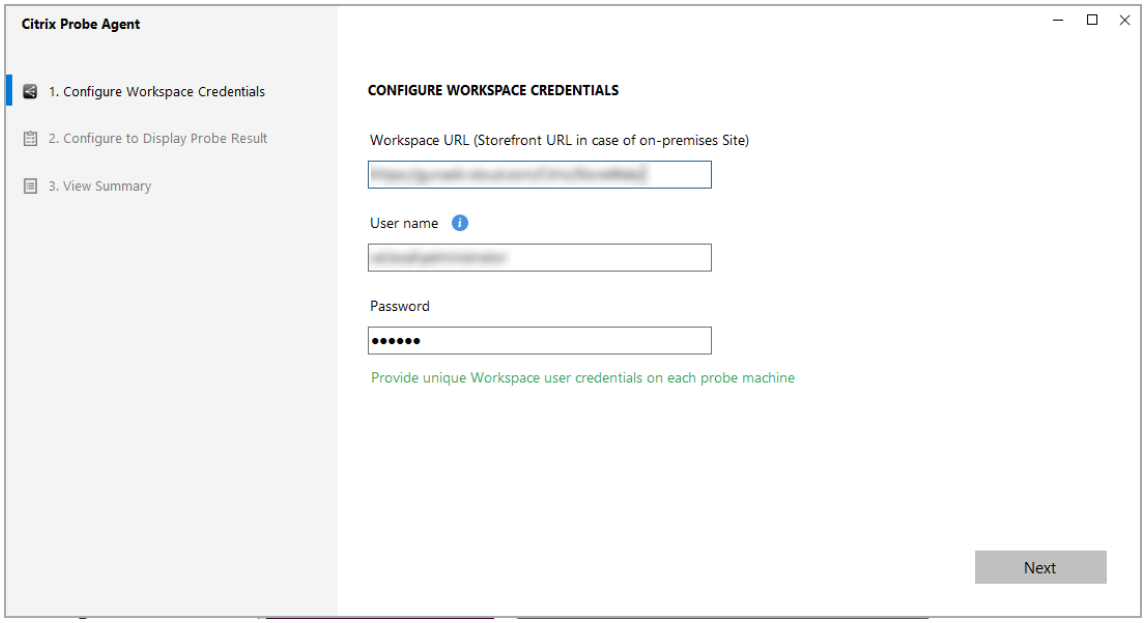
Konfigurieren von Anwendungstests

Sie können die Durchführung von Anwendungtests für außerhalb der Spitzenzeiten in mehreren Regionen planen. Die umfassenden Testergebnisse können helfen, Probleme bei Anwendungen, Hostcomputern oder Verbindung zu beheben, bevor sie sich bei den Benutzern bemerkbar machen.

Schritt 1: Installieren und Konfigurieren von Citrix Probe Agent

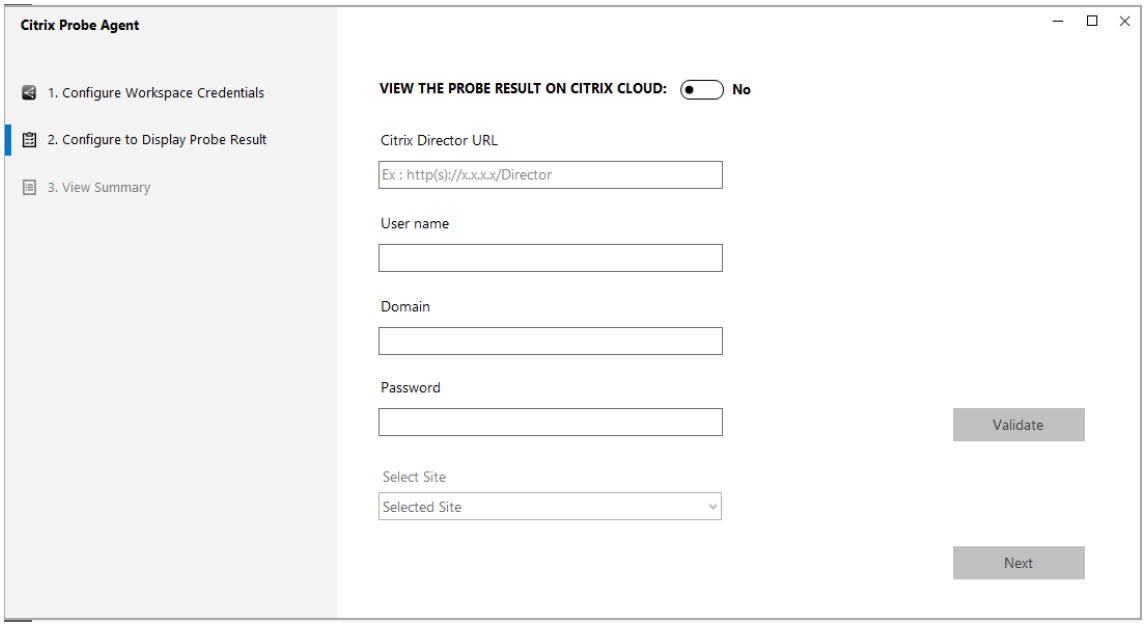
Citrix Probe Agent ist eine ausführbare Windows-Datei, die den Anwendungsstart durch einen Benutzer über StoreFront simuliert. Der Agent testet Anwendungsstarts gemäß der Konfiguration in Director und meldet die Ergebnisse an Director.

1. Identifizieren Sie die Endpunktmaschinen, auf denen Sie Anwendungtests ausführen möchten.
2. Benutzer mit Administratorberechtigung können Citrix Probe Agent auf den Endpunktmaschinen installieren und konfigurieren. Laden Sie die ausführbare Datei von Citrix Probe Agent von folgender Webseite herunter: https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/components/app-probe-agent.html
3. Starten Sie den Agent und konfigurieren Sie Ihre StoreFront-Anmeldeinformationen für Receiver für Web. Konfigurieren Sie einen eindeutigen StoreFront-Benutzer auf jeder Endpunktmaschine. Die Anmeldeinformationen werden verschlüsselt und sicher gespeichert.



> **Hinweis:**
> Um auf die gewünschte Site von außerhalb des Netzwerks zuzugreifen, geben Sie im Feld "StoreFront-URL"die Login-URL für Citrix Gateway ein. Citrix Gateway leitet die Anforderung automatisch an die entsprechende Site StoreFront-URL weiter. Das Feature ist ab Citrix Gateway-Version 12.1 (RfWebUI-Design) und ab Delivery Controller-Version 1811 verfügbar.

4. Geben Sie auf der Registerkarte **Anzeige der Testergebnisse konfigurieren** Ihre Director-Anmeldeinformationen ein und klicken Sie auf **Überprüfen**.



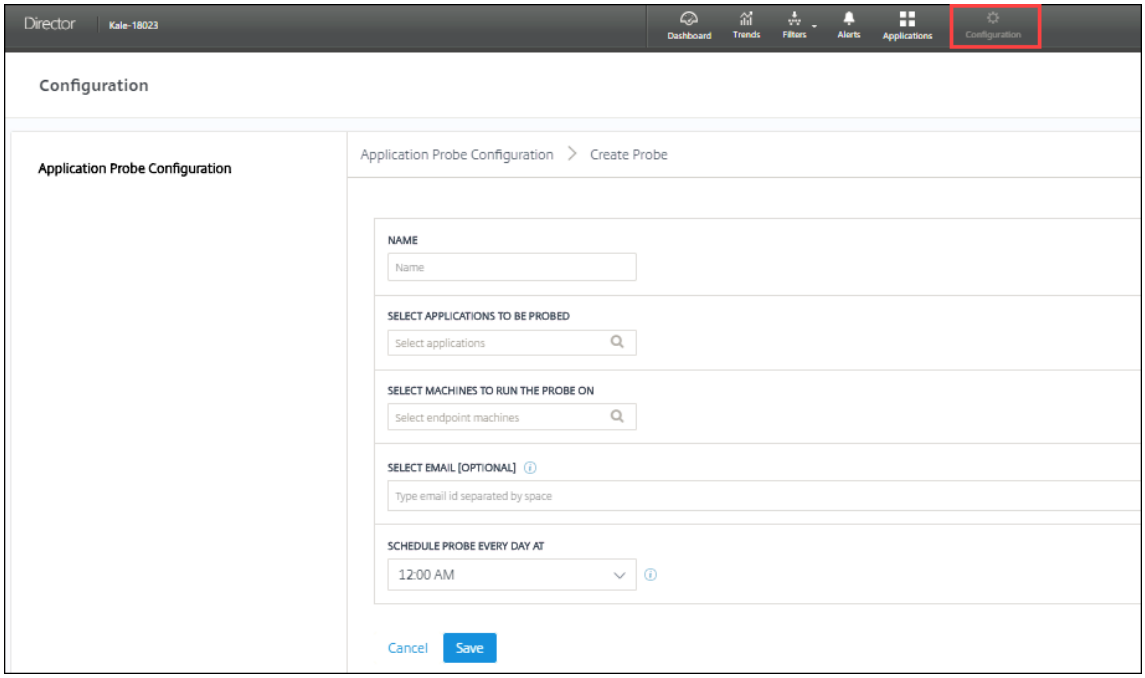
5. Wählen Sie Ihre Site aus und klicken Sie auf **Weiter**.

Schritt 2: Konfigurieren von Anwendungstests in Director

1. Gehen Sie zu **Konfiguration** > **Anwendungstestkonfiguration**.
2. Erstellen Sie einen Test und wählen Sie Folgendes aus:

   - Zu testende Anwendungen
   - Endpunktmaschinen, auf denen der Test ausgeführt werden muss
   - E-Mail-Adressen, an die Ergebnisse nicht bestandener Tests gesendet werden sollen (konfigurieren Sie Ihren E-Mail-Server unter **Benachrichtigungen** > **E-Mail-Server-Konfiguration**) und
   - Tageszeit, zu der der Test ausgeführt werden muss (gemäß lokaler Zeitzone der Endpunktmaschine)

   Nach der Konfiguration in Director benötigt der Agent 10 Minuten, bevor er mit Tests beginnen kann. Die konfigurierten Tests beginnen dann in der darauffolgenden Stunde.



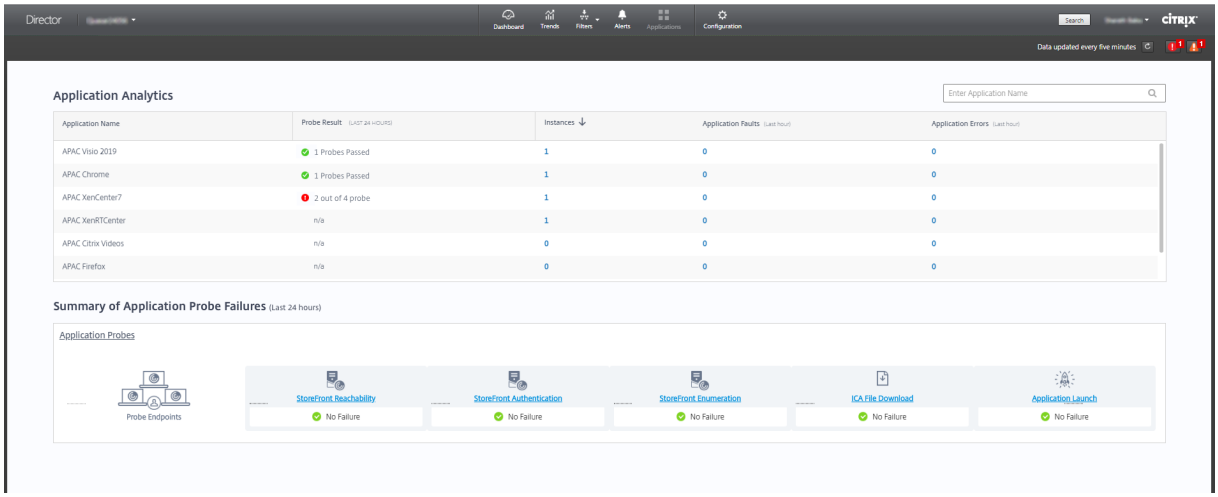
Schritt 3: Ausführen des Tests

Der Agent führt Anwendungtests regelmäßig entsprechend der von Director abgerufenen Konfiguration aus. Er startet ausgewählte Anwendungen der Reihe nach über StoreFront. Die Ergebnisse werden über die Überwachungsdatenbank an Director gemeldet. Fehler werden für fünf spezifische Phasen gemeldet:

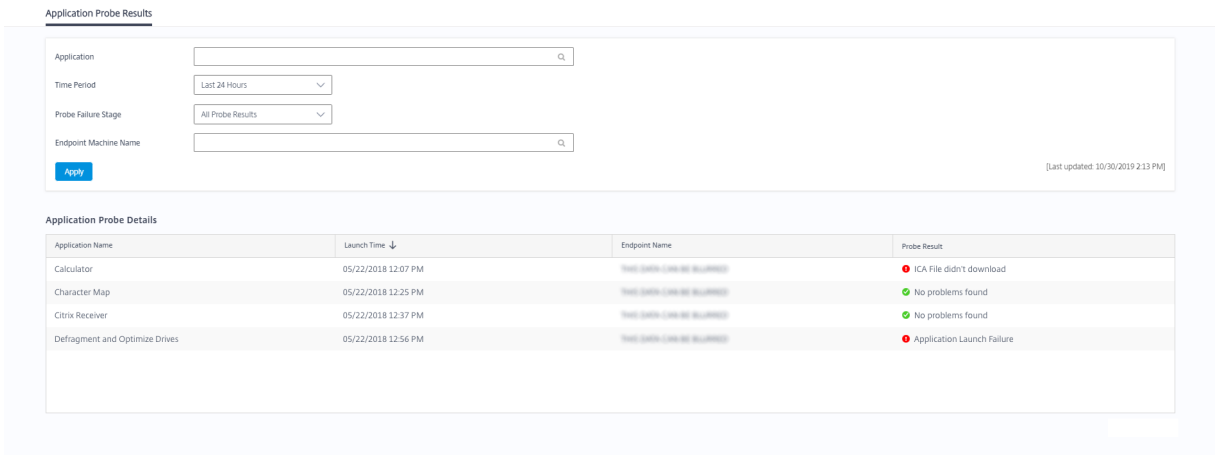
- **StoreFront-Erreichbarkeit**: Die konfigurierte StoreFront-URL ist nicht erreichbar.
- **StoreFront-Authentifizierung**: Die konfigurierten StoreFront-Anmeldedaten sind ungültig.
- **StoreFront-Enumeration**: Die Liste der enumerierten Anwendungen in StoreFront enthält die getestete Anwendung nicht.
- **ICA-Download**: Die ICA-Datei ist nicht verfügbar.
- **Anwendungsstart**: Die Anwendung konnte nicht gestartet werden.

