Citrix Virtual Apps and Desktops 7 2402 LTSR

Contents

Citrix Virtual Apps and Desktops 7 2402 LTSR (Long Term Service Release)

June 27, 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 bietet eine Virtualisierungslösung für die Anwendungs- und Desktop-Bereitstellung auf Geräten aller Art über jedes Netzwerk mit mehr Datensicherheit –kostengünstiger und produktiver.

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.

Cumulative Update 4 (CU4) ist das neueste Update für 2203 LTSR. LTSRs sind auch für Citrix Virtual Apps and Desktops 1912 verfügbar.

- 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. Weitere Informationen finden Sie unter Citrix DaaS.

Hilfreiche Links

- Citrix Supportability Pack
- LTSR FAQ

- Serviceoptionen für Citrix Virtual Apps and Desktops
- Produktlebenszyklusdaten
- LTSR-Programm für Citrix Workspace-App

Citrix Virtual Apps and Desktops 7 2402 LTSR

June 27, 2024

Info zum 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 auch für Citrix Virtual Apps and Desktops 2203 und 1912 verfügbar.

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:

- **Installieren oder Aktualisieren einer Site:** Installieren oder aktualisieren Sie Kernkomponenten und VDAs mit der ISO-Datei. Nach der Installation bzw. dem Aktualisieren auf die neueste Version können Sie die neuen Features nutzen.
- **Installieren oder Upgrade von VDAs einer bestehenden 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 kann beispielsweise nützlich sein, wenn Sie die Erweiterungen in einer Testumgebung testen möchten.

  Nach dem Upgrade der VDAs auf die aktuelle Version ist keine Aktualisierung der Funktionsebene des Maschinenkatalogs erforderlich. Weitere Informationen finden Sie unter VDA-Versionen und Funktionsebenen.

Installations- und Upgradeanweisungen:

- 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 2402 LTSR

Secure HDX (Preview)

Sie können jetzt Secure HDX verwenden, eine ALE-Lösung (Application Level Encryption), die verhindert, dass Netzwerkelemente im Datenverkehrspfad den HDX-Verkehr überprüfen können. Weitere Informationen finden Sie unter Secure HDX.

Neue HDX-Grafikrichtlinie —Windows-Bildschirmsperre zulassen

Mit der neuen Richtlinie **Windows-Bildschirmsperre zulassen** in HDX Graphics haben Sie jetzt die Möglichkeit, Windows-Anzeigetimeouts in einer Citrix Virtual Desktop-Sitzung auf Workstation OS gemäß Ihren Anforderungen zu ändern.
Weitere Informationen finden Sie unter Windows-Bildschirmsperre zulassen.

Neuer Verlusttoleranzmodus für Audiorichtlinien

Der Verlusttoleranzmodus für Audio ist jetzt verfügbar, um die Audioübertragung im Rahmen der Richtlinie für den Verlusttoleranzmodus zu ermöglichen.
Weitere Informationen finden Sie unter Verlusttoleranzmodus für Audio.

Signierte Binärdateien von Drittanbietern

Von Citrix vertriebene Binärdateien sind jetzt signiert. Signierte Binärdateien geben an, dass sie entweder durch von Citrix generierte Zertifikate oder durch authentische Zertifikate von Drittanbietern validiert wurden. Weitere Informationen finden Sie unter Installieren von VDAs.

Verbesserte Systemprotokolle für die Umleitung von Browserinhalten

Mit den Verbesserungen an den Systemprotokollen ermöglicht die Umleitung von Browserinhalten nun Administratoren, den Featurestatus zu überwachen. Weitere Informationen finden Sie unter Problembehandlung bei der Browserinhaltsumleitung.

Verbesserte Konfiguration der bidirektionalen Inhaltsumleitung

Bisher mussten für die Konfiguration der bidirektionalen Inhaltsumleitung drei verschiedene Richtlinien verwaltet werden: Bidirektionale Inhaltsumleitung zulassen, Umleitung von URLs zum VDA zulassen und Umleitung von URLs zum Client zulassen. Diese Richtlinien erfordern Konfigurationen sowohl auf der Serverseite als auch auf der Clientseite (konfiguriert über Gruppenrichtlinien).

Ab dieser Version wurden alle drei Richtlinien in einer einzigen, einheitlichen Richtlinie zusammengefasst. Dies vereinfacht und verbessert nicht nur den Konfigurationsprozess, sondern macht auch clientseitige Konfigurationen überflüssig.
Weitere Informationen finden Sie unter Bidirektionale Inhaltsumleitung konfigurieren.

HDX Reducer

Sie können jetzt die Version des HDX-Komprimierungsalgorithmus (Reducer) konfigurieren, die Sie im Sitzungshost verwenden möchten.
Weitere Informationen finden Sie unter HDX Reducer.

Neue HDX-Registrierungseinstellung für die Konfiguration des EDT-Timeouts

Sie haben jetzt die Möglichkeit, das EDT-Timeout zu konfigurieren, indem Sie die Registrierung einrichten. Weitere Informationen finden Sie unter EDT-Timeout konfigurieren.

Microsoft Teams Optimization —Registrierungseintrag auf der Positivliste

Ab Citrix Virtual Apps and Desktops 2402 müssen Sie den Registrierungseintrag `msedgewebview2.exe` nicht mehr manuell konfigurieren, da er jetzt standardmäßig auf der Positivliste steht.

Weitere Informationen finden Sie in der Microsoft-Dokumentation.

Unterstützung von Umgebungsvariablen durch die Positivliste für virtuelle Kanäle

Sie können jetzt Systemumgebungsvariablen im Pfad von vertrauenswürdigen Prozessen verwenden.
Weitere Informationen finden Sie unter Verwenden von Systemumgebungsvariablen.

Citrix Secure Private Access für On-Premises

Secure Private Access für On-Premises und Unterstützung für ZTNA und andere Verbesserungen

Die lokale Citrix Secure Private Access-Lösung verbessert die allgemeine Sicherheits- und Compliance-Situation eines Unternehmens durch die Möglichkeit, mithilfe von StoreFront als einheitliches Zugangsportal für Web- und SaaS-Apps einfach Zero Trust Network Access für browserbasierte Apps (interne Web-Apps und SaaS-Apps) bereitzustellen, zusammen mit virtuellen Apps und Desktops als integriertem Bestandteil von Citrix Workspace. Citrix Secure Private Access für On-Premises ist eine vom Kunden verwaltete Zero Trust Network Access-(ZTNA)-Lösung, die VPN-freien Zugriff auf interne Web-

und SaaS-Anwendungen mit den folgenden Funktionen sowie einer nahtlosen Endbenutzererfahrung bietet:

- Prinzip der geringsten Privilegien
- Single Sign-On (SSO)
- Multifaktorauthentifizierung
- Beurteilung des Gerätestatus
- Sicherheitskontrollen auf Anwendungsebene
- App Protection-Features

Weitere Informationen finden Sie unter Citrix Secure Private Access für On-Premises – Allgemeine Verfügbarkeit.

Virtual Delivery Agents (VDAs) 2402 LTSR

Option zum Installieren, Aktualisieren oder Deinstallieren der Citrix Workspace-App während VDA-Installation, -Upgrade oder -Deinstallation

Mit diesem Feature können Sie in den folgenden Szenarien wählen, ob Sie die Citrix Workspace-App während einer VDA-Installation, eines Upgrades oder einer Deinstallation installieren, aktualisieren oder deinstallieren möchten:

- Während einer VDA-Installation können Sie wählen, ob Sie die Citrix Workspace-App installieren möchten. Standardmäßig wird die Citrix Workspace-App während der VDA-Installation nicht installiert.
- Wenn die Citrix Workspace-App noch nicht auf dem VDA installiert ist, können Sie während eines VDA-Upgrades wählen, ob die Citrix Workspace-App installiert werden soll.
- Wenn während eines VDA-Upgrades die Version der Citrix Workspace-App aktualisiert werden kann, wird die Option zum Upgrade der Citrix Workspace-App angezeigt.
- Während einer VDA-Deinstallation können Sie sich dafür entscheiden, die Citrix Workspace-App nicht zu deinstallieren. Standardmäßig wird die Citrix Workspace-App während der VDA-Deinstallation deinstalliert. Weitere Informationen finden Sie unter Auswählen der Komponenten und des Speicherorts für die Installation sowie Befehlszeilenoptionen zur VDA-Installation.

WebSocket-Unterstützung für VDAs

Mit Citrix Virtual Apps and Desktops können Sie jetzt die WebSocket-Technologie über das Citrix Brokering Protocol (CBP) verwenden, um die Kommunikation zwischen VDAs und Delivery Controllern zu erleichtern. Dieses Feature erfordert nur den TLS-Port 443 für die Kommunikation vom VDA zum Delivery Controller.

Weitere Informationen finden Sie unter WebSocket-Kommunikation zwischen VDA und Delivery Controller.

Unterstützung von VDA-Updates von einer lokalen Dateifreigabe, auf die VDAs zugreifen können (Preview)

Sie können jetzt VDA-Updates von einer lokalen Dateifreigabe aus unterstützen und den Speicherort des VDA-Installationsprogramms mit PowerShell-Befehlen angeben. Weitere Informationen finden Sie unter Unterstützung von VDA-Updates über lokale Dateifreigaben.

Web Studio

Unterstützung für die Bereitstellung von VMware-VMs mit Maschinenprofilen

Bei der Bereitstellung von VMware-VMs mit Maschinenerstellungsdiensten (MCS) können Sie jetzt eine vorhandene VM als Maschinenprofil auswählen, sodass andere VMs im Katalog Einstellungen von der ausgewählten VM übernehmen (erben) können.

Zu den vererbten Einstellungen gehören:

- Auf der Vorlage platzierte Tags
- Benutzerdefinierte Attribute
- vSAN-Speicherrichtlinien
- Virtuelle Hardwareversion
- vSphere Virtual TPM (vTPM)
- CPU-Anzahl und Kerne pro Socket
- Anzahl Netzwerkkarten

Weitere Informationen finden Sie unter Maschinenkataloge erstellen.

Verwaltung vorbereiteter Images mit dem Knoten “Images”

In Web Studio ist jetzt ein **Images**-Knoten verfügbar, mit dem Sie ein MCS-Image (vorbereitetes Image) aus einem einzigen Quellimage vorbereiten und in verschiedenen MCS-Maschinenkatalogen bereitstellen können. Dieser Knoten ermöglicht die vollständige Imagelebenszyklusverwaltung und ermöglicht es Ihnen, Imagedefinitionen, Versionen und Kataloge zu erstellen.

Mit diesem Knoten vorbereitete Images können nur in Azure- und VMware-Umgebungen verwendet werden. Ausführliche Informationen zur Imageverwaltung finden Sie unter Imageverwaltung (Vorschau).

Alternativ können Sie auch Kataloge mit vorbereiteten Images mithilfe des Knotens **Maschinenkataloge** erstellen. Weitere Informationen finden Sie unter Maschinenkataloge erstellen.

Verwandte Richtlinien

Neue Richtlinienvalidierungen. Zusätzliche Richtlinienvalidierungen wurden hinzugefügt. Daher kann das Aktivieren von Richtlinien oder das Durchführen eines direkten Upgrades zum Verlust von Richtliniendaten führen, wenn ungültige Richtlinieneinstellungen vorhanden sind. Wenn Sie die Richtlinien mit einer anderen Methode als Web Studio erstellen oder bearbeiten, empfiehlt Citrix, die neueste Version des SDK und des Snap-Ins zu verwenden. Weitere Informationen finden Sie unter CTX676686.

Veraltete Features

Die folgenden Features und Einstellungen sind in Web Studio veraltet:

- Azure-Umgebungen:

  Die Bereitstellung von VMs mit einem Masterimage aus einer anderen Region ist veraltet. Es wird empfohlen, Azure Compute Gallery zu verwenden, um das Masterimage in die Region zu replizieren, in der die VMs erstellt werden.

- AWS-Umgebungen:

  Die Option **Maschinenvorlageneigenschaften auf virtuelle Maschinen anwenden** auf der Seite **Maschinenkatalog-Setup > Maschinenvorlage** ist veraltet. Wir empfehlen, stattdessen Maschinenprofile zu verwenden, um Maschineneigenschaften für virtuelle Maschinen anzugeben.

- Alle Hypervisor- und Cloud-Serviceumgebungen:

  Die Konfiguration des Zurückschreibcaches mit nur einem Datenträgercache und ohne Speichercache ist veraltet. Es wird empfohlen, die Speichercachegröße auf einen Wert größer als Null einzustellen.

Citrix Director

Secure Private Access-Integration mit Director (Preview)

Die Secure Private Access-Integration mit Director ermöglicht es Helpdeskadministratoren oder Volladministratoren, alle Secure Private Access-Sitzungen in Director zu überwachen und Fehler zu beheben. Um dieses Feature zu unterstützen, müssen Sie die Versionen 2402 oder höher von Director, Secure Private Access, Citrix Workspace-App und VDA verwenden.

Zu den verfügbaren Aktionen gehört das Anzeigen der folgenden Details:

- Aktive Secure Private Access-Sitzungen für einen Benutzer unter dem Popup **Sitzung auswählen** > Registerkarte **Sitzungen** > **Web-Apps und SaaS-Apps**

- Secure Private Access-Enumerationen und fehlgeschlagene App-Starts im Popup **Sitzung auswählen** > Registerkarte **Zugriff verweigert**
- Ansicht der Sitzungs- und Anwendungsdetails für aktive und fehlgeschlagene App-Starts
- Ansicht der Sitzungs- und Anwendungsdetails für fehlgeschlagene und blockierte Enumerationen

Weitere Informationen finden Sie auf der Seite Secure Private Access-Integration mit Director (Preview).

Verbesserter Bereich "Leistungsmetriken"

Der Bereich **Leistungsmetriken** bietet eine verbesserte Visualisierung der Echtzeitmetriken. Wenn Sie mit den Echtzeitdaten auf die Registerkarte **Sitzungsleistung** klicken, können Sie die Daten der letzten 15 Minuten anzeigen, ohne auf die Ladezeit der Seite warten zu müssen. Diese Verbesserung trägt dazu bei, die durchschnittliche Zeit bis zur Problembehebung zu verkürzen, da Administratoren in der Lage sind, mehrere Leistungsmetriken mehrerer Komponenten in einer einzigen Ansicht zu korrelieren. Weitere Informationen finden Sie im Abschnitt Leistungsmetriken.

Unterstützung für neuere Versionen von Microsoft Teams

Citrix Director unterstützt jetzt Microsoft Teams Version 2.1 oder früher.

Maschinenerstellungsdienste (MCS)

Imageverwaltung (Preview)

Mit der Imageverwaltungsfunktion trennt MCS die Masteringphase vom gesamten Bereitstellungsworkflow.

Sie können ein MCS-Image (vorbereitetes Image) aus einem einzigen Quellimage vorbereiten und es in mehreren verschiedenen MCS-Maschinenkatalogen verwenden. Diese Implementierung reduziert die Speicher- und Zeitkosten erheblich und vereinfacht die VM-Bereitstellung und den Imageaktualisierungsprozess.

Die Verwendung dieser Imageverwaltungsfunktion bietet folgende Vorteile:

- Generieren Sie vorbereitete Images im Voraus, ohne einen Katalog zu erstellen.
- Wiederverwenden Sie vorbereitete Images in mehreren Szenarien, z. B. beim Erstellen und Aktualisieren eines Katalogs.
- Reduzieren Sie die Zeit für die Katalogerstellung oder Aktualisierung erheblich.

Ausführliche Informationen zur Imageverwaltung finden Sie unter Imageverwaltung (Vorschau).

In VMware nach mehreren Netzwerkkarten suchen

In VMware-Umgebungen wurden verschiedene vorbereitende Prüfungen eingeführt, wenn die Hostingeinheit und die Maschinenprofilvorlage über mehrere Netzwerke verfügen und der Parameter `-NetworkMapping` in den Befehlen `New-ProvScheme` und `Set-ProvScheme` verwendet wird. Weitere Informationen zur vorbereitenden Prüfung für mehrere Netzwerkkarten finden Sie unter Nach mehreren Netzwerkkarten suchen.

Unterstützung für die Erstellung von Windows 11-VMs in GCP

Sie können jetzt Windows 11-VMs in GCP erstellen. Wenn Sie Windows 11 auf dem Masterimage installieren, müssen Sie vTPM während der Erstellung des Masterimages aktivieren. Außerdem müssen Sie vTPM auf der Maschinenprofilquelle (VM oder Instanzvorlage) aktivieren.

Dieses Feature gilt für:

- Persistente und nicht persistente MCS-Maschinenkataloge
- Nur Einzelmandantenknotengruppe

Informationen zum Erstellen von Windows 11-VMs auf dem Einzelmandantenknoten finden Sie unter Windows 11-VMs auf dem Einzelmandantenknoten erstellen.

Unterstützung für die Erstellung von Citrix Provisioning-Katalogen mit MCS PowerShell-Befehlen in VMware

Sie können jetzt Citrix Provisioning-Kataloge mit MCS PowerShell-Befehlen in VMware erstellen.

Diese Implementierung bietet Ihnen die folgenden Vorteile:

- Eine einzige, einheitliche Konsole zur Verwaltung von MCS- und Citrix Provisioning-Katalogen.
- Neue Features für Citrix Provisioning-Kataloge, wie eine Identitätsverwaltungslösung, On-Demand-Provisioning und so weiter.

Weitere Informationen finden Sie unter Citrix Provisioning-Kataloge in Citrix Studio erstellen.

Profilverwaltung

Informationen zu neuen Features finden Sie unter Neue Features.

Linux VDA

Informationen zu neuen Features finden Sie unter Neue Features.

Sitzungsaufzeichnung

Informationen zu neuen Features finden Sie unter Neue Features.

Workspace Environment Management

Informationen zu neuen Features finden Sie unter Neue Features.

Citrix Provisioning

Informationen zu neuen Features finden Sie unter Neue Features.

Verbundauthentifizierungsdienst

Informationen zu neuen Features finden Sie unter Neue Features.

Erstrelease von 2402 LTSR –Basiskomponenten

2402-Basiskomponente	Version wie unter "Programme und Funktionen"angezeigt	Dokumentation
Einzelsitzungs-VDA	2402.0.4000.4310	Einzelsitzungs-VDA
Multisitzungs-VDA	2402.0.4000.4310	Multisitzungs-VDA
Delivery Controller	7.41.100.229	Delivery Controller
Citrix Studio	7.41.100.251	Citrix Studio
Citrix Director	7.33.4000.26	Citrix Director
Citrix Gruppenrichtlinienverwaltung	7.41.100.115	Citrix Gruppenrichtlinienverwaltung
Citrix Gruppenrichtlinie - clientseitige Erweiterung	7.41.100.115	
Citrix StoreFront	2402.0.100.64	Citrix StoreFront
Citrix Provisioning	7.41.100	Citrix Provisioning
Universeller Druckserver	7.33.4000.11	Universeller Druckserver
Sitzungsaufzeichnung	24.2.100.35	Sitzungsaufzeichnung

2402-Basiskomponente	Version wie unter “Programme und Funktionen”angezeigt	Dokumentation
Linux VDA	24.02.0.93	Linux Virtual Delivery Agent
Profilverwaltung	24.2.100.52	Profilverwaltung
Citrix Verbundauthen-tifizierungsdienst	10.17.100.90	Citrix Verbundauthen-tifizierungsdienst (FAS)
Browserinhaltsumleitung	15.32.4000.12	Browserinhaltsumleitung
Citrix Probe Agent 2402	7.41.100.78	Download

Erstrelease von 2402 LTSR –kompatible Komponenten

Die folgenden Komponenten sind in der angegebenen Version kompatibel mit LTSR-Umgebungen. Für sie können die LTSR-Vorteile (erweiterter Lebenszyklus und kumulative Updates mit Fixes) nicht beansprucht werden. Citrix fordert Sie u. U. auf, ein Upgrade auf eine neuere Version der folgenden Komponenten in Ihren 2402-Umgebungen durchzuführen.

Kompatible Komponenten und Features	Version wie unter “Programme und Funktionen”angezeigt	Dokumentation
HDX RealTime Optimization Pack	2.9.600	HDX RealTime Optimization Pack
Lizenzserver	11.17.2.0_BUILD_47000	Lizenzserver
Benutzerpersonalisierungslayer	23.9.1	Benutzerpersonalisierungslayer
Webplayer für die Sitzungsaufzeichnung	22.3.4000.4	Webplayer für die Sitzungsaufzeichnung
Optimierung für Microsoft Teams	15.32.3000.9	Optimierung für Microsoft Teams
Workspace Environment Management	2402.1.100.1	Workspace Environment Management

Erstrelease von 2402 LTSR –ausgeschlossene Elemente

Für die folgenden Features, Komponenten und Plattformen können die 2402-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.

Behobene Probleme

June 27, 2024

Citrix Virtual Apps and Desktops 7 2402 LTSR beinhaltet die folgenden behobenen Probleme:

Allgemein

- Wenn der Name des Audiogeräts aus mehr als 200 Zeichen besteht, kann das Gerät möglicherweise nicht zur virtuellen Sitzung umgeleitet werden. [HDX-58341]
- Für die Webcamumleitung wird der RDP-Client zum zweiten Hop nicht unterstützt. [HDX-55630]

- Wenn Sie ein Bild in einer Desktopsitzung mit der Umgebung scannen, die wie unten beschrieben konfiguriert ist, wird das Bild möglicherweise nicht gescannt. Dieses Problem tritt nur sporadisch auf.

  - Scannertreiber und Bildverarbeitungsanwendung installieren.
  - USB-Richtungsrichtlinie auf DDC aktiviert.
  - Einrichtung der Umgebung:
    * DDC: Win2k19 + 7.33CU4
    * VDA: Win2k19/Win2k16+ 7.40.0.191
    * Client: Win10x64 22H2 + CWA 24.1.0.597

  [HDX-58888]

- Der Start einer zweiten Seamless-App schlägt fehl, wenn SSL aktiviert und die Sitzungszuverlässigkeit ausgeschaltet ist. Wenn eine Seamless-App gestartet wird, muss der nachfolgende Start einer anderen Seamless-App auf demselben Server in der vorhandenen Sitzung gestartet werden (Sitzungsfreigabe), während der Client dazu neigt, die App in einer neuen Sitzung zu starten, wodurch eine unerwartete Validierungsanfrage an den Broker gesendet wird. [HDX-52439].
- Wenn Sie Mono-Audio für Stereo-Audiostreams verwenden, hören Sie möglicherweise nur einen Audiokanal in einem Ohrhörer, anstatt beide Kanäle auf beiden Ohren zu empfangen. [HDX-56344]

Delivery Controller

- Aktualisierungen der `MonitorData.ResourceUtilization`-Tabelle in der Monitoring-Datenbank werden verzögert. [CVADHELP-22724]
- Wenn Sie eine VDA-Version 2203 CU3 mit Windows 10 verwenden, hostet das VDA-Installationsprogramm den benutzerdefinierten WCF-Port nicht, wenn Rendezvous Proxy konfiguriert ist. [CVADHELP-24199]

Director

- Wenn Sie in **Multi Forest Site** einen Desktop-VDA mit mehreren Sitzungen oder Einzelsitzungen verwenden, funktioniert die benutzerorientierte Suchfunktion nicht. [CVADHELP-23174]

Grafik

- Wenn Sie unter Windows 11 Version 22H2 ein Windows Media Player-Fensters in einer Sitzung verschieben, wird nur die unteren Hälfte des Videos angezeigt. Wählen Sie als Workaround Fol-

gendes: Settings > System > Multitasking > Snap windows > Show snap layouts when I drag a window to the top of my screen [HDX-42092]

- Wenn Sie Citrix Virtual Apps and Desktops 2203 verwenden, wird möglicherweise ein schwarzer Bildschirm angezeigt, wenn Sie die Verbindung zu den getrennten Sitzungen wiederherstellen. [CVADHELP-23615]

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]
- `CSEngine.exe` verbraucht auf dem VDA mehr Speicher als erwartet. [CVADHELP-20908, CVADHELP-19916]

Studio

- Benutzerdefinierte Administratoren, die nicht den Geltungsbereich "Alle"haben, können Richtlinien aus dem Standardrichtliniensatz nicht bearbeiten oder löschen. Als Workaround fügen Sie der Standardrichtlinie einen Bereich hinzu, auf den der benutzerdefinierte Administrator zugreifen kann. [GP-1569]
- Wenn Sie sowohl *Citrix Studio* als auch *Web Studio* in Ihrer Bereitstellung verwenden, kann Folgendes auftreten: Wenn Sie in *Citrix Studio* einen Anwendungsordner erstellen, ihm aber keine Anwendungen hinzufügen, wird dieser leere Ordner in *Web Studio* nicht angezeigt. [STUD-27526]
- Wenn Sie beim Erstellen einer Hostingverbindung zu Azure mithilfe von Web Studio auf der Seite **Verbindungsdetails** auf **Dienstprinzipal erstellen** und dann auf **Weiter** klicken, wird möglicherweise eine Fehlermeldung angezeigt. Um das Problem zu beheben, lassen Sie Drittanbietercookies im Browser zu. [STUD-24463]
- Wenn Sie die StoreFront-Serveradresse über Citrix Studio hinzufügen und sie einer Bereitstellungsgruppe zuweisen, ist der Store standardmäßig auf OFF eingestellt. [CVADHELP-24862]

Universeller Druckserver

Drucken

- 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]

- Wenn Sie UPS Version 2212 oder 2305 in Citrix Virtual Apps and Desktops Version 2212 oder 2305 mit Windows 10 VDA verwenden, zeigen Drucker, die CUPS verwenden, die folgende Meldung an:

  ```
  Access Denied, cannot connect message
  ```

  [CVADHELP-23644]