Schritt 4: Anzeigen der Testergebnisse

Sie können die neuesten Testergebnisse auf der Seite **Anwendungen** anzeigen.



Zur weitergehenden Fehlerbehebung klicken Sie auf einen Ergebnislink, um auf der Seite **Trends** > **Anwendungstestergebnisse** weitere Details aufzurufen.



Auf dieser Seite werden die konsolidierten Ergebnisdaten für die letzten 24 Stunden oder die letzten 7 Tage angezeigt. Sie können die Phase sehen, in der ein Test fehlgeschlagen ist. Sie können die Tabelle nach Anwendungen, Fehlerphasen oder Endpunktmaschinen filtern.

Desktoptests

September 21, 2021

Das Desktoptestfeature automatisiert die Überprüfung der Integrität der in einer Site veröffentlichten Citrix Virtual Desktops. Das Ergebnis der Desktoptests steht in Director zur Verfügung.

Konfigurieren Sie auf der Seite “Konfiguration”in Director die zu testenden Desktops, die Endpunktmaschinen zur Ausführung der Tests und die Testzeit. Der Agent testet den Start der ausgewählten Desktops unter Einsatz von StoreFront und meldet das Ergebnis an Director. Die Testergebnisse

werden in der Benutzeroberfläche von Director angezeigt: die Daten der letzten 24 Stunden auf der Seite "Anwendungen"und die historischen Daten auf der Seite Trends > Ergebnisse der Desktoptests. Hier sehen Sie die Phase, in der Fehler aufgetreten sind: StoreFront-Erreichbarkeit, StoreFront-Authentifizierung, StoreFront-Enumeration, ICA-Download oder Desktopstart. Der Fehlerbericht wird per E-Mail an die konfigurierten Adressen gesendet. Sie können die Durchführung von Desktoptests außerhalb der Spitzenzeiten in mehreren Regionen planen. Die umfassenden Testergebnisse können helfen, Probleme bei Desktops, Hostmaschinen oder Verbindungen zu beheben, bevor sie sich bei den Benutzern bemerkbar machen. Desktoptests stehen für Sites mit Premium-Lizenz zur Verfügung. Dieses Feature erfordert Delivery Controller Version 7 1906 oder höher und Probe Agent 1903 oder höher.

Anforderungen:

- Auf dem Delivery Controller wird Version 1906 oder höher ausgeführt.
- Endpunktmaschinen mit Testagents sind Windows-Maschinen mit Citrix Receiver für Windows 4.8 oder höher oder der Citrix Workspace-App für Windows (früher Citrix Receiver für Windows) 1906 oder höher. Die Workspace-App für Unified Windows Platform (UWP) wird nicht unterstützt.
- Director und StoreFront unterstützen die standardmäßige formularbasierte Authentifizierung.

Zum Ausführen von Anwendungstests erforderliche Benutzerkonten bzw. Berechtigungen:

- Eindeutiger StoreFront-Benutzer auf jeder Endpunktmaschine. Der StoreFront-Benutzer muss kein Administrator sein.
- Benutzerkonten mit Windows-Administratorberechtigung zum Installieren und Konfigurieren von Citrix Probe Agent auf den Endpunktmaschinen
- Ein Volladministratorkonto oder eine benutzerdefinierte Rolle mit den folgenden Berechtigungen. Die Wiederverwendung normaler Benutzerkonten für Desktoptests kann zur Abmeldung von deren aktiven Sitzungen führen.
  - Bereitstellungsgruppenberechtigungen:
    - Nur Lesen
  - Director-Berechtigungen:
    - E-Mail-Serverkonfiguration erstellen, bearbeiten, entfernen (sofern der E-Mail-Server noch nicht konfiguriert ist)
    - Testkonfigurationen erstellen, bearbeiten, entfernen
    - Konfigurationsseite anzeigen
    - Trendseite anzeigen

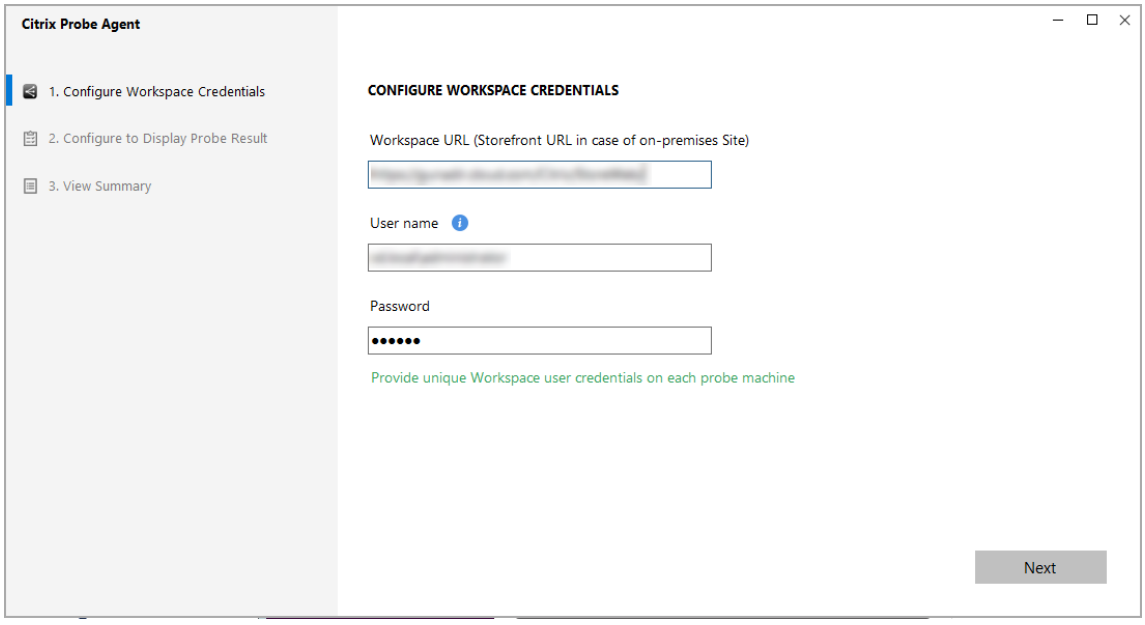
Desktoptests konfigurieren

Sie können die Durchführung von Desktoptests außerhalb der Spitzenzeiten in mehreren Regionen planen. Die umfassenden Testergebnisse können helfen, Probleme bei Desktops, Hostcomputern oder Verbindung zu beheben, bevor sie sich bei den Benutzern bemerkbar machen.

Schritt 1: Installieren und Konfigurieren von Citrix Probe Agent

Citrix Probe Agent ist eine ausführbare Windows-Datei, die den Desktopstart durch einen Benutzer über StoreFront simuliert. Der Agent testet Desktopstarts gemäß der Konfiguration in Director und meldet die Ergebnisse an Director.

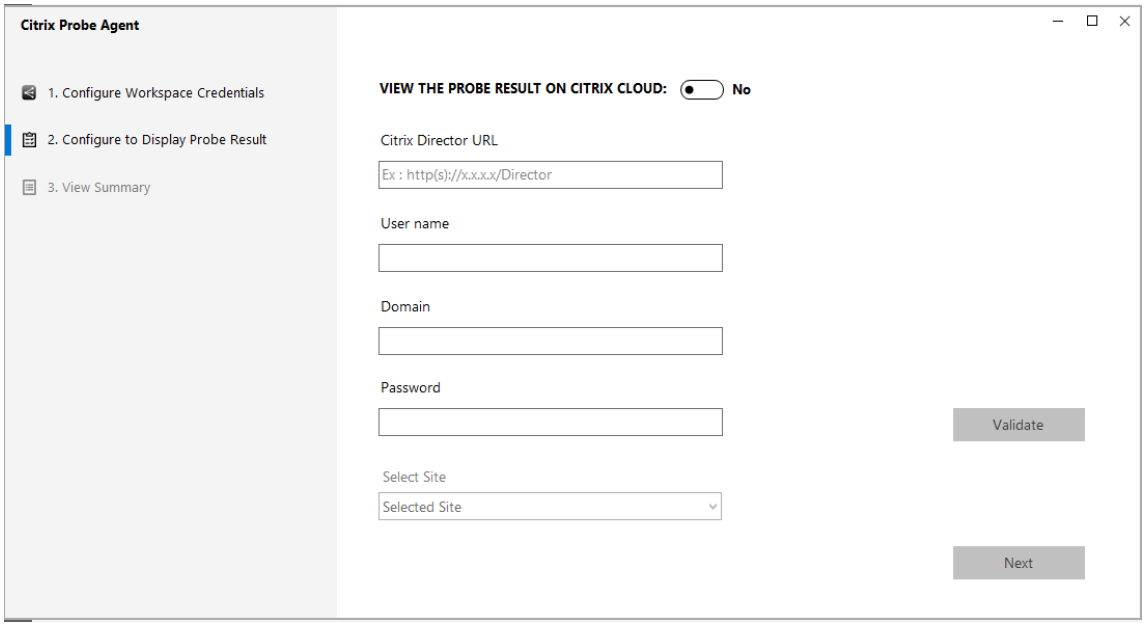
1. Identifizieren Sie die Endpunktmaschinen, auf denen Sie Desktoptests ausführen möchten.
2. Benutzer mit Administratorberechtigung können Citrix Probe Agent auf den Endpunktmaschinen installieren und konfigurieren. Laden Sie die ausführbare Datei von Citrix Probe Agent von folgender Webseite herunter: https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/components/app-probe-agent.html
3. Starten Sie den Agent und konfigurieren Sie Ihre StoreFront-Anmeldeinformationen für Receiver für Web. Konfigurieren Sie einen eindeutigen StoreFront-Benutzer auf jeder Endpunktmaschine. Die Anmeldeinformationen werden verschlüsselt und sicher gespeichert.



> Hinweis:
>
> Um auf die gewünschte Site von außerhalb des Netzwerks zuzugreifen, geben Sie die URL der Citrix Gateway-Anmeldeseite in das Feld “StoreFront-URL”ein. Citrix Gateway leitet die

> Anforderung automatisch an die entsprechende Site StoreFront-URL weiter. Das Feature ist ab Citrix Gateway-Version 12.1 und ab Delivery Controller-Version 1811 verfügbar.

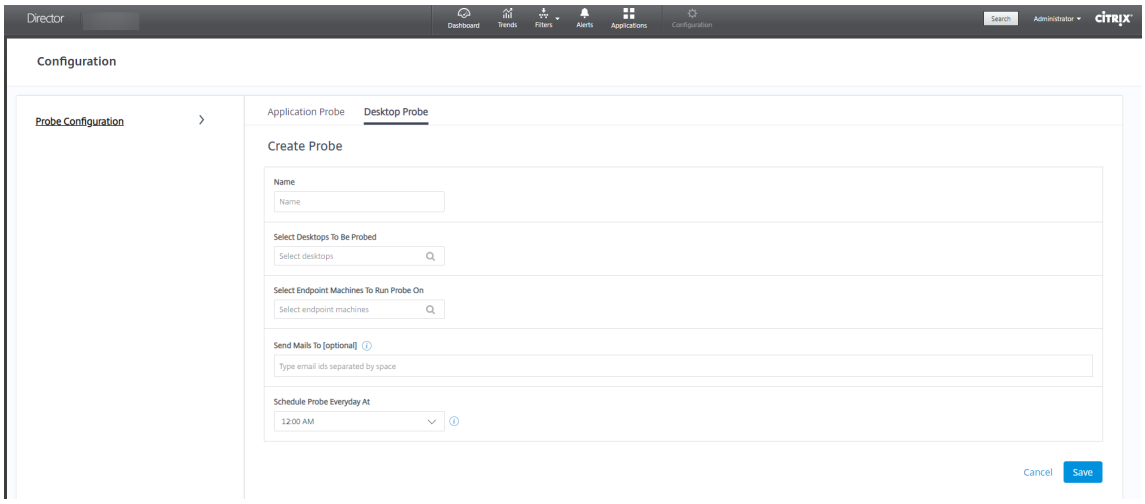
4. Geben Sie auf der Registerkarte **Anzeige der Testergebnisse konfigurieren** Ihre Director-Anmeldeinformationen ein und klicken Sie auf **Überprüfen**.



5. Wählen Sie Ihre Site aus und klicken Sie auf **Weiter**.

Schritt 2: Konfigurieren von Desktoptests in Director

1. Gehen Sie zu **Konfiguration** > **Desktoptestkonfiguration**.
2. Um einen Test zu erstellen, geben Sie die Details ein und klicken Sie auf **Speichern**.



> Hinweis:
>
> Konfigurieren Sie Ihren E-Mail-Server unter **Warnungen** > **E-Mail-Server-Konfiguration**.

Nach der Konfiguration der Desktoptests dauert es 10 Minuten, bevor der Agent mit Tests beginnen kann. Die konfigurierten Tests beginnen dann in der darauffolgenden Stunde.