VDA für Einzelsitzungs-OS

- Bei der Verwendung des Windows VDA tritt möglicherweise ein Tastaturzuordnungsfehler auf, wenn Sie von der japanischen zur koreanischen Tastatur wechseln. [HDX-59307]
- Die Werte `SaveRsopToFile`, `SaveRsopToMemory` und `SaveRsopToRegistry` unter dem Registrierungsschlüssel `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\GroupPolicy` werden möglicherweise nicht wiederhergestellt. [CVADHELP-23184]
- Nach dem Upgrade eines VDAs auf Version 2203 reagiert die Skype for Business-App möglicherweise nicht mehr auf dem Begrüßungsbildschirm. [CVADHELP-21021]
- `CSEngine.exe` verbraucht auf dem VDA mehr Speicher als erwartet. [CVADHELP-19916]
- Ein Deadlock im Broker Agent verhindert, dass sich Maschinen bei einer DNS-IP-Änderung erneut registrieren. [CVADHELP-18952]
- Mit diesem Fix wird die Befehlszeilenoption `/no_pending_reboot_check` eingeführt, die beim Installieren oder Update von Kernkomponenten die Überprüfung auf einen ausstehenden Neustart aus einer vorherigen Windows-Installation auf der Maschine verhindert. [CVADHELP-21686]
- Der Prozess `WebSocketService.exe` kann nach einem VDA-Neustart nicht gestartet werden. [CVADHELP-24771]
- Wenn Sie eine VDA-Version LTSR 2203 CU 4.1 verwenden, führt der VDA möglicherweise zu Beginn oder während einer Sitzung eine Fehlerprüfung mit der folgenden Meldung durch.

  ```
  Error "StopCode: SYSTEM THREAD EXCEPTION NOT HANDLED": Tdica.sys
  ```

[CVADHELP-24891]

- Wenn Sie eine Maschine verwenden, schlägt der Start der Benutzersitzung zeitweise fehl. [CVADHELP-23922]

- Während einer erneuten Verbindung einer ICA-Sitzung wird das Chatfenster einer Messaging-Anwendung eines Drittanbieters möglicherweise automatisch im Vordergrund angezeigt. [CVADHELP-24000]
- Der `Wfshell.exe`-Prozess stürzt möglicherweise ab, wenn Sie Dateien von einer lokalen Arbeitsstation in die Citrix-Sitzung für VDA LTSR 2203 kopieren und einfügen. [CVADHELP-24146]
- Wenn Sie eine Windows 10 VDA-Version 2308 verwenden, stürzt der `ctxappvservice.exe`-Prozess möglicherweise ab. [CVADHELP-24575]
- Das Kopieren von Inhalten aus einer veröffentlichten Microsoft Visio- oder Visio-App auf einem Desktop in eine App auf dem Benutzergerät schlägt möglicherweise fehl. [CVADHELP-23647]
- WebSocketService (HTML5 Video Redirection WebSocker Service) stürzt möglicherweise ab. [CVADHELP-23917]
- Wenn Sie Virtual Apps and Desktops 2203 LTSR, Citrix Workspace-App 2203 LTSR CU3 (2303 oder 2205) und VDA 2203 LTSR mit Windows 11 22h2 verwenden, wird eine Anwendungsgruppe auf der linken Hälfte des Bildschirms fälschlicherweise in dieser Bildschirmmitte angezeigt, nachdem Sie die Verbindung wiederhergestellt haben. [CVADHELP-23878]

VDA für Multisitzungs-OS

- Der Prozess `WebSocketService.exe` verbraucht möglicherweise mehr Speicher auf den VDAs als erwartet. [CVADHELP-23870]
- `CSEngine.exe` verbraucht auf dem VDA mehr Speicher als erwartet. [CVADHELP-19916]
- Ein Deadlock im Broker Agent verhindert, dass sich Maschinen bei einer DNS-IP-Änderung erneut registrieren. [CVADHELP-18952]
- Der Prozess `WebSocketService.exe` kann nach einem VDA-Neustart nicht gestartet werden. [CVADHELP-24771]
- Wenn Sie eine VDA-Version LTSR 2203 CU 4.1 verwenden, führt der VDA möglicherweise zu Beginn oder während einer Sitzung eine Fehlerprüfung mit der folgenden Meldung durch. `Error "StopCode: SYSTEM THREAD EXCEPTION NOT HANDLED": Tdica.sys` [CVADHELP-24891]
- Einige Prozesse der Citrix Workspace-App werden möglicherweise nicht wie erwartet geschlossen, wenn sie in einer veröffentlichten Anwendungssitzung ausgeführt werden. [CVADHELP-24225]
- In der Server 2019-VDA-Version LTSR 2203 CU3 stürzt `WmiPrvSE.exe` ab. [CVADHELP-24436]
- Der `Wfshell.exe`-Prozess stürzt möglicherweise ab, wenn Sie Dateien von einer lokalen Arbeitsstation in die Citrix-Sitzung für VDA LTSR 2203 kopieren und einfügen. [CVADHELP-24146]

- Der Terminaldiensteprozess stürzt möglicherweise nach einer automatischen Wiederverbindung von Clients ab. [CVADHELP-24364]
- Wenn in Windows Server 2022 eine Maus von der App oder dem Betriebssystem an eine bestimmte Position bewegt wird, können Sie die Maus erst wieder an die Position bewegen, wenn die Maus von der App oder dem Betriebssystem an eine andere Stelle bewegt wird. [CVADHELP-24444]
- Das Dialogfeld **Warnung: Leerlaufzeit abgelaufen** wird in der ICA-Sitzung auf dem 2022-OS-VDA nicht angezeigt, obwohl das Zeitlimit für die **Sitzungsinaktivität** wirksam wird. [CVADHELP-24646]
- Das Kopieren von Inhalten aus einer veröffentlichten Microsoft Visio- oder Visio-App auf einem Desktop in eine App auf dem Benutzergerät schlägt möglicherweise fehl. [CVADHELP-23647]

Profilverwaltung

- Die Dokumentation zur Profilverwaltung 2402 LTSR enthält Informationen zu den Updates in diesem Release.

Linux VDA

- Die Dokumentation zum Linux VDA 2402 LTSR enthält Informationen zu den Updates in diesem Release.

Sitzungsaufzeichnung

- Die Dokumentation zur Sitzungsaufzeichnung 2402 LTSR enthält Informationen zu den Updates in diesem Release.

Workspace Environment Management

- Die Dokumentation zu Workspace Environment Management 2402 LTSR enthält spezifische Informationen zu den Updates in diesem Release.

Citrix Provisioning

- Die Dokumentation zu Citrix Provisioning 2402 LTSR enthält Informationen zu den Updates in diesem Release.

Verbundauthentifizierungsdienst

- Die Verbundauthentifizierungsdienst-Dokumentation 2402 LTSR enthält spezifische Informationen über die Updates in diesem Release.

Bekannte Probleme

June 27, 2024

Citrix Virtual Apps and Desktops 7 2402 LTSR beinhaltet die folgenden bekannten Probleme:

Hinweise

- 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.

Allgemein

- Wenn Sie die App-Leiste starten und dann das Connection Center-Menü in der Citrix Workspace-App für Windows öffnen, wird die App-Leiste nicht unter dem Server angezeigt, auf dem sie gehostet wird. [HDX-27504]
- Wenn Sie die Citrix Workspace-App für Windows verwenden und die App-Leiste in vertikaler Position starten, verdeckt sie das Startmenü oder den Infobereich. [HDX-27505]
- 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]

- Der Citrix Desktopdienst kann nach einem direkten Betriebssystemupgrade von Windows 10 auf Windows 11 möglicherweise nicht gestartet werden. Starten Sie die Maschine erneut, um das Problem zu beheben. [HDX-58399]
- Die Einstellungen für **Sitzungslimits** für Multisitzungs-VDAs werden auf Sitzungshosts, auf denen Windows Server 2022, Windows 10 Enterprise Multisession und Windows 11 Enterprise Multisession ausgeführt werden, abgelehnt.
  Als Workaround können Sie **RDS-Sitzungszeitlimits** über GPO konfigurieren. [HDX-47001]
- Das mit FIDO2 verknüpfte Windows-Sicherheitsdialogfeld wird nicht vor dem ICA-Sitzungsfenster angezeigt, wenn Sie die Anwendung mit Administratorrechten ausführen. Aufgrund des Betriebssystemdesigns wird das Windows-Sicherheitsdialogfeld hinter dem ICA-Sitzungsfenster versteckt, wenn es als Prozess mit erhöhten Rechten ausgeführt wird. [HDX-26794]
- Das Kopieren und Einfügen in die Zwischenablage schlägt möglicherweise fehl, wenn Daten größer als 100 MB sind, die vom Client in die ICA-Sitzung übertragen werden. Große Pufferkopien werden nicht unterstützt. [HDX-59028]
- Obwohl ein Wiederherstellungspunkt erstellt wird, kann ein VDA nicht wiederhergestellt werden, wenn eine VDA-Installation auf der Windows 10- oder Windows 11-Multisitzungsplattform fehlgeschlagen ist. Die VDA-Installation wurde über die Benutzeroberfläche oder die Befehlszeile initiiert. [HDX-58915]
- Das Windows 10- oder Windows 11-Multisitzungs-Betriebssystem unterstützt die Windows-Systemwiederherstellung nicht. Daher ist die Option zum Erstellen eines Wiederherstellungspunkts in der Benutzeroberfläche nicht verfügbar. Die Befehlszeilenoptionen `/EnableRestore` oder `/EnableRestoreCleanup` werden ignoriert und die Meldung **Disabling System Restore as currently not supported on Windows 10/11 Multisession OS** wird protokolliert. [HDX-58915]
- Citrix signiert sowohl von Citrix generierte Binärdateien als auch von Drittanbietern. Das bedeutet, dass die Binärdateien von Citrix authentifiziert werden. Die Versionen der Binärdateien von Drittanbietern bleiben dieselben, da sie von Drittanbietern bezogen wurden. Wenn bereits eine Binärdatei installiert ist, werden die Binärdateien bei einem VDA-Upgrade nicht installiert, da die Versionen übereinstimmen. So können Sie diese Einschränkung umgehen:

  1. Nehmen Sie die Binärdateien in eine **Positivliste** auf. Dadurch entfällt die Notwendigkeit, die Binärdateien zu signieren.
  2. Deinstallieren Sie den älteren VDA und installieren Sie den neuen VDA. Dies ähnelt einer neuen VDA-Installation, bei der die signierten Versionen angewendet werden.

  [HDX-62302]
- In einigen Szenarien ist die zur Auswertung der Richtlinie verwendete IP-Adresse falsch, wenn Sie den Client-IP-Richtlinienfilter verwenden. [HDX-62375]

- Wenn Sie Enhanced Domain Passthrough für Single Sign-On verwenden, schlägt SSO in der Sitzung möglicherweise fehl, wenn auf dem Clientgerät oder Sitzungshost Windows 11 ausgeführt wird. [HDX-62973]

Richtlinien

- Wenn Sie ein Upgrade von einer früheren Version von Citrix Virtual Apps and Desktops auf 2311 oder 2402 LTSR durchführen, gehen möglicherweise Richtliniendaten verloren, wenn in den Richtlinieneinstellungen ungültige Datenwerte vorhanden sind. Weitere Informationen zu dem Problem und den zugehörigen Workarounds finden Sie unter CTX666304. [GP-1671]

Grafik

- Wenn Sie eine Videovorschau mit einer 64-Bit-Webcam-App über die Theora-Komprimierung starten, kann die Sitzung abstürzen. [HDX-21443]
- Möglicherweise stellen Sie in der Skype für Desktop-App zusätzliche Webcams fest, die mit dem Remotedesktop verbunden sind. Die Vorschau dieser zusätzlichen Webcams ist blockiert und kann aus Sicherheitsgründen einen schwarzen Bildschirm anzeigen. Sie können die zusätzliche Webcam ignorieren und die Webcam weiterhin als Endpunkt verwenden. [HDX-58807]
- H265 444 auf Intel- und einigen NVIDIA-GPUs konnte dazu führen, dass Artefakte in der Sitzung sichtbar wurden. Bei Problemen im Zusammenhang mit Intel-GPUs gibt es eine vorübergehende Problemumgehung, um die Größe der Sitzung zu ändern oder den Vollbildmodus umzuschalten. [PMCS-41084]

Maschinenerstellungsdienste

- In einer auf AWS gehosteten VMware-Umgebung schlägt die Erstellung des MCS-Maschinenkatalogs fehl, wenn das Masterimage vTPM-aktiviert ist. Dieses Problem betrifft alle Versionen von Citrix Virtual Apps and Desktops. Informationen zum VMware-Support finden Sie unter Get Support. [PMCS-37603]
- Beim Upgrade einer Multi-Delivery Controller-Site von einigen LTSR-Versionen vor 2402 (einschließlich der Versionen 2302, 2305, 2308, 2311) auf den 2402 LTSR schlagen Energieaktionen auf einer VM möglicherweise fehl, wenn die Site nur teilweise aktualisiert wird. Weitere Informationen finden Sie unter CTX666299.

Drucken

- Auf dem virtuellen Desktop ausgewählte universelle Druckserver-Drucker werden im Fenster **Geräte und Drucker** in der Systemsteuerung nicht angezeigt. In den Anwendungen stehen diese Drucker den Benutzern jedoch zur Verfügung. Dieses Problem tritt nur unter Windows 10 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]
- Einige Druckaufträge von Netzwerkdruckern mit Lastenausgleich schlagen möglicherweise fehl, wenn SSL-Verbindungen zu den universellen Druckservern aktiviert sind. Dies passiert, wenn Druckaufträge schnell nacheinander ausgeführt werden. [HDX-58316]

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]
- Wenn Sie FSLogix 2201 HF1 auf dem Sitzungshost installiert haben, wird beim Starten einer Sitzung möglicherweise ein schwarzer Bildschirm angezeigt. Um dieses Problem zu beheben, müssen Sie FSLogix auf eine neuere Version aktualisieren. [HDX-46159]

Profilverwaltung

- Die Dokumentation zur Profilverwaltung 2402 LTSR enthält Informationen zu den Updates in diesem Release.

Linux VDA

- Die Dokumentation zum Linux VDA 2402 LTSR enthält Informationen zu den Updates in diesem Release.

Sitzungsaufzeichnung

- Die Dokumentation zur Sitzungsaufzeichnung 2402 LTSR enthält Informationen zu den Updates in diesem Release.

Workspace Environment Management

- Die Dokumentation zu Workspace Environment Management 2402 LTSR enthält spezifische Informationen zu den Updates in diesem Release.

Citrix Provisioning

- Die Dokumentation zu Citrix Provisioning 2402 LTSR enthält Informationen zu den Updates in diesem Release.

Verbundauthentifizierungsdienst

- Die Verbundauthentifizierungsdienst-Dokumentation 2402 LTSR enthält spezifische Informationen über die Updates in diesem Release.

Einstellung von Features und Plattformen

June 27, 2024

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

Auslaufende Features

Die Einstellung bedeutet, dass wir beabsichtigen, das Feature oder die Funktion aus einer zukünftigen Version zu entfernen. Das Feature oder die Funktion funktioniert weiterhin und wird vollständig unterstützt, bis es oder sie offiziell entfernt wird. Diese Benachrichtigung über veraltete Versionen kann sich über einige Monate oder Jahre erstrecken. Nach dem Entfernen funktioniert das Feature oder die Funktion nicht mehr. Dieser Hinweis soll Ihnen ausreichend Zeit geben, um Ihren Code zu planen und zu aktualisieren, bevor das Feature oder die Funktion entfernt wird. Alternativen für veraltete Elemente werden nach Möglichkeit vorgeschlagen.

Element	Einstellung der Unterstützung angekündigt in Version	Alternative
Rendezvous V1	2402	Verwenden Sie Rendezvous V2.
Secure ICA	2402	-
VDA-Unterstützung unter Windows Server 2016	2402	Führen Sie ein Upgrade auf die neueste Version von Windows Server durch.
Unterstützung für Delivery Controller, Web Studio, Citrix Director, Citrix Lizenzserver, Citrix StoreFront, Server-VDI für Einzelsitzungs-OS, VDA für Multisitzungs-OS, Active Directory-Gesamtstruktur und -Domäne sowie Universal Print Server unter Windows Server 2016	2402	Führen Sie ein Upgrade auf die neueste Version von Windows Server durch.
Unterstützung für die Versionen 2016 und 2017 von Microsoft SQL Server für die Datenbanken für Sitekonfiguration, Konfigurationsprotokollierung und Überwachung von Datenbanken	2402	Führen Sie ein Upgrade auf die neueste Version von Microsoft SQL Server durch.

Element	Einstellung der Unterstützung angekündigt in Version	Alternative
Unterstützung für die Konfiguration des Zurückschreibcache, sodass er nur einen Datenträgercache und keinen Speichercache enthält	2402	Verwenden Sie die Konfigurationsoption für die Größe des Speichercaches und geben Sie eine Größe ungleich Null an.
Unterstützung für Azure-Kataloge, die vor der Funktion zur bedarfsgesteuerten Bereitstellung erstellt wurden (“ältere”Kataloge)	2402	Erstellen Sie ältere Azure-Katalog-VMs neu. Die Kataloge werden nach Bedarf bereitgestellt und helfen, Speicherkosten zu sparen.
Die Richtllinie **Mindestframeratesollwert**	2311	Verwenden Sie die **Grafikstatusanzeige**, um den Mindestframeratesollwert zu ändern.
Unterstützung für Citrix Connector 3.1 für System Center Configuration Manager	2311	Führen Sie das Image- oder Anwendungsupdate manuell durch.
Unterstützung für die Verwendung eines Masterimages in einer anderen Region als der Region, in der der Katalog erstellt wurde	2311	Verwenden Sie Azure Compute Gallery, um das Masterimage in die gewünschte Region zu replizieren.
Einstellung des Speicherlimits für HDX Graphics Display	2311	Der erforderliche Mindestspeicher wird zugewiesen, um sicherzustellen, dass das Anzeigelayout des Clients vollständig berücksichtigt wird.
Unterstützung des progressiven Modus in HDX Graphics	2311	Verwenden Sie Thinwire. Weitere Informationen finden Sie unter Progressiver Modus.
Unterstützung für die Browserinhaltsumleitung in Internet Explorer 11	2311	Verwenden Sie die Google Chrome-basierte Browserinhaltsumleitung.

Element	Einstellung der Unterstützung angekündigt in Version	Alternative
Die Unterstützung für AWS Volume Worker wurde entfernt	2311	Verwenden Sie den direkten Disk-Upload und -Download. Siehe Direkter Disk-Upload und -Download.
Unterstützung für SQL Server 2016 in Broker	2308	Aktuelle Versionen verwenden. Weitere Informationen finden Sie unter Systemanforderungen.
Unterstützung für XenApp 5.x in Director	2308	—
Unterstützung für XenApp 6.x in Director	2308	—
SCOM-Paket für Benachrichtigungen in Director	2308	—
Unterstützung für Plug-Ins in Director	2308	—
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.
Unterstützung für die Verwendung von `AwsCaptureInstanceProperties` in AWS-Umgebungen	2308	Verwenden Sie ein Maschinenprofil. Siehe Katalog mithilfe eines Maschinenprofils erstellen.
PowerShell-Befehl `Schedule-ProvVMUpdate`	2305	Verwenden Sie `Set-ProvVMUpdateTimeWindow`.

Element	Einstellung der Unterstützung angekündigt in Version	Alternative
PowerShell-Befehl `Request-ProvVMUpdate`	2305	`Set-ProvVMUpdateTimeWindow` mit den Parametern `-StartsNow` und `-DurationInMinutes -1` verwenden.
PowerShell-Befehl `Cancel-ProvVMUpdate`	2305	Verwenden Sie `Clear-ProvVMUpdateTimeWindow`.
Parameter `DedicatedTenancy`, verwendet im Befehl `New-ProvScheme`	2303	Verwenden Sie den Parameter `TenancyType`.
Lizenzserver VPX	2206	—
Nicht verwalteter Datenträger für das VM-Provisioning in Azure-Umgebungen	2206	Verwaltete Datenträger verwenden.
Host-zu-Client-URL-Umleitung	2203	Bidirektionale Inhaltsumleitung.
Unterstützung für vier AWS-spezifische Befehle: `Revoke-HypSecurityGroupIngress`, `Revoke-HypSecurityGroupEgress`, `Grant-HypSecuritygroupegress` und `Grant-HypSecurityGroupIngress` in Cloud- und On-Premises-Umgebungen.	2203	—

Element	Einstellung der Unterstützung angekündigt in Version	Alternative
Citrix Files für Windows und Citrix Files für Outlook vom VDA-Metainstaller.	2203	Verwenden Sie die eigenständigen Installationsprogramme.
WEM-Agent-Komponente aus dem VDA-Metainstaller.	2203	—
SCCM-integrierte Wake on LAN-Option für Remote-PC-Zugriff.	2012	Verwenden Sie das eigenständige Wake-On-LAN-Feature.
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.
Mobility SDK/Mobile SDK (aus dem älteren Citrix Labs)	7.16	Ersetzt durch Einstellungen der Richtlinie “Mobilerfahrung”und native Benutzeroberflächen für gehostete Desktops / Apps.

Entfernte Elemente

Entfernte Elemente wurden entweder entfernt oder in Citrix Virtual Apps and Desktops nicht mehr unterstützt.

Element	Einstellung der Unterstützung angekündigt in Version	Entfernt in Version	Alternative
Citrix Workspace-App für Windows 1912	—	2402	Aktuelle Versionen verwenden.

Element	Einstellung der Unterstützung angekündigt in Version	Entfernt in Version	Alternative
HDX Graphics FullScreen + Textoptimierung	2311	2311	
Unterstützung für NVIDIA Frame Buffer Capture (NVFBC) mit HDX 3D Pro	2308	2311	Verwenden Sie die Desktop Duplication API (DDAPI).
VDA-Unterstützung für die Richtlinieneinstellung “Automatische Installation von mitgelieferten Druckertreibern”.	7.16	2311	Keine. Richtlinieneinstellung, die nur von VDAs unter früheren Betriebssystemen (Windows 7, Windows Server 2012 R2 und früher) unterstützt wird.
NVIDIA-GPU-Hardwarecodierung (NVENC) mit vGPU 11 und älter und Treiberversion 466.77 und älter.	2305	2305	Verwenden Sie derzeit unterstützte NVIDIA-Treiber: vGPU 13 oder neuer, Version 471.41 oder neuer.
Citrix Supportability Tools (Supportability-Tool_x64 .msi) aus dem VDA Meta-Installationsprogramm.	—	2212	—

Element	Einstellung der Unterstützung angekündigt in Version	Entfernt in Version	Alternative
Citrix License Administration Console (zuletzt enthalten in Windows-Lizenzserver 11.16.3 Build 30000, ab Windows-Lizenzserver v11.16.6 Build 31000 entfernt).	2003	2006	Verwenden Sie den Citrix Licensing Manager.
Unterstützung für Grafikadapter Citrix Indirect Display Driver (IDD) unter Windows 10 Version 1709 und früher.	2003	2003	Verwenden Sie Citrix Virtual Apps and Desktops 7 1912 LTSR-VDAs.
Hardwarecodierung mit NVIDIA-GPUs (NVENC), die GRID 9 oder ältere Monitortreiber verwenden.	2003	2003	Verwenden Sie GRID 10-Monitortreiber für Citrix Virtual Apps and Desktops 7 2003 oder höher oder verwenden Sie Citrix Virtual Apps and Desktops 7 1912 LTSR-VDAs.
Self-Service-Kennwortzurücksetzung (SSPR).	2003	2006	—

Element	Einstellung der Unterstützung angekündigt in Version	Entfernt in Version	Alternative
Unterstützung für Microsoft .NET Framework-Versionen vor Version 4.8 für VDAs und Serverkernkomponenten. Lieferumfang: Delivery Controller, Studio, Director und StoreFront.	1912	2003	Upgrade auf .NET Framework Version 4.8.
VDAs unter Windows Server 2012 R2.	1912	2003	Installation von VDAs unter einem unterstützten Betriebssystem.
AppDNA - Komponente für die Anwendungsmigration in Citrix Virtual Apps and Desktops Premium Edition.	1909	2003	—
Installieren von Studio auf 32-Bit-Maschinen (x86).	1909	2003	Installation unter einem unterstützten x64-Betriebssystem.
Unterstützung für den Excel-Hook in Seamlessanwendungen. Dieser wurde zum Erstellen separater Taskleistensymbole für jede Microsoft Excel 2010-Arbeitsmappe verwendet.	1909	1909	—

Element	Einstellung der Unterstützung angekündigt in Version	Entfernt in Version	Alternative
Kernserverkomponenten unter Windows Server 2012 R2 (einschließlich Service Packs). Lieferumfang: Delivery Controller, Studio und Director.	1906	2003	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	2003	Datenbankinstallation auf einer unterstützten Microsoft SQL Server-Version.
Unterstützung für VDAs unter Windows 10 auf x86-Plattformen.	1906	1909*	Installieren Sie VDAs auf 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	—

Element	Einstellung der Unterstützung angekündigt in Version	Entfernt in Version	Alternative
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 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	2203	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.
VDA-Unterstützung für die Richtlinieneinstellung "Automatische Installation von mitgelieferten Druckertreibern".	7.16	2311	Keine. Richtlinieneinstellung, die nur von VDAs unter früheren Betriebssystemen (Windows 7, Windows Server 2012 R2 und früher) unterstützt wird.

Element	Einstellung der Unterstützung angekündigt in Version	Entfernt in Version	Alternative
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.
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

Element	Einstellung der Unterstützung angekündigt in Version	Entfernt in Version	Alternative
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.
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 in Version	Entfernt in Version	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 in Version	Entfernt in Version	Alternative
Flash-Umleitung	7.15 LTSR	1912	Erstellen Sie Videos als HTML5-Video. Verwenden Sie die HTML5-Videoumleitung für verwalteten Inhalt und die Browserinhaltsumleitung 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.

Element	Einstellung der Unterstützung angekündigt in Version	Entfernt in Version	Alternative
Unterstützung des universellen Druckservers (UpsServer) unter Windows Server 2008 (32-Bit)	7.14	7.14	Installation unter einem neueren unterstützten Betriebssystem.
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.

Element	Einstellung der Unterstützung angekündigt in Version	Entfernt in Version	Alternative
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.
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.

Element	Einstellung der Unterstützung angekündigt in Version	Entfernt in Version	Alternative
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.
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.
Unterstützung für CloudPlatform-Verbindungen	7.12	2003	Verwenden Sie einen anderen unterstützten Hypervisor oder Clouddienst.
Unterstützung für Verbindungen mit Azure Classic (auch “Azure Service Management”)	7.12	2003	Verwenden Sie ggf. Virtual Apps and Desktops Service in Citrix Cloud.
AppDisks-Funktionalität (sowie unterstützende AppDNA-Integration in Studio)	7.13	2003	Verwenden Sie Citrix App Layering.
Persönliche vDisk-Funktionalität	7.15	2006†	Verwenden Sie Citrix App Layering – Benutzerlayer oder Benutzerpersonal-isierungslayer.