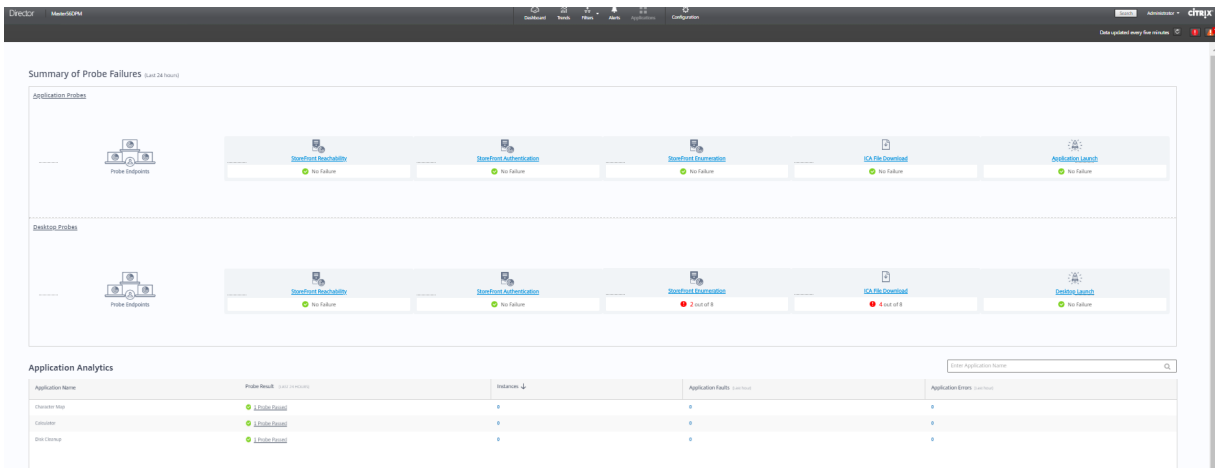
Schritt 3: Ausführen des Tests

Der Agent führt Desktoptests regelmäßig entsprechend der von Director abgerufenen Konfiguration aus. Er startet ausgewählte Desktops der Reihe nach über StoreFront. Die Ergebnisse werden über die Überwachungsdatenbank an Director gemeldet. Fehler werden für fünf spezifische Phasen gemeldet:

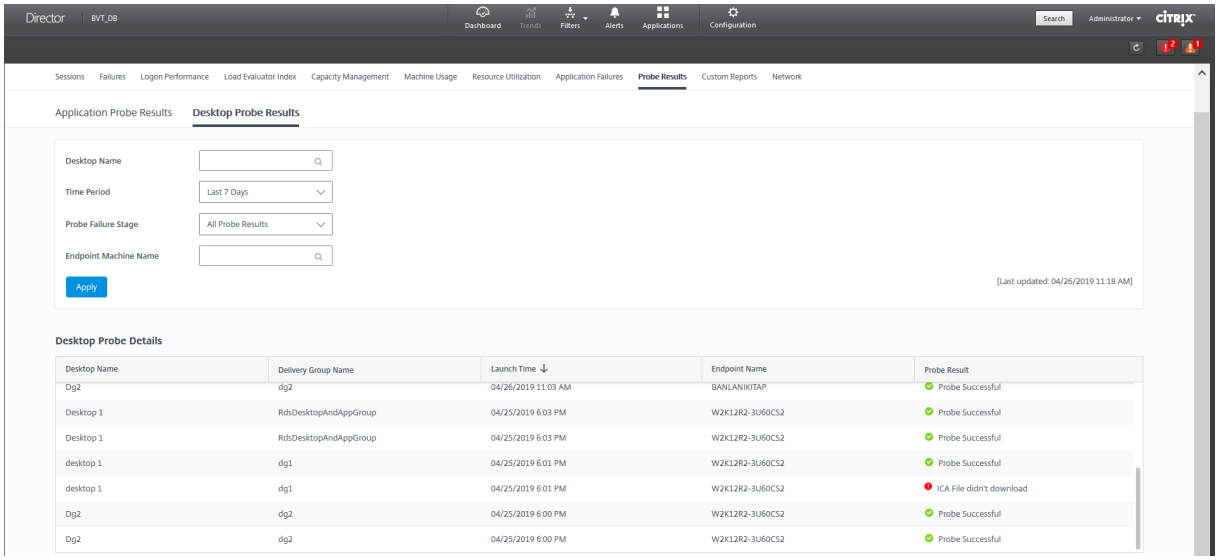
- **StoreFront-Erreichbarkeit**: Die konfigurierte StoreFront-URL ist nicht erreichbar.
- **StoreFront-Authentifizierung**: Die konfigurierten StoreFront-Anmeldedaten sind ungültig.
- **StoreFront-Enumeration**: Die Liste der enumerierten Desktops in StoreFront enthält den getesteten Desktop nicht.
- **ICA-Download**: Die ICA-Datei ist nicht verfügbar.
- **Desktopstart:** Der Desktop kann nicht gestartet werden.

Schritt 4: Anzeigen der Testergebnisse

Sie können die neuesten Testergebnisse auf der Seite **Desktops** anzeigen.



Zur weitergehenden Fehlerbehebung klicken Sie auf einen Ergebnislink, um auf der Seite **Trends** > **Testergebnisse** > **Desktoptestergebnisse** weitere Details aufzurufen.



Auf dieser Seite werden die konsolidierten Ergebnisdaten für die letzten 24 Stunden oder die letzten 7 Tage angezeigt. Sie können die Phase sehen, in der ein Test fehlgeschlagen ist. Sie können die Tabelle nach Desktops, Fehlerphasen oder Endpunktmaschinen filtern.

Problembehandlung bei Maschinen

June 27, 2024

> **Hinweis:**
> **Citrix Health Assistant** ist ein Tool zum Beheben von Konfigurationsproblemen bei nicht registrierten VDAs. Durch verschiedene automatisierte Systemdiagnosen wird die mögliche Ursache von Konfigurationsproblemen bei der VDA-Registrierung, beim Sitzungsstart und bei der Zeitzonenumleitung gesucht. Der Knowledge Center-Artikel Citrix Health Assistant - Troubleshoot VDA Registration and Session Launch enthält eine Downloadversion von **Citrix Health Assistant** und Anweisungen zu dessen Verwendung.

Die Ansicht **Filter > Maschinen** in der Director-Konsole zeigt die in der Site konfigurierten Maschinen an. Die Registerkarte "Maschinen mit Multisitzungs-OS"enthält den Lastauswertungsindex, der die Verteilung der Leistungsindikatoren angibt, und Quickinfos zur Sitzungsanzahl, die Sie aufrufen können, wenn Sie mit der Maus auf den Link zeigen.

Klicken Sie für fehlerhafte Maschinen auf die Spalte **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.

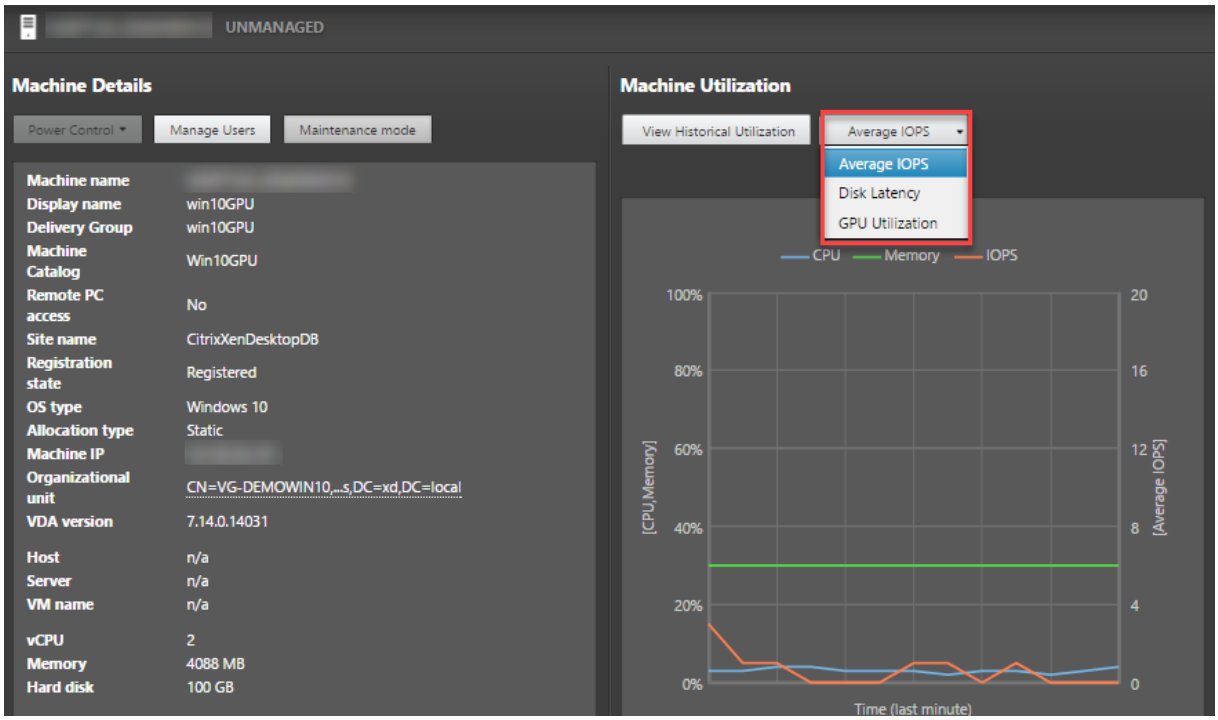
Klicken Sie auf Link mit dem Maschinennamen, um die Seite **Maschinendetails** aufzurufen.

Die Seite “Maschinendetails”enthält die Einzelheiten zu der Maschine, der Infrastruktur und den auf die Maschine angewandten Hotfixes.

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 Server- oder Einzelsitzungs-OS-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-Einzelsitzungs-OS sowie GPU-Beschleunigung

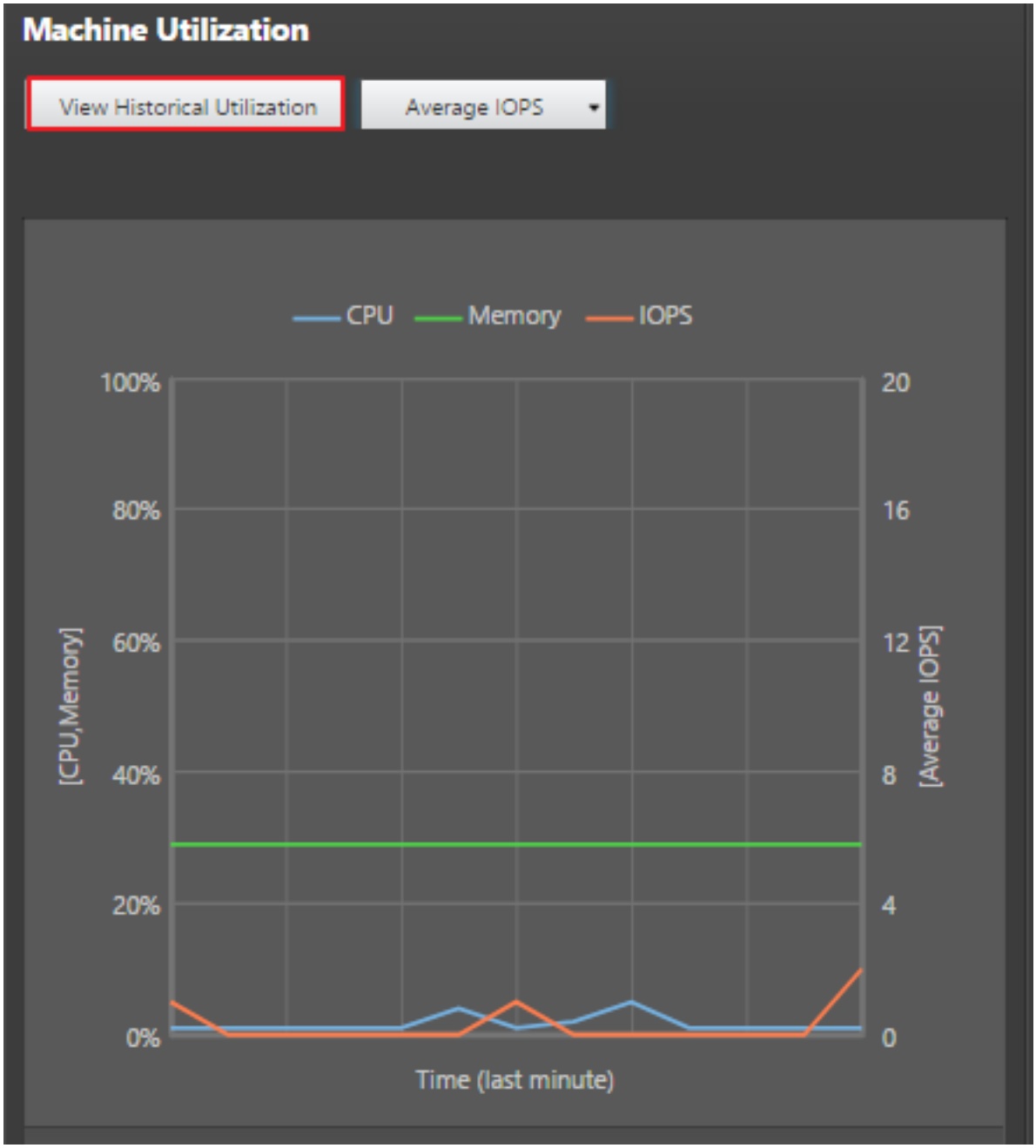
für Windows-Multisitzungs-OS.
Wenn ein VDA auf mehrere GPUs greift, zeigt das Auslastungsdiagramm den Durchschnitt der bei den einzelnen GPUs gesammelten Kennzahlen. GPU-Kennzahlen werden für den gesamten VDA und nicht für einzelne Prozesse gesammelt.

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.

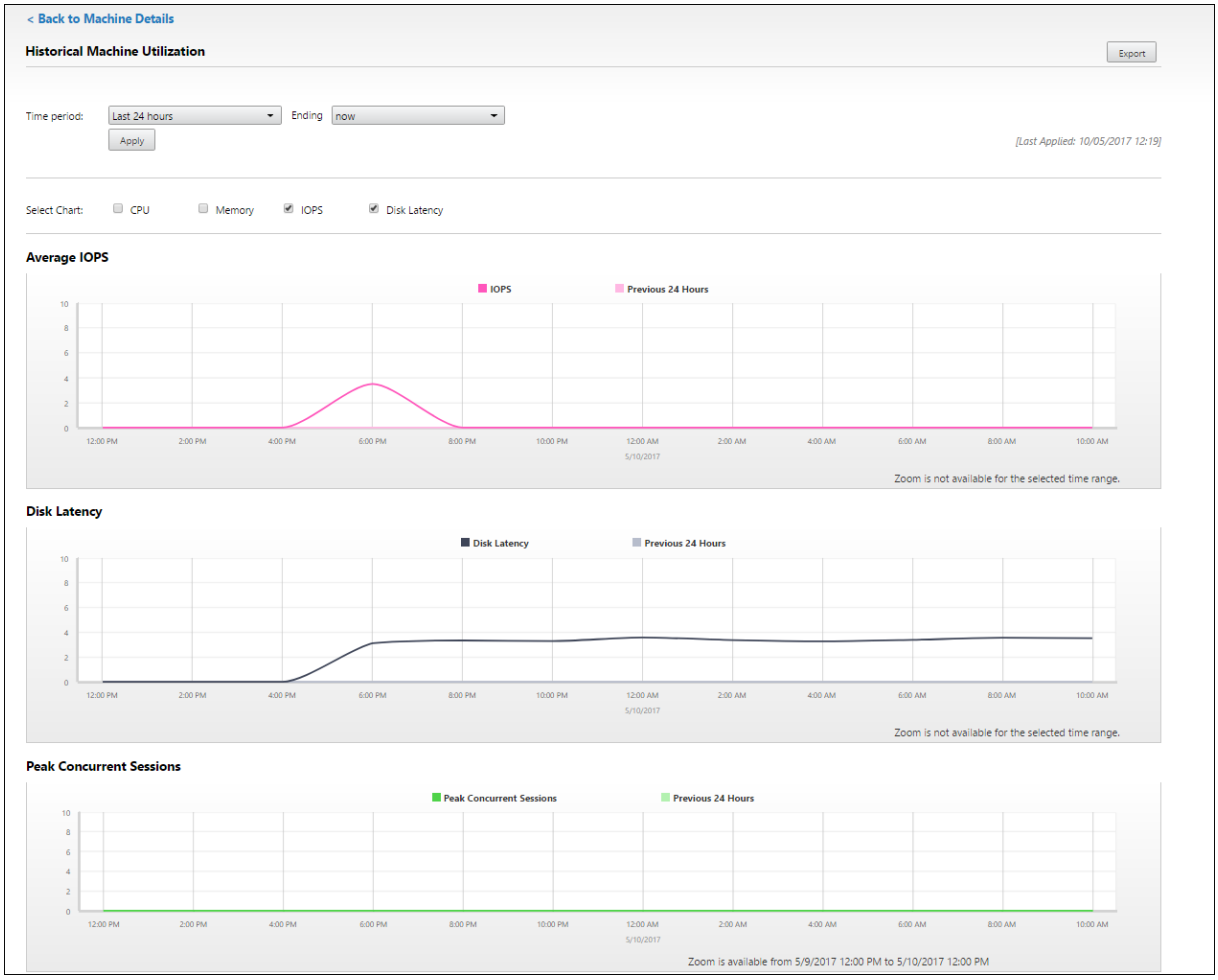


1. Wählen Sie im Bereich **Maschinenauslastung** der Ansicht **Maschinendetails** die Option **Historische Auslastung anzeigen**.
2. Legen Sie auf der Seite **Historische Maschinenauslastung** die Option **Zeitraum** auf die letzten 2 oder 24 Stunden, auf die letzten 7 Tage, den letzten Monat oder das 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.

1. 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.
2. Unterhalb der Diagramme wird eine Tabelle mit den 10 Prozessen mit der höchsten CPU- bzw. Speicherauslastung angezeigt. Sie können diese nach einer beliebigen Spalte (Anwen-

dungsname, Benutzername, Sitzungs-ID, CPU-Durchschnitt, CPU-Maximum, Speicherdurchschnitt und Speichermaximum) sortieren. Die Spalten für IOPS und Datenträgerlatenz können nicht sortiert werden.

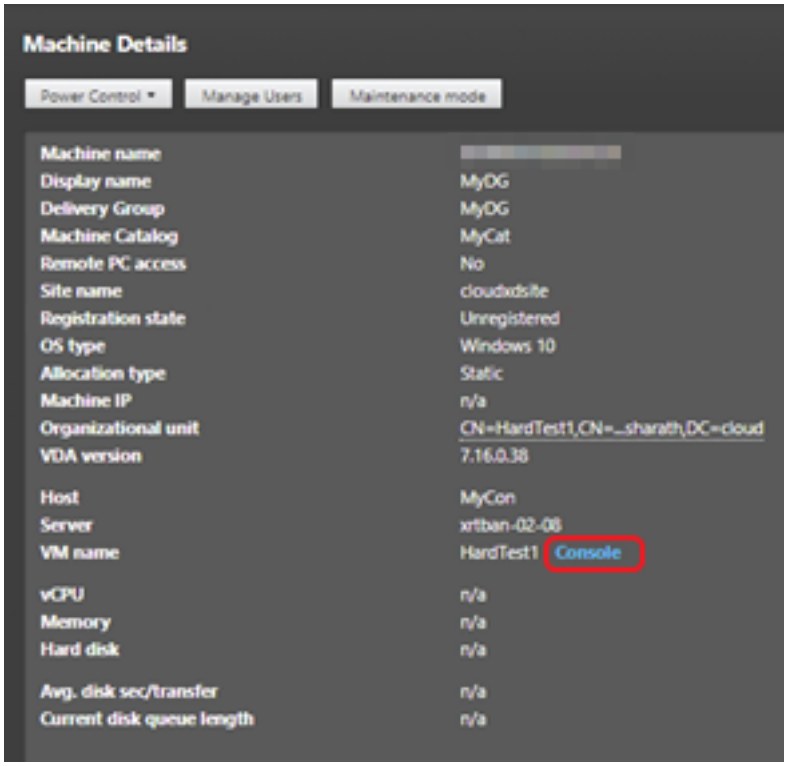
> **Hinweis:**
> Die Sitzungs-ID für Systemprozesse wird mit "0000"angegeben.

3. Zum Anzeigen des historischen Trends für den Ressourcenverbrauch einzelner Prozesse können Sie einen Drilldown für jeden der aufgelisteten Top-10-Prozesse durchführen.

Zugriff auf die Maschinenkonsole

Sie können auf die Konsolen von Maschinen mit Einzelsitzungs-OS und Multisitzungs-OS, die unter XenServer ab Version 7.3 gehostet werden, direkt von Director aus zugreifen. XenCenter ist dann nicht zur Problembehandlung von auf XenServer gehosteten VDAs erforderlich. Das Feature erfordert Folgendes:

- Delivery Controller ab Version 7.16
- Der XenServer, der die Maschine hostet, muss Version 7.3 oder höher haben und über die Director-Benutzeroberfläche zugänglich sein.



Zur Problembehandlung auf einer Maschine klicken Sie im zugehörigen Bereich "Maschinendetails" auf den Link **Konsole**. Nach Authentifizierung der von Ihnen angegebenen Hostanmeldeinformatio-

nen wird die Maschinenkonsole mit dem webbasierten VNC-Client noVNC auf einer separaten Registerkarte geöffnet. Sie haben nun über Tastatur und Maus Zugriff auf die Konsole.

> **Hinweis:**
>
> - Das Feature wird unter Internet Explorer 11 nicht unterstützt.
> - Ist der Mauszeiger auf der Maschinenkonsole nicht korrekt ausgerichtet, finden Sie unter CTX230727 einen Fix.
> - Der Konsolenzugriff wird von Director auf einer neuen Registerkarte gestartet. Vergewissern Sie sich daher, dass Ihre Browsereinstellungen Popups zulassen.
> - Citrix empfiehlt aus Sicherheitsgründen die Installation von SSL-Zertifikaten in Ihrem Browser.

Microsoft RDS-Lizenzstatus

Sie können den Status der Lizenz für Microsoft RDS (Remotedesktopdienste) im Fenster "Maschinendetails"auf den Seiten **Maschinendetails** und **Benutzerdetails** auf Maschinen mit Multisitzungs-OS anzeigen.

Eine der folgenden Meldungen wird angezeigt:

- Lizenz verfügbar
- Nicht richtig konfiguriert (Warnung)
- Lizenzfehler (Fehler)
- Nicht kompatible VDA-Version (Fehler)

> **Hinweis:**
> Der Status der Microsoft RDS-Lizenz für Maschinen mit gültiger Lizenz im Kulanzzeitraum wird als **Lizenz verfügbar** in grün angezeigt. Erneuern Sie die Lizenzen, bevor sie ablaufen.

Zum Anzeigen von Warn- und Fehlermeldungen (siehe Tabelle unten) zeigen Sie mit der Maus auf das Infosymbol.

Meldungstyp	Meldungen in Director
Fehler	Verfügbar ab VDA-Version 7.16
Fehler	Neue RDS-Verbindungen sind nicht erlaubt.
Fehler	Die Microsoft RDS-Lizenzierung hat den Kulanzzeitraum überschritten.
Fehler	Ein Lizenzserver ist nicht für die erforderliche Betriebssystemstufe mit dem Lizenztyp ‘Pro Gerät-Clientzugriffslizenz’konfiguriert.
Fehler	Der konfigurierte Lizenzserver ist nicht kompatibel mit der RDS-Hostbetriebssystemstufe des Lizenztyps ‘Pro Gerät-Clientzugriffslizenz’.
Warnung	‘Persönlicher Terminalserver’ist kein gültiger RDS-Lizenztyp in einer Citrix Virtual Apps and Desktops-Bereitstellung.
Warnung	‘Remotedesktop für Verwaltung’ist in einer Citrix Virtual Apps and Desktops-Bereitstellung kein gültiger Lizenztyp.
Warnung	Kein RDS-Lizenztyp konfiguriert.
Warnung	Mit dem Lizenztyp ‘Per User Client Access RDS’ ist der Domänencontroller oder Lizenzserver nicht erreichbar.
Warnung	Mit dem Lizenztyp ‘Pro Gerät-Clientzugriffslizenz’konnte die Clientgerätelizenz nicht ermittelt werden, da der Lizenzserver für die erforderliche Betriebssystemstufe nicht erreichbar ist.

> **Hinweis:**
> Diese Funktion gilt nur für Microsoft RDS-CAL (Client Access License).

Behandeln von Benutzerproblemen

March 9, 2022

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
Sitzungsstart dauert lange oder schlägt periodisch oder wiederholt fehl	Diagnostizieren von Problemen beim Sitzungsstart
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.

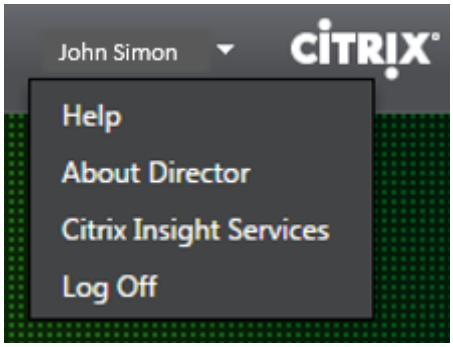
Die Suchergebnisse schließen auch Benutzer ein, die derzeit keine Maschine verwenden bzw. keiner Maschine zugewiesen sind.

- 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 Citrix Virtual Apps and Desktops-Komponenten installiert. Je nach Windows-Version erscheint Scout im Startmenü bzw. Startbildschirm nach der Installation von (bzw. einem Upgrade auf) Citrix Virtual Apps and Desktops.

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.

Diagnose von Sitzungsstartproblemen

May 24, 2024

Zusätzlich zu den in Abschnitt Diagnose von Benutzeranmeldeproblemen genannten Anmeldeprozessphasen zeigt Director die Dauer des Sitzungsstarts an. Diese ist unterteilt in die Dauer des Workspace App-Sitzungsstarts und die des VDA-Sitzungsstarts auf den Seiten **Benutzerdetails** und **Maschinendetails**. Diese beiden Prozesse sind ihrerseits in Phasen unterteilt, deren Dauer ebenfalls angezeigt wird. Anhand dieser Daten können Sie Verzögerungen beim Sitzungsstart auf den Grund gehen und beheben. Darüber hinaus lassen sich anhand der Angaben zur Zeitdauer der einzelnen Sitzungsstartphasen Probleme mit diesen Phasen gezielt beheben. Wenn beispielsweise die Dauer der Laufwerkzuordnung lang ist, können Sie überprüfen, ob alle gültigen Laufwerke im Gruppenrichtlinienobjekt oder Skript korrekt zugeordnet sind. Das Feature ist ab Delivery Controller-Version 7 1906 und ab VDA-Version 1903 verfügbar.

Voraussetzungen

Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind, damit Daten zur Dauer des Sitzungsstarts angezeigt werden:

- Delivery Controller 7 1906 oder höher.
- VDA 1903 oder höher.
- Der Dienst Citrix End User Experience Monitoring (EUEM) wird auf dem VDA ausgeführt.

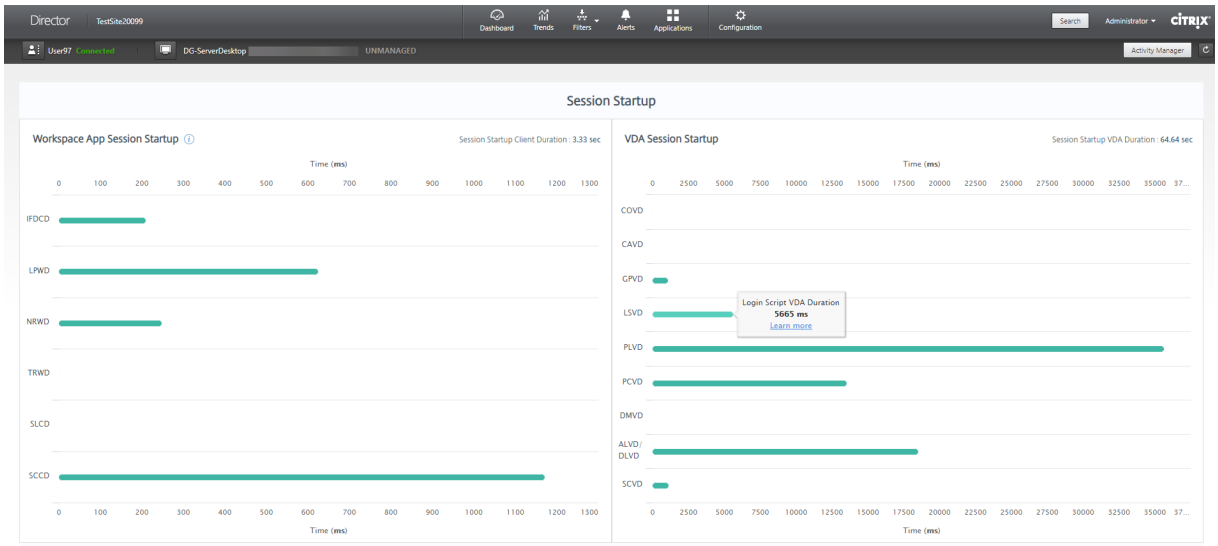
Einschränkungen

Die folgenden Einschränkungen gelten bei der Anzeige der Startdauerdaten in Director.

- Die Sitzungsstartdauer ist nur für HDX-Sitzungen verfügbar.