† Bei Citrix Virtual Apps and Desktops 7 2003 wurde der Treiber für persönliche vDisks aus dem VDA-Installationsprogramm entfernt. Bei Citrix Virtual Apps and Desktops 7 2006 wurde der Treiber für persönliche vDisks aus Studio entfernt.

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 und StoreFront auf einem Server, nur für eine Evaluierung, keine Produktionsbereitstellung	5 GB RAM
Alle Kernkomponenten und StoreFront 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
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. Die Ausnahme ist RAM. Sie brauchen mehr RAM für Anwendungen, die mehr verbrauchen.

Weitere Informationen:

- Citrix Tech Zone enthält Anweisungen zur 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 ++

Bei der Installation eines Delivery Controllers, VDAs oder universellen Druckservers installiert das Citrix Installationsprogramm automatisch die Microsoft Visual C++ 2015–2022 Redistributable.

- Wenn die Maschine eine frühere Version dieser Laufzeitkomponente enthält (z. B. 2015–2019), wird diese vom Citrix Installationsprogramm aktualisiert.
- Wenn die Maschine eine Version vor 2015 enthält, installiert Citrix die neuere Version parallel.

Delivery Controller

Unterstützte Betriebssysteme:

- Windows Server Core 2022
- Windows Server 2022
- 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

Anforderungen:

- Microsoft .NET Framework 4.8 wird automatisch installiert, wenn es (bzw. eine neuere Version) nicht bereits installiert ist.
- Windows PowerShell 3.0, 4.0 oder 5.0.
- Microsoft Visual C++ 2015–2019 Redistributable.

Datenbanken

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

- SQL Server 2022, Express, Standard und Enterprise Edition.
- 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 SP2, Express, Standard und Enterprise Editions.

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.

Überlegungen zum lokalen Hostcache: 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 Controller installieren, wird SQL Server Express LocalDB 2019 mit CU 15 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 automatisch aktualisiert. Informationen zu Anforderungen und Verfahren für den Ersatz finden Sie unter Ersetzen von SQL Server Express LocalDB.

Weitere Datenbankinformationen:

- Datenbanken
- CTX114501 listet die aktuellen unterstützten Datenbanken auf
- Leitfaden für die Datenbankgröße
- Lokaler Hostcache

Web Studio

> **Hinweis:**
>
> - Sie können Ihre Citrix Virtual Apps and Desktops-Bereitstellung mithilfe von zwei Verwaltungskonsolen verwalten: Web Studio (webbasiert) und Citrix Studio (Windows-basiert). Dieser Artikel behandelt nur Web Studio. Informationen zu Citrix Studio finden Sie im entsprechenden Artikel in Citrix Virtual Apps and Desktops 7 2212 oder früher.
> - Web Studio ist eine webbasierte Verwaltungskonsole, mit der Sie On-Premises-Bereitstellungen von Citrix Virtual Apps and Desktops konfigurieren und verwalten. Sie wurde zur Verbesserung der Benutzererfahrung entwickelt und reagiert im Allgemeinen schneller als Citrix Studio, die Windows-basierte Verwaltungskonsole. Siehe Web Studio installieren.

Unterstützte Betriebssysteme:

- Windows Server Core 2022
- Windows Server 2022
- 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

Citrix Director

Unterstützte Betriebssysteme:

- Windows Server Core 2022

- Windows Server 2022
- 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

Anforderungen:

- Microsoft .NET Framework 4.8 wird automatisch installiert, wenn es (bzw. eine neuere Version) nicht bereits installiert ist.
- Microsoft Internetinformationsdienste (IIS) 7.0 und ASP.NET 2.0. Vergewissern Sie sich, 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 installiert.
- Um die Ereignisprotokolle auf Computern anzuzeigen, auf denen Citrix Director installiert ist, müssen Sie Microsoft .NET Framework 2.0 installieren.

Citrix Profilverwaltung:

- Vergewissern Sie sich, dass die Citrix Profilverwaltung und das WMI-Plug-In für die Citrix Profilverwaltung auf dem VDA installiert sind (**Zusätzliche Komponenten** im Installationsassistenten) und dass der Citrix Profilverwaltungsdienst ausgeführt wird, um die Benutzerprofildetails in Director anzuzeigen.

Anforderungen für eine System Center Operations Manager (SCOM)-Integration:

- System Center 2012 R2 Operations Manager

Unterstützte Browser zum Anzeigen von Director:

- Internet Explorer 11. 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 1440 x 1024.

Virtual Delivery Agent (VDA) für Einzelsitzungs-OS

Unterstützte Betriebssysteme:

- Windows 11
- Windows 10 (nur x64), jede derzeit vom Mainstream-Support abgedeckte Version.
  - Informationen zur Unterstützung von Editionen finden Sie im Knowledge Center-Artikel CTX224843.

Anforderungen:

- Microsoft .NET Framework 4.8 wird automatisch installiert, wenn es (bzw. eine neuere Version) nicht bereits installiert ist.
- Microsoft Visual C++ 2015–2019 Redistributable.

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 11 und 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 auf einer unterstützten Windows-Maschine 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 11 (nur mit Citrix DaaS unterstützt)
- Windows 10 (nur x64; wird nur mit Citrix DaaS unterstützt), jede Version, die derzeit standardmäßig unterstützt wird.
- Windows Server 2022
- Windows Server 2019, Standard und Datacenter Edition

- Windows Server 2016, 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 4.8 wird automatisch installiert, wenn es (bzw. eine neuere Version) nicht bereits installiert ist.
- Microsoft Visual C++ 2015–2019 Redistributable.

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 die 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 VDA auf einer Windows Server 2008 R2-Maschine 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 möglicherweise 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.

Unterstützte Hypervisors:

- **XenServer (ehemals Citrix Hypervisor)**

  CTX131239 enthält aktuelle Versionshinweise sowie Links zu bekannten Problemen.

  Weitere Informationen finden Sie unter XenServer-Virtualisierungsumgebungen.

- **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.

Unterstützte Hosts öffentlicher Clouds:

- **Amazon Web Services (AWS)**

  Informationen zur Verwendung von AWS zum Provisioning virtueller Maschinen finden Sie im Abschnitt Amazon Web Services-Virtualisierungsumgebungen.

- **Google Cloud Platform**
  Weitere Informationen finden Sie unter Google Cloud Platform-Virtualisierungsumgebungen und Getting Started with Citrix DaaS on Google Cloud.

- **Microsoft Azure Resource Manager**

  Informationen zum Provisioning virtueller Maschinen mit Microsoft Azure Resource Manager finden Sie unter Microsoft Azure Resource Manager-Virtualisierungsumgebungen.

- **Nutanix-Cloud und Partnerlösungen**

  Informationen zur Verwendung von Nutanix-Cloud und Partnerlösungen finden Sie unter Nutanix-Cloud und Partnerlösungen.

- **Cloud- und Partnerlösungen von VMware**

  Informationen zur Verwendung von VMware-Cloud und Partnerlösungen finden Sie unter VMware-Cloud und Partnerlösungen.

Beachten Sie Folgendes, wenn Sie Verbindungen mit Hosts öffentlicher Clouds in Ihrer Bereitstellung hinzufügen:

- Sie benötigen eine Hybrid Rights-Lizenz. Informationen zur Hybrid Rights-Lizenz finden Sie unter Transition und Trade-Up (TTU) mit Hybrid Rights. Informationen zum Hinzufügen einer Lizenz finden Sie unter Erstellen einer Site.
- Die Informationsquellen leiten Sie zur Citrix DaaS-Dokumentation. Wenn Sie bereits mit Hosts öffentlicher Clouds in Citrix DaaS vertraut sind, werden Ihnen Unterschiede zur On-Premises-Version auffallen.
  - In Citrix DaaS wird die Verwaltungsoberfläche als "Vollständige Konfiguration"bezeichnet. In der On-Premises-Version von Citrix Virtual Apps and Desktops heißt die Verwaltungsoberfläche Web Studio.
  - Updates für Citrix DaaS werden ungefähr alle vier Wochen bereitgestellt. Daher könnten Sie feststellen, dass bestimmte Citrix DaaS-Features nicht in der On-Premises-Version verfügbar sind.

Funktionsebenen von Active Directory

Die folgenden Funktionsebenen werden für Active Directory-Gesamtstrukturen und -Domänen unterstützt:

- Windows Server 2016
- 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 steht bei folgenden Lösungen zur Verfügung:
  - XenServer
  - Nutanix AHV
  - VMware vSphere und VMware ESX (wird in diesem Zusammenhang als vDGA, "Virtual Direct Graphics Acceleration"bezeichnet).
  - Microsoft Hyper-V in Windows Server 2016 (hier wird es als Discrete Device Assignment, DDA bezeichnet)
- vGPU ist verfügbar bei:
  - XenServer
  - Nutanix AHV
  - VMware vSphere

Siehe https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/2402-ltsr/graphics/hdx-3d-pro.

Als Minimalausstattung für den Hostcomputer empfiehlt Citrix 4 GB RAM und vier virtuelle CPUs mit einer Taktfrequenz von 2,3 GHz.

Grafikprozessor (GPU):

- Für die virtualisierte Grafikbeschleunigung mit der NVIDIA GRID-API können Sie HDX 3D Pro mit allen NVIDIA GRID-GPUs verwenden, die von der NVIDIA Virtual GPU-(vGPU)-Softwareversion 13

und höher unterstützt werden. Weitere Informationen finden Sie unter https://docs.nvidia.com/grid/index.html.
Eine detaillierte Liste der unterstützten Hypervisors und der unterstützten Hardware finden Sie in der NVIDIA vGPU-Softwaredokumentation.

- Die virtualisierte Grafikbeschleunigung wird auf den Grafikplattformen der Intel Xeon Prozessoren der E3-Familie für Datencenter und der Intel GPU Flex-Serie für Datencenter unterstützt. Weitere Informationen finden Sie unter GPU Flex-Serie.
- AMD-GPUs werden mit der mxGPU-Virtualisierung von AMD unterstützt. Weitere Informationen zur unterstützten Hardware finden Sie in der AMD-Dokumentation.

Benutzergerät:

- Citrix unterstützt je nach Hardwareressourcen bis zu 8 4K-Monitore. Je nach verwendeter GPU kann es andere Hardwarebeschränkungen für dieses Maximum geben.
- Als Mindestausstattung für Benutzergeräte empfiehlt Citrix mindestens 4 GB RAM und eine CPU mit einer Taktfrequenz von 1,6 GHz. Zur Erzielung der optimalen Leistung wird die Ausstattung von Benutzergeräten mit mindestens 8 GB RAM und einer Dual-Core-CPU mit einer Taktfrequenz von mindestens 3 GHz empfohlen.
- Bei Multimonitorzugriff empfiehlt Citrix Benutzergeräte mit Vierkern-CPUs.
- 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 2022
- Windows Server 2019
- Windows Server 2016

Anforderungen:

- Microsoft Visual C++ 2015–2019 Redistributable
- Microsoft .NET Framework 4.8 (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 11.17.2 und höher unterstützt. Weitere Informationen finden Sie unter Lizenzierung.

Weitere Informationen zur Versionskompatibilität finden Sie in der Produktmatrix.

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

Die Microsoft-Gruppenrichtlinien-Verwaltungskonsole (GPMC) 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. Weitere Informationen finden Sie in der Microsoft-Dokumentation.

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.

Unter Lokaler App-Zugriff finden Sie Informationen zu unterstützten Browsern für dieses Feature.

Diese Version von Citrix Virtual Apps and Desktops erfordert mindestens HDX RealTime Connector 2.9 LTSR. Weitere Informationen finden Sie in der Dokumentation zum HDX RealTime Optimization Pack.

Dieses Produkt unterstützt die PowerShell-Versionen 3 bis 5.

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.

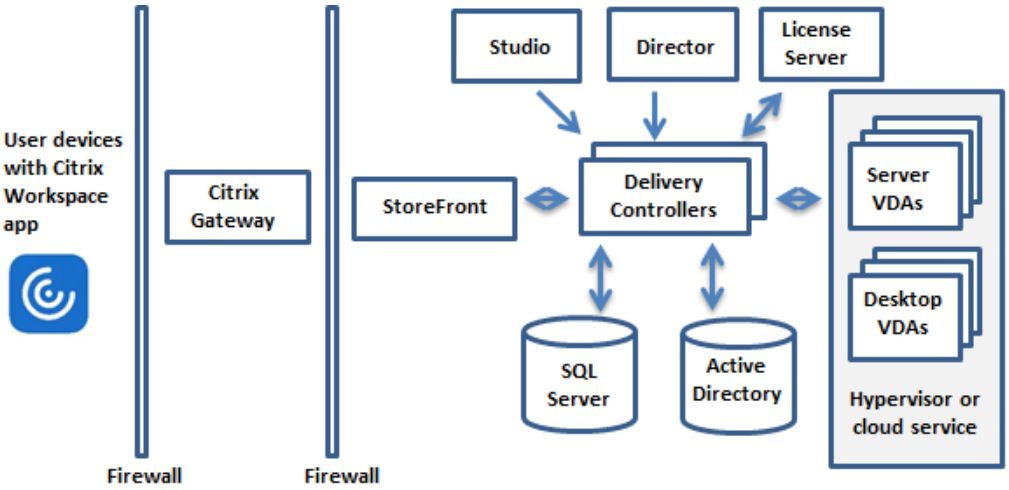
Citrix Virtual Apps and Desktops hat eine einheitliche Architektur: die FlexCast Management Architecture (FMA). Die Hauptfunktion von FMA umfasst die Ausführung mehrerer Versionen von Citrix Virtual Apps oder Citrix Virtual Desktops in einer Site und die Bereitstellung von integriertem Provisioning.