- Für iOS- und Android OS-Sitzungsstarts ist nur die VDA-Startdauer verfügbar.
- Die Dauer des ICA-Dateidownloads (IFDCD) ist nur verfügbar, wenn die Workspace-App beim Starten von einem Browser erkannt wird.
- Für Mac OS-Sitzungsstarts ist die IFDCD nur ab Workspace-App-Version 1902 verfügbar.
- Für Windows OS-Sitzungsstarts ist die IFDCD für Workspace-App-Version ab 1902 verfügbar. In früheren Versionen wird die IFDCD nur für App-Starts aus dem Browser unter Erkennung der Workspace-App angezeigt.

> Hinweise:
>
> - Treten bei der Anzeige der Sitzungsstartdauer Probleme auf, obwohl die Voraussetzungen erfüllt sind, überprüfen Sie das Director-Serverprotokoll und das VDA-Protokoll (siehe CTX130320). Für gemeinsam genutzte Sitzungen (mehrere Anwendungen in einer Sitzung gestartet) werden die Workspace-App-Kennzahlen für die neueste Verbindung bzw. den letzten Anwendungsstart angezeigt.
> - Einige Kennzahlen des VDA-Sitzungsstarts gelten nicht bei Wiederverbindungen. In solchen Fällen wird eine Meldung angezeigt.



Phasen des Workspace-App-Sitzungsstarts

Sitzungsstartdauer auf Client (SSCD)

Ist der Wert hoch, deutet dies auf ein clientseitiges Problem hin, das eine lange Startdauer verursacht. Überprüfen Sie nachfolgende Kennzahlen, um die Ursache des Problems zu ermitteln. Dies beginnt möglichst nah am Zeitpunkt der Anforderung (Mausklick) und endet bei Herstellung der ICA-Verbindung zwischen dem Clientgerät und VDA. Bei einer gemeinsamen Sitzung ist diese Dauer viel

geringer, da ein Großteil der mit der Erstellung einer neuen Verbindung zum Server verbundenen Einrichtung entfällt. Auf der nächsten Ebene darunter stehen mehrere detaillierte Kennzahlen zur Verfügung.

Dauer des ICA-Dateidownloads

Dies ist die Zeit, die das Herunterladen der ICA-Datei vom Server auf den Client in Anspruch nimmt. Der Gesamtprozess ist folgender:

1. Der Benutzer klickt in der Workspace-Anwendung auf eine Ressource (Anwendung oder Desktop).
2. Eine Anforderung wird über Citrix Gateway (falls konfiguriert) an StoreFront und von dort an den Delivery Controller gesendet.
3. Der Delivery Controller sucht eine verfügbare Maschine und sendet die Maschineninformationen und weitere Details an StoreFront. Außerdem fordert StoreFront ein einmaliges Ticket von der Secure Ticket Authority an.
4. StoreFront generiert eine ICA-Datei und sendet sie über Citrix Gateway (falls konfiguriert) an den Benutzer.

IFDCD entspricht der Zeit, die für den gesamten Prozess benötigt wird (Schritte 1–4). Die IFDCD-Dauer endet, wenn der Client die ICA-Datei empfängt.

LPWD ist der StoreFront-Teil des Prozesses.

Wenn IFDCD hoch und LPWD normal ist, war die serverseitige Verarbeitung des Starts erfolgreich, aber es gab Kommunikationsprobleme zwischen dem Clientgerät und StoreFront. Ursache sind Netzwerkprobleme zwischen den beiden Maschinen. Behandeln Sie in diesem Fall ggf. mögliche Netzwerkprobleme.

Dauer des Seitenstarts auf Webserver (LPWD)

Dies ist die Zeit für die Verarbeitung der Startseite (launch.aspx) in StoreFront. Ist der LPWD-Wert hoch, liegt bei StoreFront ggf. ein Engpass vor.

Mögliche Ursachen:

- Hohe Last in StoreFront. Suchen Sie die Ursache der Verzögerung in den Protokollen von IIS, Überwachungstools, Task-Manager, Systemmonitor usw.
- Kommunikationsprobleme zwischen StoreFront und anderen Komponenten, z. B. Delivery Controllern. Prüfen Sie, ob die Netzwerkverbindung zwischen StoreFront und Delivery Controllern langsam ist oder ob Delivery Controller ausgefallen oder überlastet sind.

Dauer der Namensauflösung auf Webserver (NRWD)

Dies ist die Zeit, die der Delivery Controller zum Auflösen des Namens einer veröffentlichten Anwendung/eines veröffentlichten Desktops in eine VDA-IP-Adresse braucht.

Ist der Wert hoch, bedeutet dies, dass der Delivery Controller lange braucht, um den Namen einer veröffentlichten Anwendung in eine IP-Adresse aufzulösen. Mögliche Ursachen sind ein Problem auf dem Client, Probleme mit dem Delivery Controller, z. B. der Überlastung, oder ein Problem mit der Netzwerkverbindung zwischen diesen Maschinen.

Dauer der Antwort auf Tickets für Webserver (TRWD)

Dies ist die Zeit, die für den Abruf eines Tickets (falls erforderlich) vom Secure Ticket Authority-Server (STA) oder dem Delivery Controller benötigt wird. Ist der Wert hoch, deutet dies auf eine Überlastung des STA-Servers bzw. Delivery Controllers hin.

Sitzungslookupdauer auf Client (SLCD)

Dies ist die Zeit, die benötigt wird, um jede Sitzung zum Hosten der angeforderten veröffentlichten Anwendung abzufragen. Die Überprüfung wird auf dem Client durchgeführt, um festzustellen, ob eine bestehende Sitzung die Anforderung zum Starten der Anwendung verarbeiten kann. Die verwendete Methode hängt davon ab, ob die Sitzung neu ist oder gemeinsam genutzt wird.

Sitzungserstellungsdauer auf Client (SCD)

Dies ist die Zeit, die das Erstellen einer Sitzung ab dem Starten von wfica32.exe (oder einer äquivalenten Datei) bis zum Herstellen der Verbindung dauert.

Phasen des VDA-Sitzungsstarts

Sitzungsstartdauer auf VDA (SSVD)

Diese serverseitige Kennzahl entspricht der Zeit, die der VDA für den gesamten Startvorgang benötigt. Ist der Wert hoch, deutet dies auf ein VDA-seitiges Problem hin, das eine lange Startdauer verursacht. Dies umfasst die Zeit, die der VDA für den gesamten Startprozess benötigt.

Dauer des Anmeldeinformationsabrufs auf VDA (COVD)

Die Zeit, die der VDA zum Abrufen der Benutzeranmeldeinformationen benötigt.

Die Dauer kann sich erhöhen, wenn ein Benutzer die Anmeldeinformationen nicht zügig eingibt, sie wird daher nicht in die VDA-Startdauer eingerechnet. Die Dauer ist in der Regel nur relevant, wenn eine manuelle Anmeldung verwendet wird und das serverseitige Anmeldedialogfeld angezeigt wird (oder wenn ein Rechtshinweis vor Beginn der Anmeldung angezeigt wird).

Dauer der Authentifizierung von Anmeldeinformationen auf VDA (CAVD)

Dies ist die Zeit, die der VDA für die Authentifizierung der Anmeldeinformationen des Benutzers anhand des Authentifizierungsanbieters benötigt (Kerberos, Active Directory oder ein SSPI).

Gruppenrichtliniendauer für VDA (GPVD)

Dies ist die Zeit, die für das Anwenden von Gruppenrichtlinienobjekten während der Anmeldung benötigt wird.

Anmeldeskriptdauer für VDA (LSVD)

Dies ist die Zeit, die der VDA zum Ausführen der Anmeldeskripts des Benutzers benötigt.

Erwägen Sie, die Anmeldeskripts des Benutzers oder der Gruppe asynchron zu machen. Erwägen Sie, Anwendungskompatibilitätsskripts zu optimieren oder stattdessen Umgebungsvariablen zu verwenden.

Profilladedauer für VDA (PLVD)

Dies ist die Zeit, die der VDA zum Laden des Benutzerprofils in Anspruch nimmt.

Ist der Wert hoch, prüfen Sie die Benutzerprofilkonfiguration. Die Größe und der Speicherort von Roamingprofilen wirken sich auf die Dauer von Sitzungsstarts aus. Wenn ein Benutzer sich an einer Sitzung anmeldet, in der Terminaldienste-Roamingprofile und -Basisordner aktiviert sind, werden die Roamingprofilinhalte und der Zugriff auf diesen Ordner während der Anmeldung zugeordnet, wodurch zusätzliche Ressourcen benötigt werden. Dies kann zu einer erheblichen CPU-Auslastung führen. Verwenden Sie Terminaldienste-Basisordner mit umgeleiteten persönlichen Ordnern, um dieses Problem zu beheben. Verwenden Sie allgemein ggf. die Citrix Profilverwaltung für Benutzerprofile in Citrix Umgebungen. Wenn Sie die Citrix Profilverwaltung verwenden und die Anmeldedauer hoch ist, prüfen Sie, ob Ihre Antivirensoftware die Citrix Profilverwaltung blockiert.

Dauer der Druckererstellung auf VDA (PCVD)

Dies ist die Zeit, die der VDA benötigt, um die Clientdrucker des Benutzers synchron zuordnen. Ist die asynchrone Druckererstellung konfiguriert, wird kein PCVD-Wert aufgezeichnet, da sie sich nicht auf den Sitzungsstart auswirkt.

Ein hoher Zeitaufwand für die Zuordnung von Druckern wird oft von den Richtlinieneinstellungen für die automatische Druckererstellung verursacht. Die Anzahl der lokal auf den Clientgeräten der Benutzer hinzugefügten Drucker und die Druckkonfiguration können sich direkt auf die Sitzungsstartdauer auswirken. Beim Start einer Sitzung muss Citrix Virtual Apps and Desktops jeden lokal zugeordneten Drucker auf dem Clientgerät erstellen. Konfigurieren Sie evtl. die Druckrichtlinien neu, um die Anzahl der erstellten Drucker zu verringern, insbesondere wenn Benutzer viele lokale Drucker haben. Bearbeiten Sie hierzu die Richtlinie "Druckererstellung"auf dem Delivery Controller und in Citrix Virtual Apps and Desktops.

Dauer der Laufwerkzuordnung auf VDA (DMVD)

Dies ist die Zeit, die der VDA für die Zuordnung der Clientlaufwerke, -geräte und -ports des Benutzers in Anspruch nimmt.

Stellen Sie sicher, dass die Basisrichtlinien Einstellungen zum Deaktivieren nicht verwendeter virtueller Kanäle (z. B. Audio- oder COM-Portzuordnung) enthalten, um das ICA-Protokoll zu optimieren und die Gesamtsitzungsleistung zu verbessern.

Startdauer von Anwendung/Desktop für VDA (ALVD/DLVD)

Diese Phase ist die kombinierte aus UserInit- und Shell-Dauer. Wenn sich ein Benutzer bei einem Windows-Computer anmeldet, führt Winlogon userinit.exe aus. Userinit.exe führt Anmeldeskripts aus, stellt Netzwerkverbindungen wieder her und startet dann explorer.exe die Windows-Benutzeroberfläche. Userinit repräsentiert die Dauer zwischen dem Start von userinit.exe bis zum Start der Benutzeroberfläche des virtuellen Desktops oder der Anwendung. Die Shell-Phase ist die Dauer zwischen der Initialisierung der Benutzeroberfläche und dem Zeitpunkt, zu dem der Benutzer die Kontrolle über Tastatur und Maus erhält.

Dauer der Sitzungserstellung auf VDA (SCVD)

Diese Zeit umfasst verschiedene Verzögerungen bei der Erstellung der Sitzung auf dem VDA.

Diagnose von Benutzeranmeldeproblemen

December 8, 2022

Mit den Anmeldedauerdaten können Sie Benutzeranmeldeprobleme beheben.

Die Anmeldedauer wird nur bei der ersten Verbindung mit einem Desktop oder einer App über HDX gemessen. Diese Daten umfassen keinen Verbindungsversuch über RDP oder die Wiederverbindung getrennter Sitzungen. Insbesondere wird die Anmeldedauer nicht gemessen, wenn ein Benutzer sich anfänglich mit einem anderen Protokoll als HDX verbindet und bei der Wiederverbindung HDX verwendet.

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 Citrix Virtual Apps and Desktops anmelden, verfolgt der Überwachungsdienst die Phasen des Anmeldeprozesses ab Herstellung der Verbindung über die Citrix Workspace-App 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) angezeigt.

Voraussetzungen

Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind, damit Daten zur Anmeldedauer und Drilldowns angezeigt werden:

1. Installieren Sie **Citrix User Profile Manager** und das **Citrix User Profile Manager-WMI-Plug-In** auf dem VDA.
2. Stellen Sie sicher, dass der Citrix Profilverwaltungsdienst ausgeführt wird.
3. Deaktivieren Sie die GPO-Einstellung **Herkömmliche Ausführungsliste nicht verarbeiten**, in XenApp und XenDesktop-Sites der Version bis einschließlich 7.15.
4. "Prozessverfolgung überwachen"muss für den Drilldown interaktiver Sitzungen aktiviert sein.
5. Erhöhen Sie für den GPO-Drilldown die Größe der Gruppenrichtlinien-Betriebsprotokolle.

> **Hinweis:**
> Die Anmeldedauer wird nur auf der Standard-Windows-Shell (explorer.exe) und nicht auf benutzerdefinierten Shells unterstützt.

Beheben von Benutzeranmeldeproblemen

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.

Phasen des Anmeldeprozesses

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

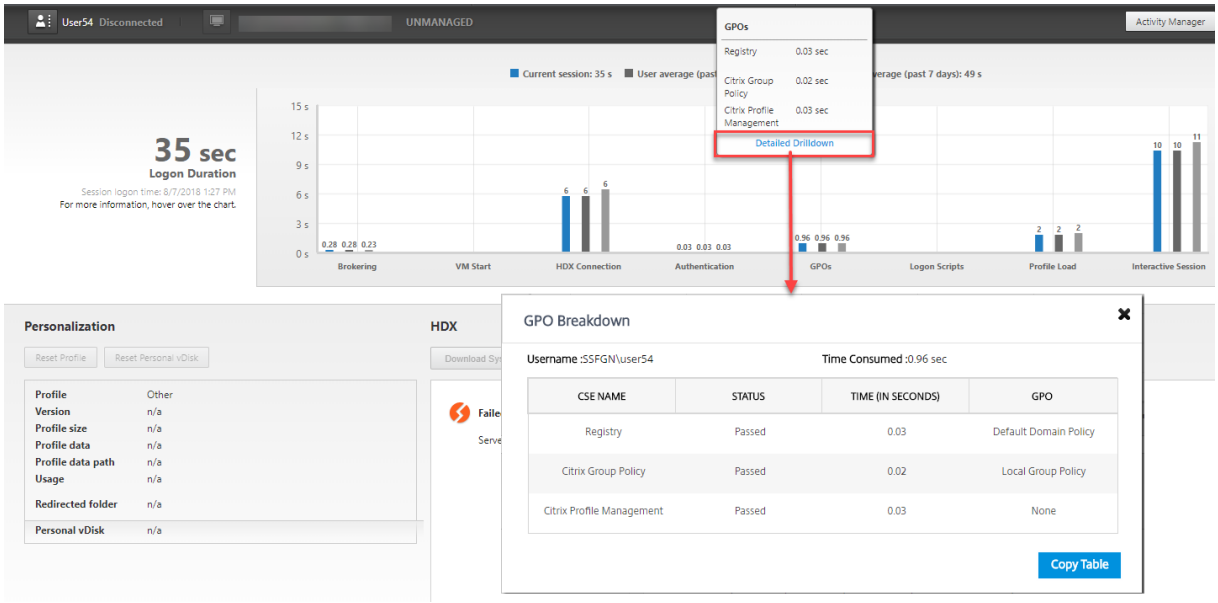
Zum Einrichten der HDX-Verbindung vom Client zur virtuellen Maschine benötigte Zeit.

Authentifizierung

Zum Abschließen der Authentifizierung bei der Remotesitzung benötigte Zeit.

Gruppenrichtlinienobjekte

Zum Anwenden von Gruppenrichtlinienobjekten benötigte Zeit, wenn bei der Anmeldung Gruppenrichtlinieneinstellungen auf den virtuellen Maschinen aktiviert sind. Die Aufschlüsselung der für die Anwendung der einzelnen Richtlinien gemäß CSE (clientsseitige Erweiterungen) benötigten Zeit wird als QuickInfo angezeigt, wenn mit der Maus auf die GPO-Leiste zeigen.



Klicken Sie auf **Detaillierter Drilldown**, um eine Tabelle mit dem Richtlinienstatus und dem entsprechenden GPO-Namen anzuzeigen. Die Zeitangaben im Drilldown repräsentieren nur die CSE-Verarbeitungszeit und nicht die gesamte GPO-Dauer. Sie können die Drilldowntabelle zur weiteren Fehlerbehebung oder zur Verwendung in Berichten kopieren. Die GPO-Zeit für die Richtlinien wird aus den Ereignisanzeigeprotokollen abgerufen. Die Protokolle können je nach dem für die Betriebsprotokolle zugewiesenen Speicher (Standardwert = 4 MB) überschrieben werden. Weitere Informationen zum Erhöhen der Größe der Betriebsprotokolle finden Sie im Microsoft-Artikel zum Konfigurieren von Ereignisprotokollen.

Anmeldeskripts

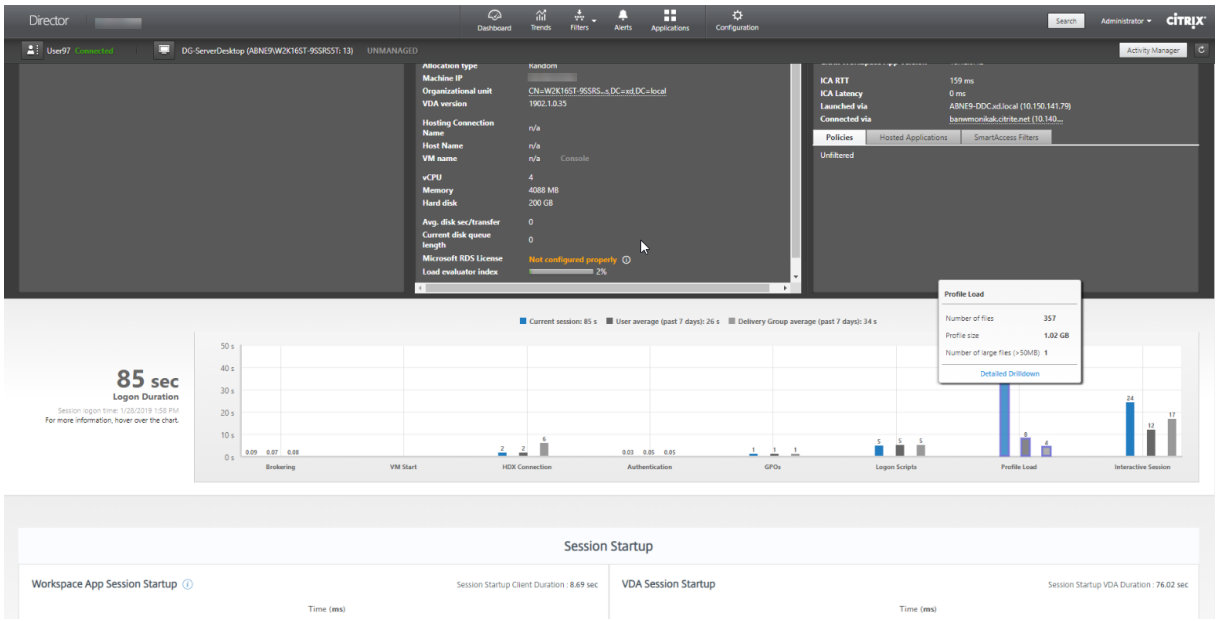
Zum Ausführen von Anmeldeskripts benötigte Zeit, wenn Anmeldeskripts für die Sitzung konfiguriert sind.

Profilladezeit

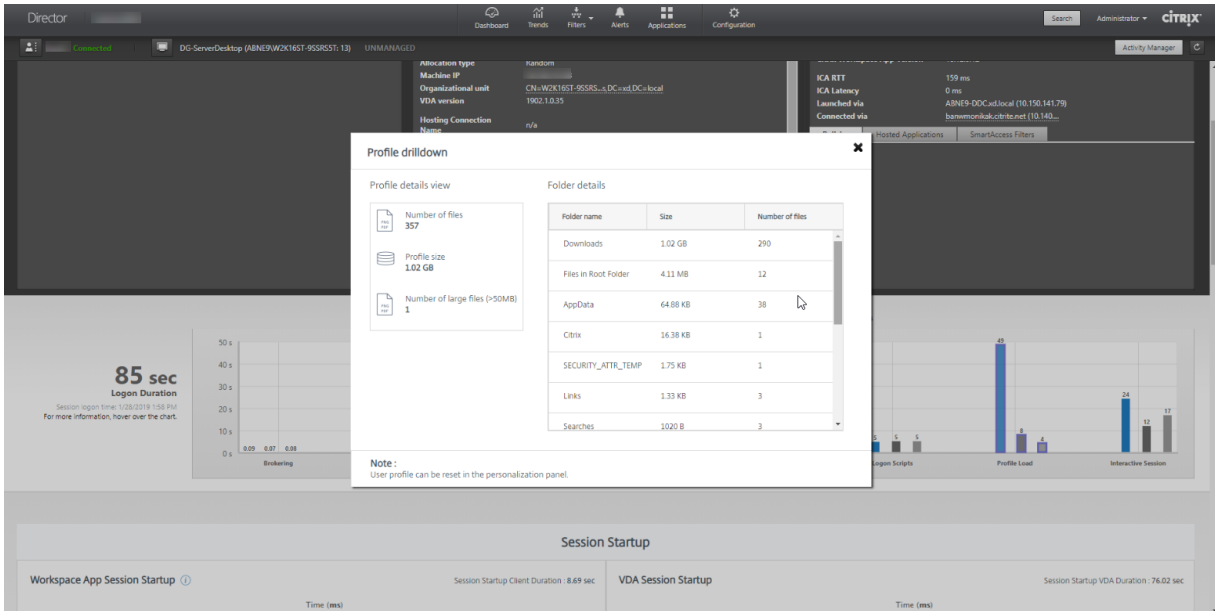
Zum Laden des Profils benötigte Zeit, wenn für den Benutzer Profileinstellungen auf der virtuellen Maschine konfiguriert sind.

Wenn die Citrix Profilverwaltung konfiguriert ist, wird die Dauer der Profilverarbeitung durch die Profilverwaltung im Balken “Profilladezeit”angezeigt. Anhand dieser Informationen ist eine gezieltere Problembehandlung bei langsamer Profilverarbeitung möglich. Wenn die Profilverwaltung konfiguriert ist, wird eine erhöhte Dauer im Balken “Profilladezeit”angezeigt. Der Anstieg der Dauer begründet sich durch diese Erweiterung und bedeutet keine Leistungseinbuße. Diese Erweiterung ist bei VDAs der Version 1903 und höher verfügbar.

Wenn Sie mit der Maus auf die Profilladezeitleiste zeigen, wird eine QuickInfo mit den Benutzerprofildetails der aktuellen Sitzung angezeigt.



Klicken Sie auf **Detaillierter Drilldown**, um Informationen zu den einzelnen Ordnern im Profilstammordner (z. B. C:/Users/username), dessen Größe und die Zahl der enthaltenen Dateien (einschließlich solcher in verschachtelten Ordnern) anzuzeigen.



Der Profildrilldown ist ab Delivery Controller-Version 7 1811 und ab VDA-Version 1811 verfügbar. Anhand der Profildrilldown-Informationen können Sie Probleme lösen, die das Laden von Profilen verlangsamen. Sie haben folgende Möglichkeiten:

- Zurücksetzen des Benutzerprofils

- Optimieren des Profils durch Entfernen unerwünschter, großer Dateien
- Reduzieren der Anzahl Dateien zur Verringerung der Netzwerklast
- Verwenden von Profilstreaming

Standardmäßig werden alle Ordner im Profilstamm im Drilldown angezeigt. Um Ordner auszublenden, bearbeiten Sie folgenden Registrierungswert auf der VDA-Maschine:

> 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. Fügen Sie auf dem VDA den Wert **ProfileFoldersNameHidden** für HKEY_LOCAL_MACHINE\Software\Citrix\Di hinzu.1. Legen Sie den Wert auf 1 fest. Der Wert muss ein DWORD-Wert (32-Bit) sein. Die Anzeige der Ordnernamen ist damit deaktiviert.
2. Um die Ordnernamen wieder einzublenden, legen Sie den Wert auf 0 fest.

> **Hinweis:**
> Sie können die Registrierungswertänderung über die GPO oder PowerShell-Befehle auf mehrere Maschinen anwenden. Weitere Informationen zum Ändern von Registrierungswerten per GPO finden Sie in diesem Blog.

Weitere Informationen

- Beim Profildrilldown werden umgeleitete Ordner nicht berücksichtigt.
- Die NTUser.dat-Dateien im Stammordner sind für Endbenutzer möglicherweise nicht sichtbar. Sie sind jedoch im Profildrilldown enthalten und werden in der Liste der Dateien unter **Stammordner** angezeigt.
- Einige verborgene Dateien im Ordner “AppData”sind nicht im Profildrilldown enthalten.
- Die Anzahl der Dateien und Profilgrößendaten stimmen aufgrund bestimmter Windows-Einschränkungen möglicherweise nicht mit den Daten unter “Personalisierung”überein.

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**

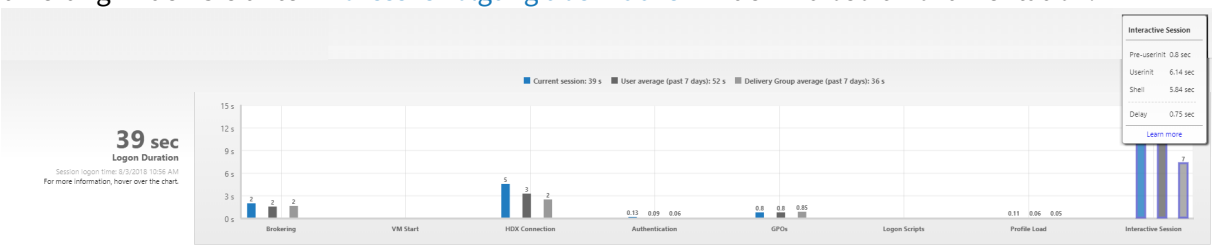
auf VDA). Die interaktive Sitzung hat drei Teilphasen: Pre-Userinit, Userinit und Shell. Durch Zeigen auf "Interaktive Sitzung"wird eine QuickInfo mit den Teilphasen, der Zeitdauer jeder Teilphase, der kumulativen Zeitverzögerung zwischen den Teilphasen und einem Link zur Dokumentation angezeigt.

> Hinweis:
>
> Dieses Feature ist ab VDA-Version 1811 verfügbar. Wenn Sie Sitzungen auf Sites vor Version 7.18 gestartet haben und dann ein Upgrade auf 7.18 oder höher durchführen, wird die Meldung "Drilldown aufgrund eines Serverfehlers nicht verfügbar"angezeigt. Wenn Sie hingegen Sitzungen nach dem Upgrade gestartet haben, wird keine Fehlermeldung angezeigt.

Um die Zeitdauer jeder Teilphase anzuzeigen, aktivieren Sie die Überwachung der Prozessverfolgung auf der VM (VDA). Wenn die Überwachung der Prozessverfolgung deaktiviert ist (Standardeinstellung), werden die Dauer der Teilphase Pre-Userinit und die kombinierte Dauer der Teilphasen Userinit und Shell angezeigt. Die Überwachung der Prozessverfolgung können Sie folgendermaßen über ein Gruppenrichtlinienobjekt aktivieren:

1. Erstellen Sie ein neues Gruppenrichtlinienobjekt, und bearbeiten Sie es mit dem Gruppenrichtlinienobjekt-Editor.
2. Rufen Sie Computerkonfiguration > Windows-Einstellungen > Sicherheitseinstellungen > Lokale Richtlinien > Überwachungsrichtlinie auf.
3. Doppelklicken Sie im rechten Fensterbereich auf **Prozessverfolgung überwachen**.
4. Wählen Sie **Erfolg** und klicken Sie auf "OK".
5. Wenden Sie das Gruppenrichtlinienobjekt auf die entsprechenden VDAs oder Gruppen an.

Weitere Informationen zur Überwachung der Prozessverfolgung und der Aktivierung bzw. Deaktivierung finden Sie unter Prozessverfolgung überwachen in der Microsoft-Dokumentation.