Informationen zu Änderungen an Produktnamen.

Hauptkomponenten

Dieser Artikel ist besonders für neue Anwender von Citrix Virtual Apps and Desktops geeignet.

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 und Verfügbarkeit der Site zu gewährleisten, installieren Sie Controller auf mehreren Servern.) Wenn Ihre Bereitstellung einen Hypervisor oder einen anderen Dienst enthält, kommunizieren die Controller-Dienste damit zu folgendem Zweck:

- Verteilung von Anwendungen und Desktops

- Authentifizierung und Verwaltung des Benutzerzugriffs
- Vermittlung der Verbindungen zwischen Benutzern und ihren Desktops und Anwendungen
- Optimieren der Benutzerverbindungen
- Lastausgleich für Verbindungen

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.

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 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. 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.

Studio

Sie können Ihre Citrix Virtual Apps and Desktops-Bereitstellung mithilfe von zwei Verwaltungskonsolen verwalten: Web Studio (webbasiert) und Citrix Studio (Windows-basiert). Diese Produktdokumentation behandelt nur Web Studio. Informationen zu Citrix Studio finden Sie in Citrix Virtual Apps and Desktops 7 2212 oder früher.

Web Studio Web Studio ist eine webbasierte Verwaltungskonsole, mit der Sie On-Premises-Bereitstellungen von Citrix Virtual Apps and Desktops konfigurieren und verwalten. Sie wurde zur Verbesserung der Benutzererfahrung entwickelt und reagiert im Allgemeinen schneller als Citrix Studio, die Windows-basierte Verwaltungskonsole. Siehe Web Studio installieren.

Citrix Studio Citrix Studio dient als Verwaltungskonsole zum Konfigurieren und Verwalten der Citrix Virtual Apps and Desktops-Bereitstellung. Dank Citrix Studio sind keine separaten Verwaltungskonsolen für die Bereitstellung von Anwendungen und Desktops erforderlich. Citrix 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.

Citrix Studio erhält die angezeigten Informationen vom Brokerdienst auf dem Controller und kommuniziert über TCP-Port 80.

Secure Private Access

Die lokale Citrix Secure Private Access-Lösung verbessert die allgemeine Sicherheits- und Compliance-Situation eines Unternehmens durch die Möglichkeit, mithilfe von StoreFront als einheitliches Zugangsportal für Web- und SaaS-Apps einfach Zero Trust Network Access für browserbasierte Apps (interne Web-Apps und SaaS-Apps) bereitzustellen, zusammen mit virtuellen Apps und Desktops als integriertem Bestandteil von Citrix Workspace. Die Lösung ist mit vorhandenen Versionen von NetScaler und StoreFront kompatibel, ohne dass Änderungen an den Versionen vorgenommen werden müssen. Einzelheiten finden Sie unter Secure Private Access für On-Premises.

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 anderer Dienst

Der Hypervisor oder ein anderer Service 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 andere Services.

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.

Zusätzliche Komponenten

Citrix Virtual Apps and Desktops-Bereitstellungen können die folgenden 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

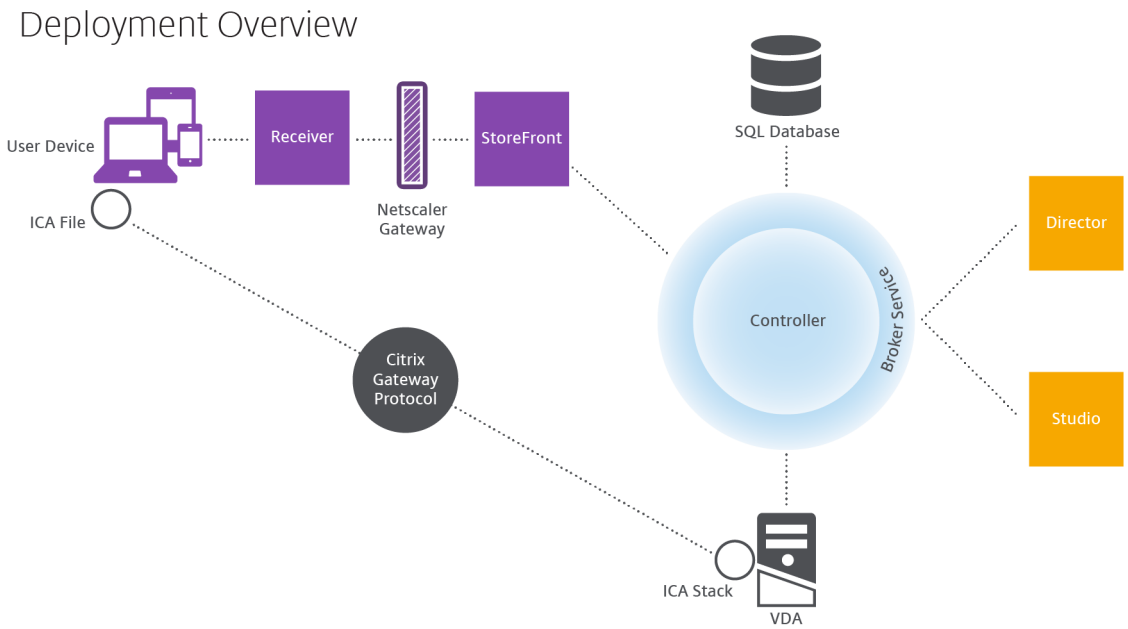
Wenn Benutzer eine Verbindung von außerhalb der Unternehmensfirewall herstellen, können diese Verbindungen in Citrix Virtual Apps and Desktops mit Citrix Gateway (zuvor "Access Gateway"und "NetScaler Gateway") und TLS geschützt werden. Citrix Gateway bzw. das virtuelle VPX-Gerät ist ein SSL-VPN-Gerät, 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 virtuellen Maschinen 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, platzieren Sie möglichst alle Controller im gleichen LAN.

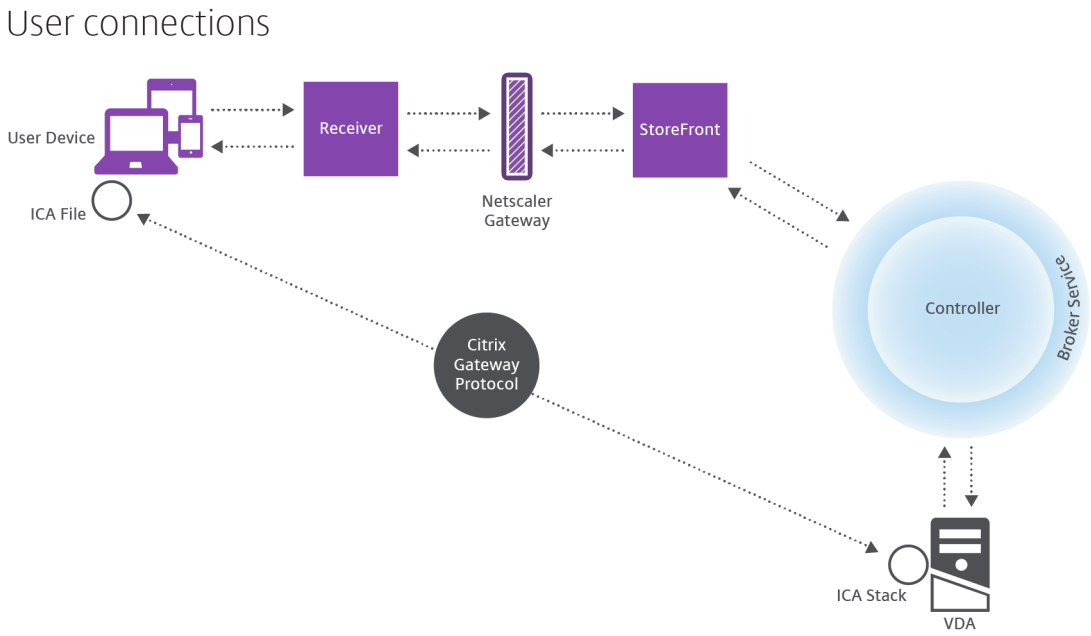
Benutzer greifen niemals direkt auf den Controller zu. Der VDA dient als Vermittler zwischen den Benutzern und dem Controller. Wenn sich Benutzer über StoreFront anmelden, werden ihre Anmeldeinformationen an den Brokerdienst auf dem Controller übermittelt. Der Brokerdienst ruft dann basierend auf den 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-Website 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 heruntergeladen. Wenn die Site ordnungsgemäß eingerichtet wurde, sind die Anmeldeinformationen während des gesamten Vorgangs verschlüsselt.

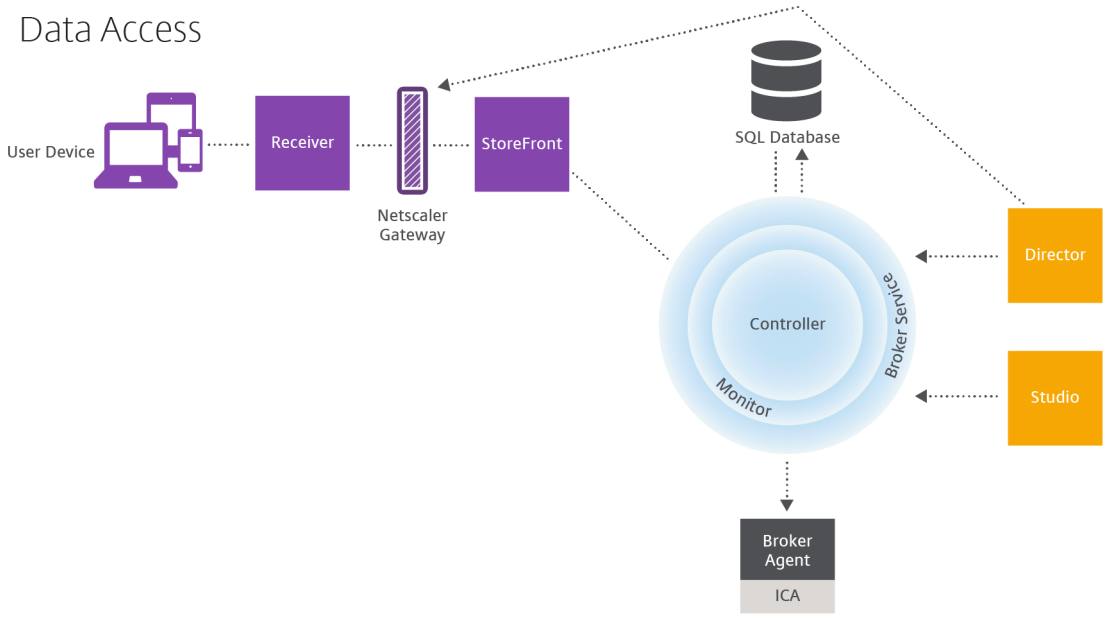
Die ICA-Datei wird auf das Benutzergerät kopiert und richtet eine direkte Verbindung zwischen dem Gerät und dem auf dem VDA ausgeführten ICA-Stack ein. Diese Verbindung umgeht die Verwaltungsinfrastruktur (Citrix Workspace-App, StoreFront und Controller).

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. Es greift nur 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 Bereitstellungsgruppen erstellen.

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 weiterer 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
- Netzwerkports
- Datenbanken
- Unterstützte Hypervisors und andere Dienste

Datenbanken

June 27, 2024

> **Hinweis:**
>
> Sie können Ihre Citrix Virtual Apps and Desktops-Bereitstellung mithilfe von zwei Verwaltungskonsolen verwalten: Web Studio (webbasiert) und Citrix Studio (Windows-basiert). Dieser Artikel behandelt nur Web Studio. Informationen zu Citrix Studio finden Sie im entsprechenden Artikel in Citrix Virtual Apps and Desktops 7 2212 oder früher.

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.

- **Protokollierung:** (auch "Konfigurationsprotokollierung") 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 in Bezug auf Datenbanken Folgendes:

- **Führen Sie regelmäßig Backups aus.** Führen Sie regelmäßig ein Backup der Datenbanken durch, damit diese bei einem Ausfall des Datenbankservers von dem Backup wiederhergestellt werden können. Die Backupstrategie kann für jede Datenbank anders sein. Weitere Informationen finden Sie unter CTX135207. Diese gelten jedoch für die nicht mehr verfügbare bzw. unterstützte CitrixXenDesktopDB.
- **Sichern Sie regelmäßig die SQL Server-Datenbanken für Site, Überwachung und Protokollierung.** Spezifische Informationen über SQL Server-Datenbanken finden Sie unter Creating Full and Differential Backups of a SQL Server Database.