Bereich "Anmeldedauer"in der Ansicht "Benutzerdetails"

- **Interaktive Sitzung –Pre-Userinit:** Dieser Teil der interaktiven Sitzung überschneidet sich mit Gruppenrichtlinienobjekten und Skripts. Die Teilphase kann durch Optimierung der GPOs und Skripts verkürzt werden.
- **Interaktive Sitzung –Userinit:** Wenn sich ein Benutzer bei einem Windows-Computer anmeldet, führt Winlogon userinit.exe aus. Userinit.exe führt Anmeldeskripts aus, stellt Netzwerkverbindungen wieder her und startet dann explorer.exe die Windows-Benutzeroberfläche. Diese Teilphase der interaktiven Sitzung repräsentiert die Dauer zwischen dem Start von

userinit.exe bis zum Start der Benutzeroberfläche des virtuellen Desktops oder der Anwendung.

- **Interaktive Sitzung –Shell:** In der vorherigen Phase wurde von userinit die Initialisierung der Windows-Benutzeroberfläche begonnen. Die Shell-Teilphase erfasst die Dauer zwischen der Initialisierung der Benutzeroberfläche und dem Zeitpunkt, zu dem der Benutzer die Kontrolle über Tastatur und Maus erhält.
- **Verzögerung:** Dies ist die kumulative Verzögerung zwischen den Teilphasen **Pre-Userinit und Userinit** und den Teilphasen **Userinit und Shell**.

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.
Die Gesamtanmeldedauer umfasst nicht die ICA-Leerlaufzeit, d. h. die Zeit zwischen dem Herunterladen der ICA-Datei und dem Start der ICA-Datei für eine Anwendung.
Um das automatische Öffnen der ICA-Datei beim Start einer Anwendung zu ermöglichen, konfigurieren Sie den Browser so, dass ICA-Dateien nach dem Download automatisch gestartet werden. Weitere Informationen finden Sie unter CTX804493.

> **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.

Spiegeln von Benutzern

March 15, 2022

Mit dem Feature Benutzer spiegeln in Director können Sie die virtuelle Maschine oder Sitzung eines Benutzers direkt anzeigen und darauf arbeiten. Sie können Windows- und Linux-VDAs spiegeln. 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.

Die Spiegelung wird in einer neuen Registerkarte gestartet. Aktualisieren Sie Ihre Browsereinstellungen dahingehend, dass Popups von der Director-URL zugelassen sind.

Das Feature "Spiegeln"über die Ansicht **Benutzerdetails** aufgerufen. Sie wählen die Benutzersitzung und klicken dann auf **Spiegeln** in der Aktivitätsmanageransicht oder im Bereich "Sitzungsdetails".

Spiegeln von Linux-VDAs

Spiegeln ist bei Linux-VDAs ab Version 7.16 möglich, auf denen die Linux-Distribution RHEL7.3 oder Ubuntu Version 16.04 ausgeführt wird.

> **Hinweis:**
>
> - Für das Spiegeln muss die Director-Benutzeroberfläche Zugriff auf den VDA haben. Das Spiegeln ist daher nur bei Linux-VDAs möglich, die im selben Intranet wie der Director-Client sind.
> - Director verwendet den FQDN zum Herstellen einer Verbindung mit dem Linux-VDA. Vergewissern Sie sich, dass der Director-Client den FQDN des Linux-VDAs auflösen kann.
> - Auf dem VDA müssen die Pakete "python-websockify"und "x11vnc"installiert sein.
> - Die noVNC-Verbindung zum VDA verwendet das WebSocket-Protokoll. Standardmäßig wird das WebSocket-Protokoll (**ws://**) verwendet. Aus Sicherheitsgründen empfiehlt Citrix, das

> **wss://**-Protokoll zu verwenden. Installieren Sie SSL-Zertifikate auf jedem Director-Client und Linux-VDA.

Folgen Sie den Anweisungen unter Sitzungsspiegelung, um den VDA für die Spiegelung zu konfigurieren.

1. Nachdem Sie auf **Spiegeln** geklickt haben, wird die Spiegelungsverbindung initialisiert und auf dem Benutzergerät eine Bestätigungsaufforderung angezeigt.
2. Weisen Sie die Benutzer an, auf **Ja** zu klicken, um die Maschinen- oder die Sitzungsfreigabe zu starten.
3. Der Administrator kann nur die gespiegelte Sitzung anzeigen.

Spiegeln von Windows-VDAs

Windows-VDA-Sitzungen werden mithilfe der Windows-Remoteunterstützung gespiegelt. Aktivieren Sie die Windows-Remoteunterstützung bei der VDA-Installation. Weitere Informationen finden Sie im Artikel zur VDA-Installation unter Aktivieren oder Deaktivieren von Features.

1. Wenn Sie auf **Spiegeln** klicken, wird die Verbindung initialisiert und es erscheint ein Dialogfeld mit der Aufforderung, die MSRC-Incidentdatei zu öffnen oder zu speichern.
2. Öffnen Sie die Vorfalldatei mit dem Remoteunterstützung-Viewer, wenn er nicht standardmäßig ausgewählt ist. Auf dem Benutzergerät wird eine Bestätigungsaufforderung angezeigt.
3. Weisen Sie die Benutzer an, auf **Ja** zu klicken, um die Maschinen- oder die Sitzungsfreigabe zu starten.
4. 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.

Senden von Nachrichten an Benutzer

May 6, 2020

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 Benachrichtigungen über administrative Aktionen senden, wie bevorstehende Desktopwartung, Abmeldungen bzw. Neustarts von Maschinen und das Zurücksetzen von Profilen.

Gehen Sie folgendermaßen vor, um eine Nachricht an einen Benutzer zu senden:

1. Gehen Sie zu **Überwachen** > **Filter** > **Maschinen** > **Alle Maschinen**.
2. Wählen Sie die Maschine aus, an die Sie die Nachricht senden möchten, und klicken Sie auf **Nachricht senden**.
3. Geben Sie die Nachricht ein 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.

Beheben von Anwendungsstörungen

February 4, 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 Maschinen mit Multisitzungs-OS und Einzelsitzungs-OS 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 Maschinen mit Einzelsitzungs-OS: 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 Maschinen mit Multisitzungs-OS 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.

Wiederherstellen von Desktopverbindungen

February 6, 2020

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. Neustarten der Maschine des Benutzers	Achten Sie auf der Seite Benutzerdetails darauf, dass der Wartungsmodus deaktiviert ist. 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.

Wiederherstellen von Sitzungen

January 8, 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 Maschinen mit Multisitzungs-OS zur Verfügung. Für nicht vermittelte Sitzungen ist die Option deaktiviert.
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.

Ausführen von HDX-Kanalsystemberichten

January 8, 2021

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.

Zurücksetzen eines Benutzerprofils

January 8, 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.

Bei den zuvor erläuterten Schritten wird davon ausgegangen, dass Sie Citrix Virtual Desktops (Desktop-VDA) verwenden. Wenn Sie Citrix Virtual Desktops (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:

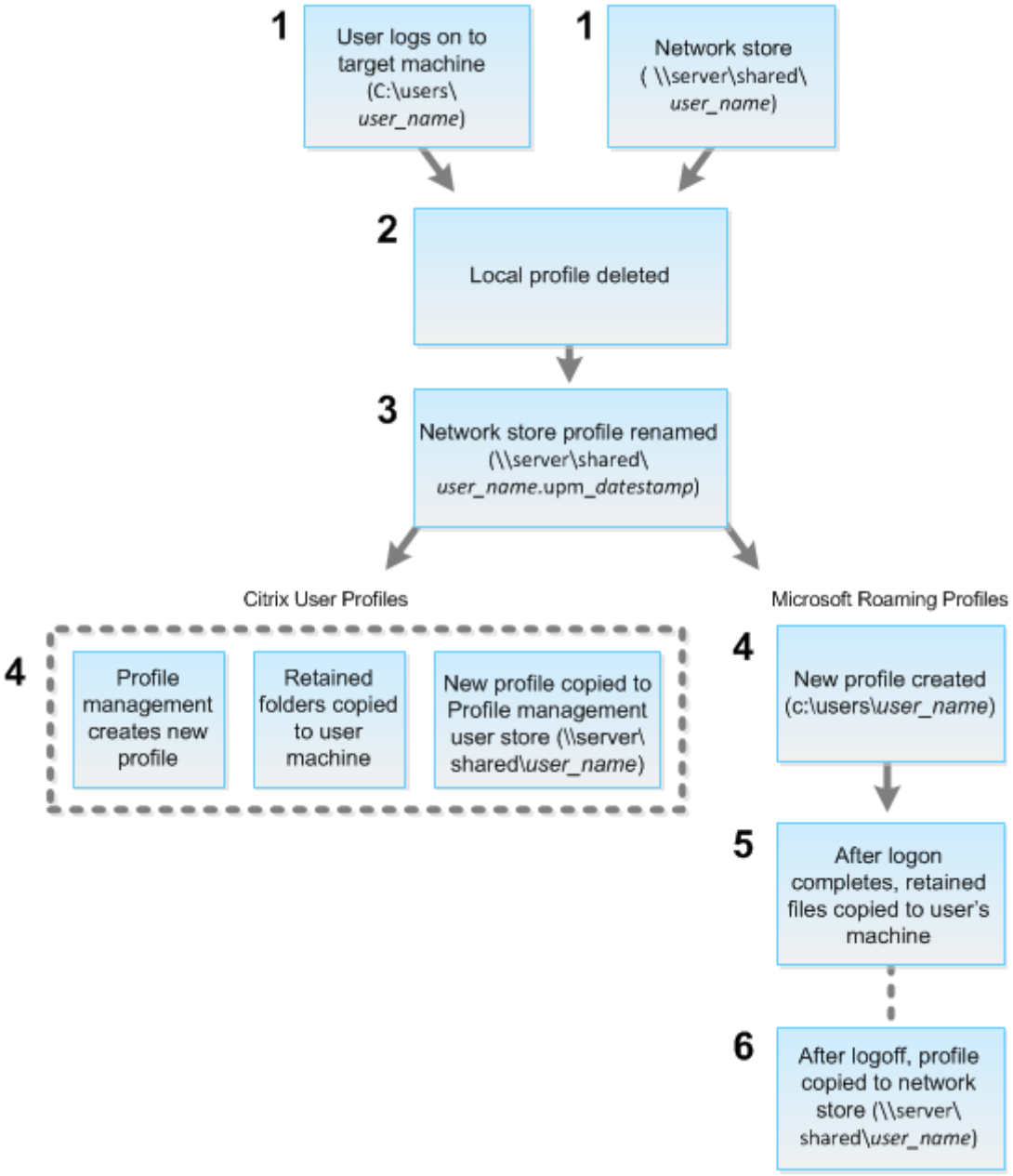
- Desktop
- Cookies
- Favoriten
- Dokumente
- Bilder
- Musik
- Videos

> **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, wenn ein Profil zurückgesetzt wird.



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).

1. Wenn ein lokales Profil vorhanden ist, wird es gelöscht.
2. Das Netzwerkprofil wird umbenannt.
3. 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. 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.

Zurücksetzen eines Profils mit dem PowerShell SDK

Sie können ein Profil mit dem Broker PowerShell SDK zurücksetzen.

New-BrokerMachineCommand

Erstellt einen Befehl, der für die Bereitstellung an einen bestimmten Benutzer, eine Sitzung oder eine bestimmte Maschine in der Warteschlange steht. Weitere Informationen zu diesem Cmdlet finden Sie unter https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerMachineCommand/.

Beispiele

Die folgenden Beispiele verdeutlichen das Zurücksetzen eines Profils mit den PowerShell-Cmdlets:

Zurücksetzen eines Profilverwaltungsprofils

- Angenommen, Sie möchten das Profil für Benutzer1 zurücksetzen. Verwenden Sie hierfür den PowerShell-Befehl New-BrokerMachineCommand. Beispiel:


```
- New-BrokerMachineCommand -Category UserProfileManager -CommandName
  "ResetUpmProfile"-DesktopGroups 1 -CommandData $byteArray -
  SendTrigger logon -user domain1\user1
```

> **Wichtig:**
>
> `CommandData $byteArray` muss im folgenden Format vorliegen: `<SID>[,<backup path>]`. Wenn Sie keinen Sicherungspfad angeben, wird automatisch ein Sicherungsordner erstellt und nach dem aktuellen Datum und der Uhrzeit benannt.

Zurücksetzen eines Windows-Roamingprofils

- Angenommen, Sie möchten das Roamingprofil für Benutzer1 zurücksetzen. Verwenden Sie hierfür den PowerShell-Befehl New-BrokerMachineCommand. Beispiel:

  ```
  - New-BrokerMachineCommand -Category UserProfileManager -CommandName
    "ResetRoamingProfile"-DesktopGroups 1 -CommandData $byteArray
    -SendTrigger logon -user domain1\user1
  ```

Aufzeichnen von Sitzungen

March 15, 2022

Sie können mit den Steuerelementen der Sitzungsaufzeichnung der Seiten **Benutzerdetails** und **Maschinendetails** in Director ICA-Sitzungen aufzeichnen. Dieses Feature steht bei Sites mit **Premium**-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 Erstellen und Aktivieren von Aufzeichnungsrichtlinien.
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.

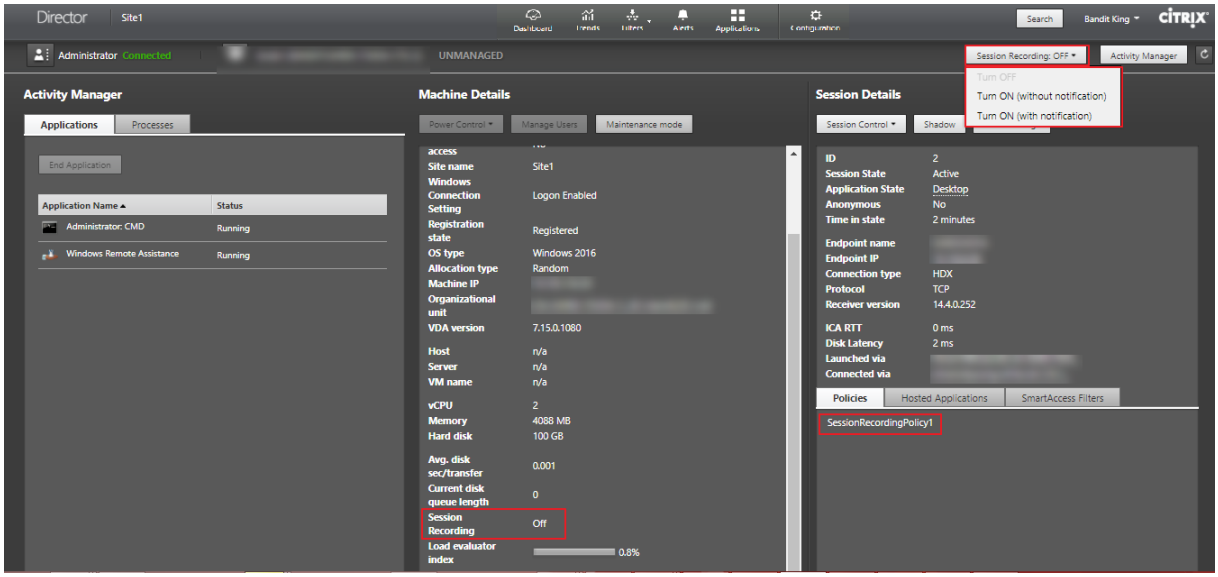
Steuerelemente der Sitzungsaufzeichnung in Director

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.

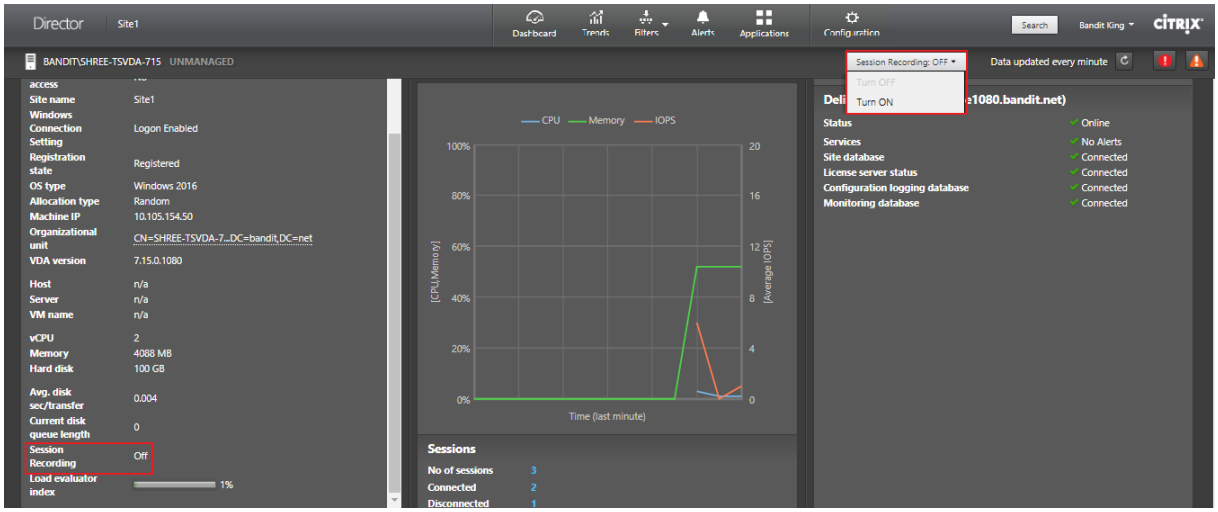
Sie haben folgende Möglichkeiten:

- 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.



Featurekompatibilitätsmatrix

August 22, 2022

Citrix Director 7 1912 ist mit folgenden Lösungen kompatibel:

- Citrix Virtual Apps and Desktops 7 1909 und höher
- XenApp and XenDesktop Version 7.15 LTSR

Sie können Director innerhalb jeder Site mit älteren Delivery Controller-Versionen verwenden, jedoch sind dann u. U. nicht alle Features der aktuellen Director-Version verfügbar. 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.

Wenn Sie sich nach einem Director-Upgrade zum ersten Mal anmelden, wird für die konfigurierten Sites eine Versionsüberprüfung durchgeführt. Wird in einer Site eine Controllerversion ausgeführt, die älter ist als die von Director, wird in der Director-Konsole eine Meldung mit einer Site-Upgradeempfehlung angezeigt. Solange die Version der Site älter ist als die von Director, wird außerdem ein entsprechender Hinweis im Director-Dashboard angezeigt.

> **Hinweis:**
>
> In älteren Versionen von Citrix Director werden keine Richtlinien angezeigt, die auf unter neueren VDA-Versionen ausgeführte Benutzersitzungen angewendet werden. Citrix Director

> 1912 und frühere Versionen zeigen keine Richtlinien an, die auf unter VDA-Versionen ab 2003 ausgeführte Benutzersitzungen angewendet werden. Verwenden Sie Citrix Director ab Version 2003, um solche Richtlinien anzuzeigen.

Spezifische Director-Features und die erforderliche Mindestversion von Delivery Controller (DC), VDA und anderer abhängiger Komponenten sowie die Lizenz-Edition werden nachfolgend aufgeführt.

Director-Version	Feature	Abhängigkeiten - erforderliche Mindestversion	Edition
1909	Konfiguration von On-Premises-Sites mit Citrix Analytics for Performance	DC 7 1906 und VDA 1906	Alle
1906	Automatische Sitzungswiederverbindung	DC 7 1906 und VDA 1906	Alle
1906	Sitzungsstartdauer	DC 7 1906 und VDA 1903	Alle
1906	Desktoptests	DC 7 1906 und Citrix Probe Agent 1903	Premium
7.9 und höher	Citrix Profilverwaltung –Verarbeitungsdauer	VDA 1903	Alle
1811	Profildrilldown	DC 7 1811 und VDA 1811	Alle
1811	Überwachen von Hypervisorwarnungen	DC 7 1811	Premium
1811	Anwendungstests	DC 7 1811 und Citrix Application Probe Agent 1811	Premium
1811	Microsoft RDS-Lizenzstatus	DC 7 1811 und VDA 7.16	Alle
1808	Export von Filterdaten	DC 7 1808	Alle
1808	Drilldown für interaktive Sitzungen	DC 7 1808 und VDA 1808	Alle
1808	GPO-Drilldown	DC 7 1808 und VDA 1808	Alle

Director-Version	Feature	Abhängigkeiten - erforderliche Mindestversion	Edition
1808	Maschinendaten über OData-API verfügbar	DC 7 1808	Alle
7.18	Anwendungstests	DC 7.18	Premium (zuvor Platinum)
7.18	Intelligente Benachrichti-gungsrichtlinien	DC 7.18	Premium (zuvor Platinum)
7.18	Health Assistant-Link	Ohne	Alle
7.18	Drilldown für interaktive Sitzungen	Ohne	Alle
7.17	PIV-Smartcardauthentifizierung	Ohne	Alle
7.16	Anwendungsanalyse	DC 7.16 and VDA 7.15	Alle
7.16	OData API V.4	DC 7.16	Alle
7.16	Spiegeln von Linux-VDA-Benutzersitzungen	VDA 7.16	Alle
7.16	Unterstützung für domänenlokale Gruppen	Ohne	Alle
7.16	Zugriff auf die Maschinenkonsole	DC 7.16	Alle
7.15	Überwachen von An-wendungsstörungen	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	Premium (zuvor 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	Premium (zuvor Platinum)
7.11	Verbesserungen am Berichtexport	DC 7.11 und VDA 7.x	Alle
7.11	Integration von Citrix ADM	DC 7.11, VDA 7.x und MAS-Version 11.1 Build 49.16	Premium (zuvor 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	Premium (zuvor Platinum)
7.7	SCOM-Integration	DC 7.7, VDA 7.x, SCOM 2012 R2 und PowerShell 3.0	Premium (zuvor Platinum)
7.7	Integration der Windows-Authentifizierung	DC 7.x und VDA 7.x	Alle
7.7	Nutzung von Maschinen mit Einzelsitzungs-OS und Multisitzungs-OS	DC 7.7 und VDA 7.x	Premium (zuvor Platinum)

Director-Version	Feature	Abhängigkeiten - erforderliche Mindestversion	Edition
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	Premium (zuvor Platinum)
7	Integration von HDX Insight	DC 7.6, VDA 7.x und Citrix ADM	Premium (zuvor Platinum)

Datengranularität und -beibehaltung

December 2, 2022

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 Premium-Lizenz kann der Aufbewahrungszeitraum auf die gewünschte Anzahl an Tagen eingestellt werden, ansonsten wird der Standardwert verwendet. Im Fall eines Verbindungsverlusts mit der Sitedatenbank gilt der standardmäßige Aufbewahrungszeitraum für Premium-Ansprüche (siehe Tabelle unten).

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-->
```


	Einstellungsname	Betroffene Bereinigung	Standardwert Premium (Tage)	Standardwert nicht Premium (Tage)
1	GroomSessionsRetentionDays	Zeitlicher Datensatz 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 Premium (Tage)	Standardwert nicht Premium (Tage)
4	GroomDeletedRetentionDays	Maschinen-, 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 Premium (Tage)	Standardwert nicht Premium (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 Ressourcennauslastung	1	1
12	GroomResourceUsageMinuteDataRetentionDays	Zusammengefasste Daten zur Ressourcennauslastung mit minutengenauer Granularität	7	7
13	GroomResourceUsageHourDataRetentionDays	Zusammengefasste Daten zur Ressourcennauslastung mit stundengenauer Granularität	30	7

	Einstellungsname	Betroffene Bereinigung	Standardwert Premium (Tage)	Standardwert nicht Premium (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 Premium (Tage)	Standardwert nicht Premium (Tage)
21	GroomMachineMetricsDataRetentionDays	Zu lange gespeicherte Daten zu Maschinenkennzahlen	93	7
22	GroomApplicationErrorsRetentionDays	Anwendungsfehlerdaten	31	1
23	GroomApplicationFaultsRetentionDays	Anwendungsabsturzdaten	31	1

> **Achtung:**
>
> Nach dem Ändern von Werten auf 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.

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

May 24, 2024

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
–	[0] Unknown. 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] None	[1] None	Ohne	–

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] Other	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 Monitoring service converts [12] NoDesktopAvailable to this error code.	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
Max. Kapazität	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.
Beim Starten hängen geblieben	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.
Fehler beim Start	1	Beim Starten der VM auf dem Hypervisor sind Probleme aufgetreten.	Überprüfen Sie die Hypervisorprotokolle.
Ohne	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	1101	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.
Ausschalten	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

November 4, 2021

Das aktuelle Release enthält mehrere SDKs und APIs. Um auf die SDKs und APIs zuzugreifen, gehen Sie zu Build anything with Citrix. Wählen Sie dort **Citrix Workspace** aus, um auf Programmierinformationen für Citrix Virtual Apps and Desktops und die zugehörigen Komponenten zuzugreifen.

> **Hinweis:**
>
> Das Citrix Virtual Apps and Desktops SDK und das Citrix Group Policy SDK können als Modul oder Snap-In installiert werden. Mehrere Komponenten-SDKs (wie Citrix Lizenzierung, Citrix Provisioning und StoreFront) werden nur mit einem Snap-In installiert.

Citrix Virtual Apps and Desktops SDK

Dieses SDK wird automatisch als PowerShell-Modul installiert, wenn Sie einen Delivery Controller oder Studio installieren. Auf diese Weise können Sie die Cmdlets dieses SDK verwenden, ohne Snap-Ins hinzufügen zu müssen. (Anweisungen finden Sie weiter unten, wenn Sie dieses SDK als Snap-In installieren möchten.)

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 Citrix Virtual Apps oder Citrix Virtual Desktops zu installieren, empfiehlt Citrix, dass Sie für den normalen Betrieb Citrix Administratoren mit den entsprechenden Rechten erstellen und nicht das lokale Administratorkonto verwenden.

Zugreifen auf und Ausführen von 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. Informationen zur PowerShell-Ausführungsrichtlinie finden Sie in der Dokumentation von Microsoft.
3. Wenn Sie das Snap-In (anstelle des Moduls) verwenden möchten, fügen Sie das Snap-In über das Cmdlet `Add-PSSnapin` (oder `asnp`) hinzu.

   V1 und V2 beziehen sich auf die Version des Snap-Ins. XenDesktop 5-Snap-Ins sind Version 1. Citrix Virtual Apps and Desktops sowie frühere XenDesktop 7-Snap-Ins sind Version 2. Um beispielsweise das Citrix Virtual Apps and Desktops-Snap-In zu installieren, geben Sie `Add-PSSnapin Citrix.ADIdentity.Admin.V2` ein. Geben Sie Folgendes ein, um alle Cmdlets zu importieren: `Add-PSSnapin Citrix.*.Admin.V*`

Sie können jetzt die Cmdlets und Hilfedateien verwenden.

- Auf die Hilfedateien für dieses SDK können Sie zugreifen, indem Sie zunächst das Produkt oder die Komponente in der Liste Kategorien und dann **Citrix Virtual Apps and Desktops SDK** auswählen.
- Anleitungen zu PowerShell finden Sie unter Windows PowerShell Integrated Scripting Environment (ISE).

Group Policy SDKs

Mit dem Citrix Group Policy SDK können Sie Einstellungen und Filter für Gruppenrichtlinien anzeigen und konfigurieren. Dieses SDK 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 Citrix Virtual Apps and Desktops-SDK installiert sein.

Der PowerShell-Anbieter für Citrix Gruppenrichtlinien ist als Modul oder Snap-In verfügbar.

- Wenn Sie das Modul verwenden möchten, sind keine zusätzlichen Maßnahmen erforderlich.

- Um das Snap-In hinzuzufügen, geben Sie `Add-PSSnapin citrix.common.grouppolicy` ein.

Um auf die Hilfe zuzugreifen, geben Sie Folgendes ein: `help New-PSDrive -path localgpo:/`.

Zum Erstellen einer virtuellen Festplatte und Laden dieser Festplatte mit Einstellungen geben Sie Folgendes ein: `New-PSDrive <Standard Parameters> [-PSProvider] CitrixGroupPolicy -Controller <string>`, wobei die Controller-Zeichenfolge der vollqualifizierte Domänenname eines Controllers in der Site ist, aus der die Einstellungen geladen werden sollen.

Überwachungsdienst-OData

Die Überwachungsdienst-API ermöglicht den Zugriff auf die Überwachungsdienstdaten mit Version 3 oder 4 der OData-API. Sie können Dashboards zur Überwachung und Berichterstellung basierend auf den vom Überwachungsdienst abgefragten Daten erstellen. Version 4 von OData basiert auf der ASP.NET Web API und unterstützt Aggregationsabfragen.

Weitere Informationen finden Sie unter Monitor Service OData API.

WCAG 2.0 Voluntary Product Accessibility Templates

May 14, 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.