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 Failoverclustering in Windows Server mit SQL Server.
- **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 die anderen Lösungen, da auf jedem Datenbankserver eine vollständige SQL Server-Lizenz vorliegen muss. Die SQL Server Express Edition kann in einer gespiegelten Umgebung nicht verwendet werden.

- **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.

Der lokale Hostcache ergänzt die bewährten Methoden zum Bereitstellen hoher Verfügbarkeit bei SQL Server. Der lokale Hostcache ermöglicht Benutzern die Wiederverbindung mit Anwendungen und Desktops, 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 können. Im Hochverfügbarkeitsmodus akzeptiert der VDA direkte ICA-Verbindungen von Benutzern anstelle von durch den Controller vermittelten Verbindungen. Verwenden Sie dieses Feature nur in den seltenen Fällen, wenn die Kommunikation mit allen Controllern fehlschlägt. Das Features 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 normalerweise 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 Web 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, empfehlen wir die ausschließliche Verwendung einer anderen unterstützten SQL Server-Version als SQL Server Express. Installieren Sie SQL Server auf anderen Maschinen als dem Server, auf dem der erste Controller installiert ist. Unter 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 als Web Studio-Benutzer und Citrix Administrator die erforderlichen Berechtigungen für die Datenbank haben. (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 **Datenbanken mit Studio erstellen und einrichten**. Geben Sie dann die Namen und Adressen der Hauptdatenbanken an.

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 Web Studio automatisch erstellt und die Initialisierungsskripts für die Haupt- und Replikatdatenbanken ausgeführt.

Einrichtung per Skript

Wenn Sie nicht über die erforderlichen Datenbankrechte verfügen, bitten Sie einen Datenbankadministrator oder eine andere Person, die über entsprechende Berechtigungen verfügt, um Hilfe. Verfahren:

1. Wählen Sie im Assistenten für die Siteerstellung auf der Seite **Datenbanken** die Option **Generieren Sie Skripts, um Datenbanken auf dem Datenbankserver manuell einzurichten**. Dadurch werden die folgenden drei Skripttypen für jede der folgenden Hauptdatenbanken und deren Replikate erstellt: Site-, Überwachungs- und Protokollierungsdatenbank.

   - *Skript mit "SysAdmin"im Namen.* Skript, das die Datenbanken und die Delivery Controller-Anmeldung erstellt. Diese Aufgaben erfordern securityadmin-Rechte.
   - *Skript mit "DbOwner"im Namen.* Skript, das die Benutzerrollen in der Datenbank erstellt, die Anmeldungen hinzufügt und dann die Datenbankschemas erstellt. Diese Aufgaben erfordern `db_owner`-Rechte.
   - *Skript mit "Mixed"im Namen.* Alle Aufgaben in einem Skript, unabhängig von den erforderlichen Rechten.

   Sie können den Speicherort für die Skripts festlegen.

> **Hinweis:**
>
> In Unternehmensumgebungen umfasst die Datenbankeinrichtung Skripts, die ggf. von verschiedenen Teams mit unterschiedlichen Rollen (Rechten) verwendet werden: `securityadmin` oder `db_owner`. Zunächst werden ggf. "SysAdmin"-Skripts von Administratoren mit der Rolle `securityadmin` und anschließend "DbOwner"-Skripts von Administratoren mit der Berechtigung `db_owner` ausgeführt. Zum Generieren der Skripts können Sie auch PowerShell verwenden. Weitere Informationen finden Sie unter Skripts für bevorzugte Datenbankrechte.

2. Geben Sie die Skripts Ihrem Datenbankadministrator. Der Assistent für die Siteerstellung wird zu diesem Zeitpunkt automatisch angehalten. Wenn Sie später zu diesem Punkt zurückkommen, 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. Wir empfehlen 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 (sofern vorhanden).
- 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 dann die Backupdatei auf dem Spiegelungsserver wieder her. Starten Sie dann die Spiegelung auf dem Hauptserver.

Der Datenbankadministrator verwendet das SQLCMD-Hilfsprogramm oder mit SQL Server Management Studio im SQLCMD-Modus , um:

- Führen Sie jedes `xxx_Replica.sql`-Skript an den hoch verfügbaren SQL Server-Datenbankinstanzen aus (sofern hohe Verfügbarkeit konfiguriert ist).
- Führen Sie jedes `xxx\\_Principal.sql`-Skript an den SQL Server-Hauptdatenbankinstanzen aus.

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.

Web Studio fordert Sie auf, die Siteerstellung fortzusetzen. Sie werden zur Seite **Datenbanken** zurückgeleitet. 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 Web 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 ein Controller von einer Site entfernt wird, wird die Controller-Anmeldung für den Datenbankserver nicht entfernt. Auf diese Weise soll vermieden werden, dass eine Anmeldung entfernt wird, die von anderen Diensten als diesem Citrix Produkt auf derselben Maschine verwendet wird. Die Anmeldung muss manuell entfernt werden, wenn sie nicht mehr erforderlich ist. Dazu benötigen Sie die Serverrollenmitgliedschaft `securityadmin`.

Wenn Sie Web Studio für diese Vorgänge verwenden, muss der Web Studio-Benutzer entweder ein Datenbankserverkonto haben, das explizit Mitglied der entsprechenden Serverrollen ist, oder die Anmeldeinformationen eines Kontos angeben können.

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 die bevorzugten Datenbankrechte festlegen. 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. Melden Sie sich bei Web Studio an und wählen Sie im linken Bereich **Einstellungen**.
3. Suchen Sie die **Datenbank**-Kachel und wählen Sie **Bearbeiten**.
4. Wählen Sie auf der Seite **Datenbank verwalten** die Datenbank aus, für die Sie einen neuen Speicherort angeben möchten, und wählen Sie dann in der Aktionsleiste die Option **Datenbank ändern**.
5. Geben Sie den neuen Speicherort und den Datenbanknamen ein.
6. Wenn die Datenbank von Web Studio erstellt werden soll und Sie die notwendigen Berechtigungen haben, klicken Sie auf **Fertig**. Wenn Sie dazu aufgefordert werden, klicken Sie auf **Fertig**. Die Datenbank wird dann von Studio automatisch erstellt. Web 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 Web Studio in die Datenbank hochgeladen. Die Anmeldeinformationen werden nur für den Zeitraum der Datenbankerstellung gespeichert.
7. Wenn die Datenbank nicht von Web Studio erstellt werden soll oder Sie die erforderliche Berechtigung nicht haben, klicken Sie auf **Datenbankskript 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:

- Sizing the site database and configuring connection strings when using SQL Server high availability solutions.

Bereitstellungsmethoden

June 27, 2024

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. Weitere Informationen finden Sie unter App-V-Anwendungen bereitstellen.
- **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.

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.

Remote-PC-Zugriff

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.

Informationen hierzu finden Sie unter Remote-PC-Zugriff.

Netzwerkports

June 27, 2024

Die vollständigen Netzwerkportinformationen werden unter Von Citrix-Technologien verwendete Kommunikationsportsbereitgestellt.

Wenn Citrix Komponenten installiert werden, wird standardmäßig die Hostfirewall des Betriebssystems gemäß den Standardnetzwerkports aktualisiert.

Sie benötigen Portinformationen eventuell in folgenden Situationen:

- Zur Erfüllung gesetzlicher Auflagen
- Wenn sich zwischen Citrix Virtual Apps and Desktops-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

Einige 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.

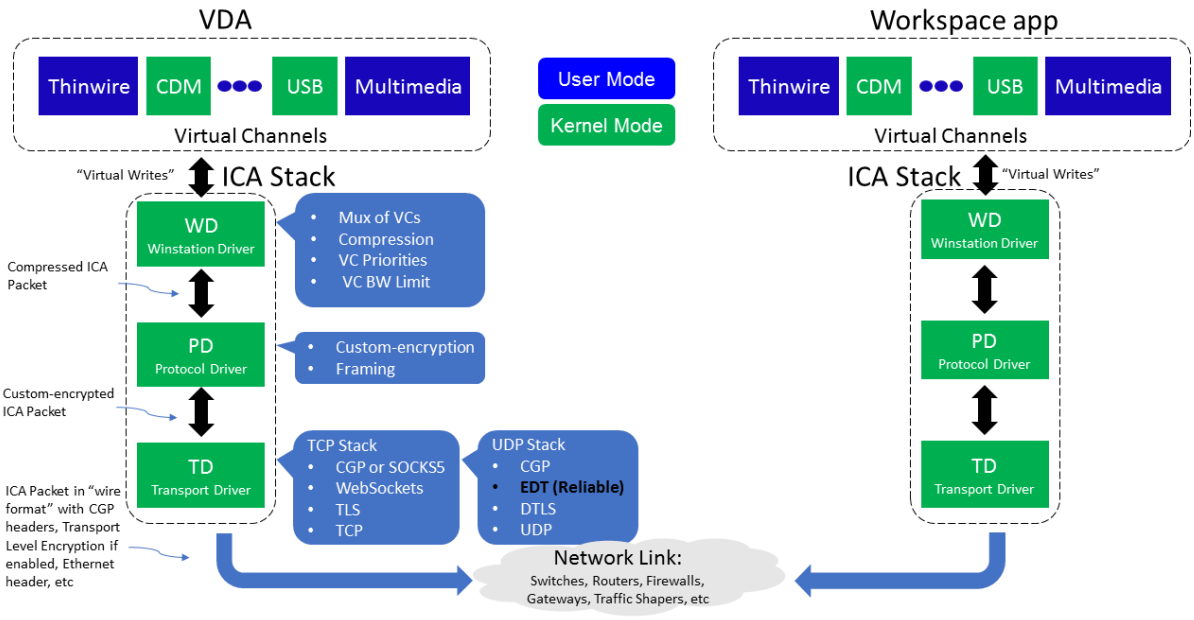
Das Betriebssystem auf dem VDA und auf dem Delivery Controller benötigt außerdem eigene eingehende Ports. Einzelheiten finden Sie in der Microsoft Windows-Dokumentation.

HDX

June 27, 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. Erstellen 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.

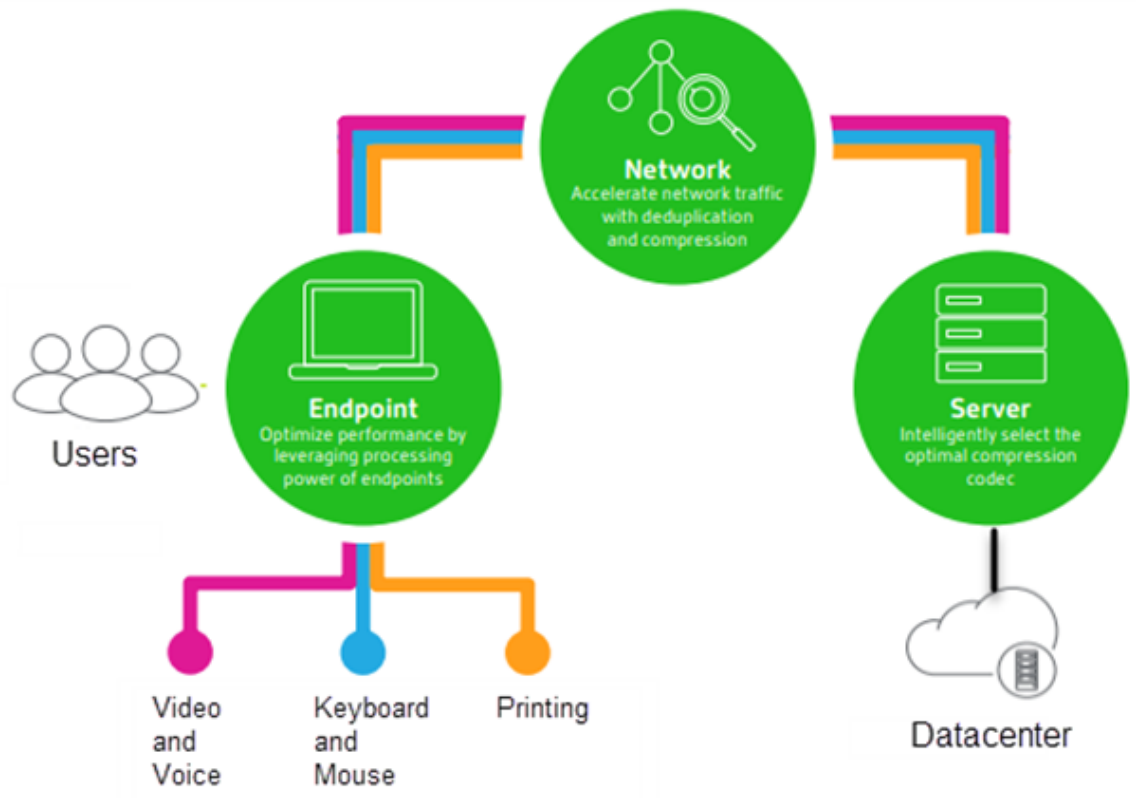


HDX basiert auf drei technischen Prinzipien:

- 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.

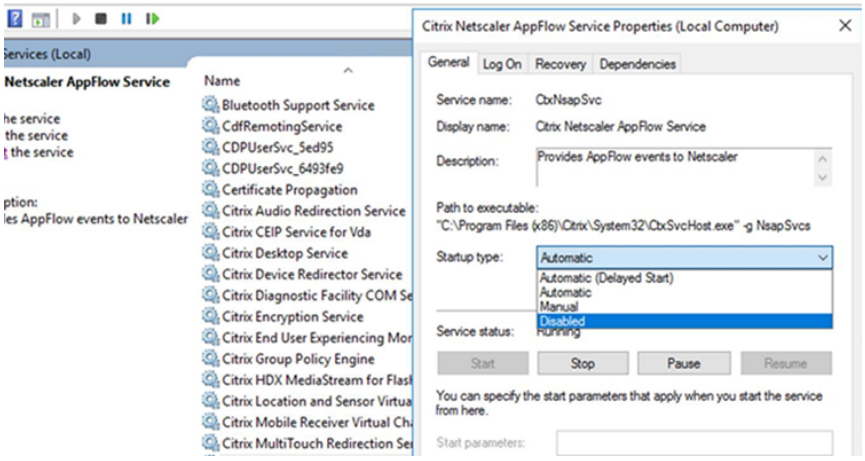
Sie können NetScaler zur Verwendung des virtuellen HDX Insight-Kanals aktivieren, um alle erforderlichen Datenpunkte unkomprimiert zu verschieben. Wenn Sie das Feature deaktivieren, entschlüsselt und dekomprimiert das NetScaler-Gerät den ICA-Datenverkehr über verschiedene virtuelle Kanäle hinweg. Die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

Mindestanforderungen:

- 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. Erstellen 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. 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.

> **Hinweis:**
>
> Die Einstellung **Anzeigespeicherlimit** ist veraltet. Seit dieser Änderung begrenzt Citrix den Anzeigespeicher jetzt nicht mehr. Stattdessen wird der erforderliche Mindestspeicher zugewiesen, um sicherzustellen, dass das Anzeigelayout des Clients vollständig berücksichtigt wird.

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

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-NetScaler SD-WAN 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 Registrierungs-Editor zu HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citri
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. Fügen Sie den folgenden Registrierungsschlüssel hinzu:

KEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

Name: EnableKlMap

Typ: DWORD

Wert: 1

Zum Deaktivieren des Features legen Sie **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. Fügen Sie den folgenden Registrierungsschlüssel hinzu:

HKEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

Name: DisableWindowHook

Typ: DWORD

Wert: 1

Legen Sie zur Verwendung der normalen Unicode-Tastaturzuordnung **DisableWindowHook** auf 0 fest.

Virtuelle ICA-Kanäle von Citrix

June 27, 2024

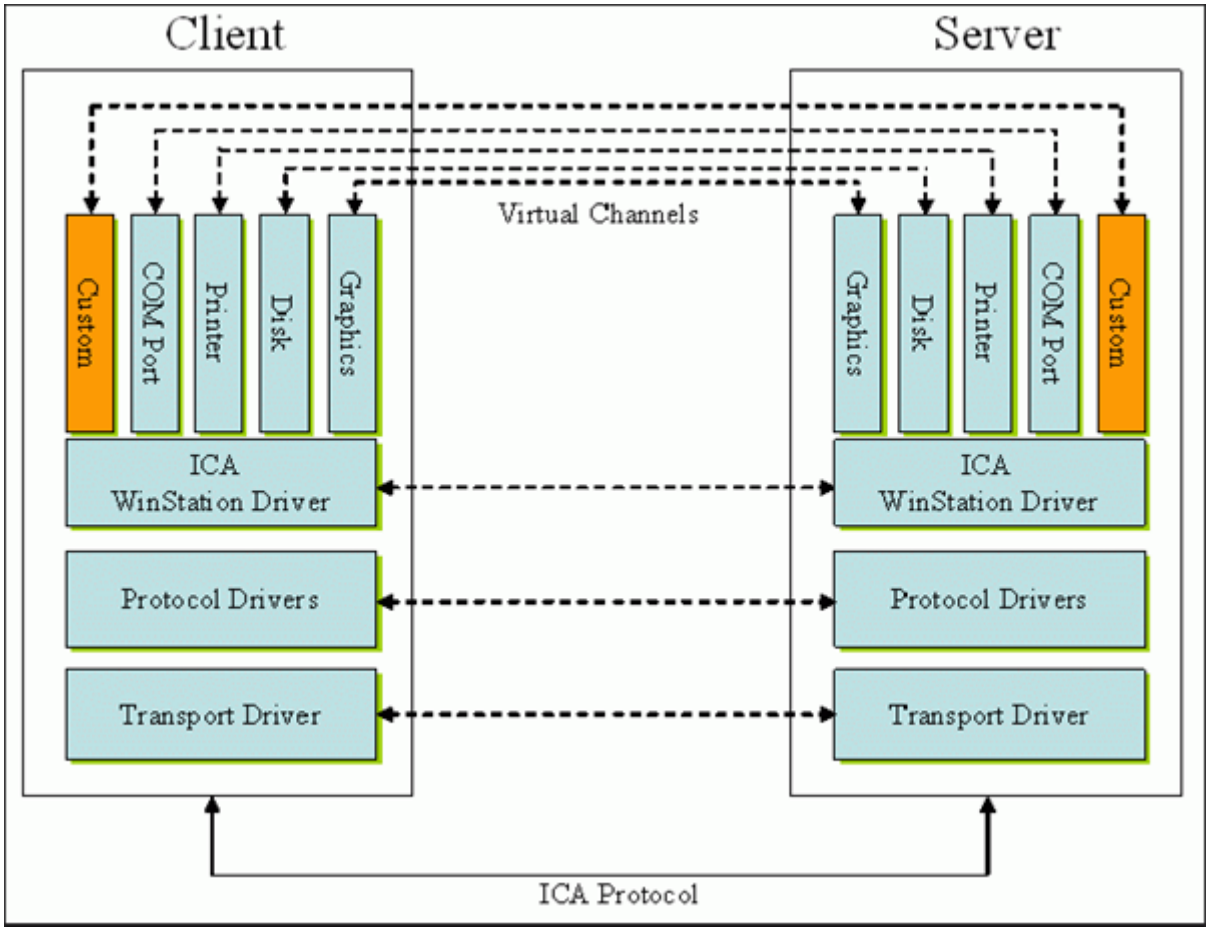
> **Warnung:**
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Erstellen 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

`ctxgfx.exe` hostet 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

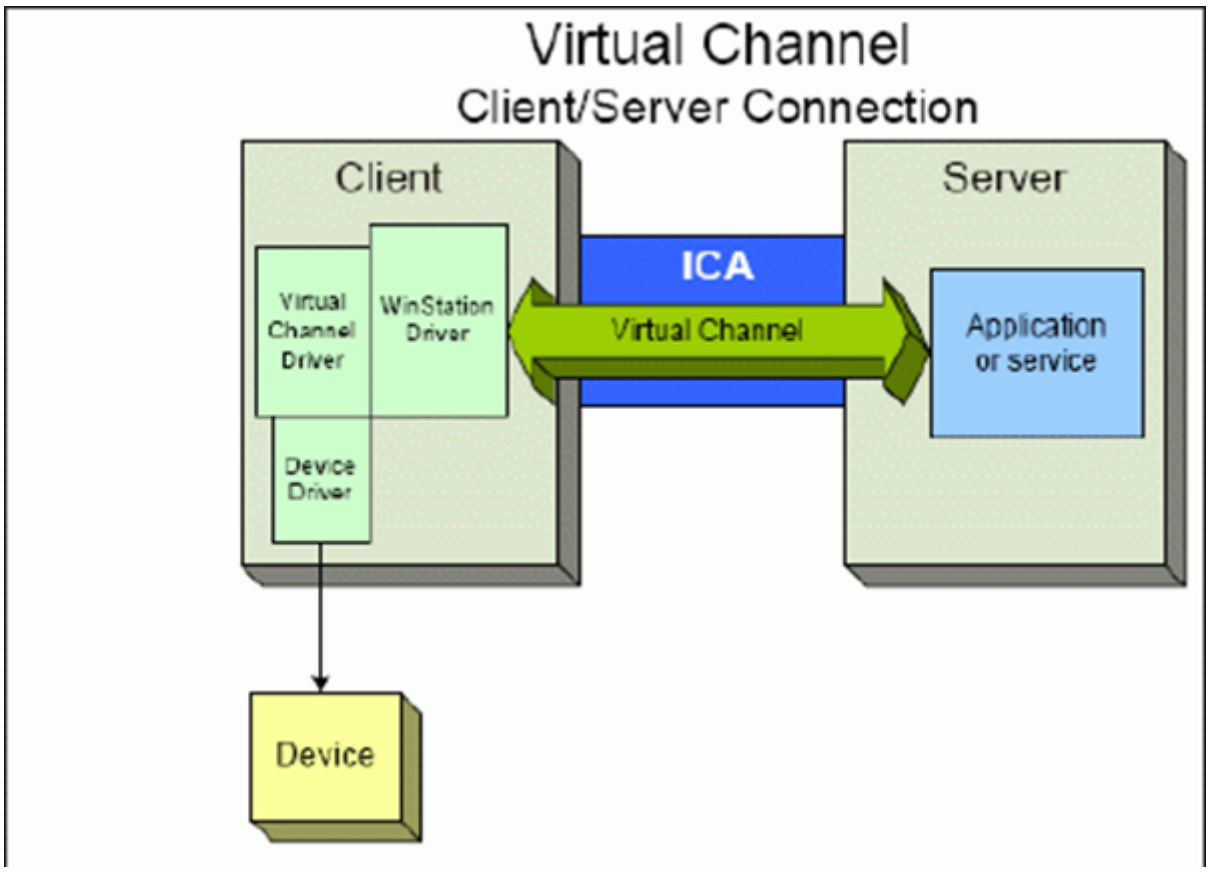
Auf Citrix Virtual Apps and Desktops-Servern werden verschiedene Kanäle als Windows-Dienste gehostet. Ein solches Hosting bietet eine Zuordnungssemantik vom Typ 1:n für mehrere Anwendungen in einer Sitzung und für mehrere Sitzungen auf dem Server. Beispiele für derartige Dienste:

- 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)
- Citrix ICA Status Channel Service

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

> **Hinweis:**
>
> Citrix SDKs sind im Citrix Developer-Portal unter https://developer.cloud.com verfügbar.

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.

> **Hinweis:**
>
> - Das Virtual Channel SDK erfordert, dass das WFAPI SDK die serverseitige Komponente des virtuellen Kanals schreibt.
> - Aufgrund des erhöhten Sicherheitsniveaus in Citrix Virtual Apps and Desktops müssen Sie angeben, welche virtuellen Kanäle in einer ICA-Sitzung geöffnet werden dürfen. Weitere Informationen finden Sie unter Richtlinieneinstellungen für Positivliste virtueller Kanäle.

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.

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
- Clientlaufwerkzuordnung
- Clientdruckerzuordnung
- Client-UPD
- End User Experience Monitoring
- Standard-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
- Clientlaufwerkzuordnung
- 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
Browserinhaltsumleitung	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

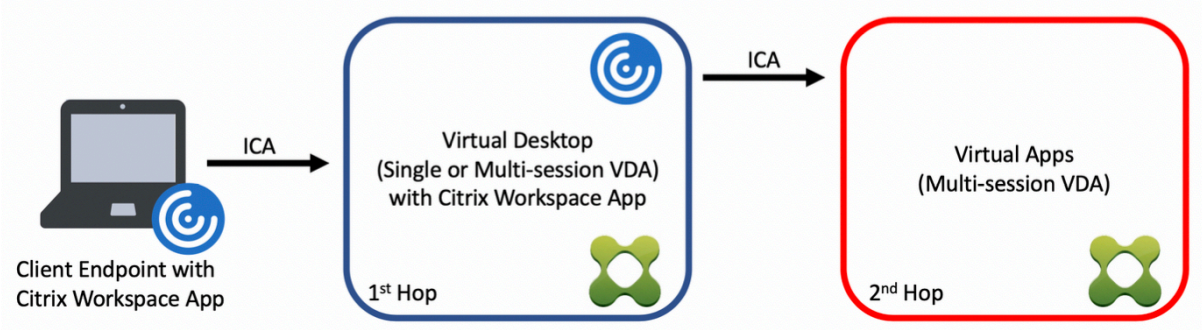
Siehe auch

- 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

June 27, 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 zum virtuellen Desktop 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 Desktops-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

June 27, 2024

Lesen Sie vor jedem Bereitstellungsschritt die Artikel, auf die verwiesen wird, um sich alle für die Bereitstellung erforderlichen Kenntnisse anzueignen.

Folgen Sie bei der Bereitstellung von Citrix Virtual Apps and Desktops der nachfolgend aufgeführten 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

Kernkomponenten installieren

Installieren Sie Delivery Controller, Web Studio, Citrix Director und Citrix Lizenzserver. Sie können auch Citrix StoreFront installieren. Einzelheiten finden Sie unter Installieren von Kernkomponenten bzw. Installieren über die Befehlszeile.

Site erstellen

Wenn Sie nach der Installation der Kernkomponenten Studio starten, werden Sie zum Erstellen einer Site aufgefordert.

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 Remote-PC-Zugriffbereitstellungen einen VDA für Einzelsitzungs-OS 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.

Maschinenkatalog erstellen

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 anderen Service 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.

Bereitstellungsgruppe erstellen

Nachdem Sie den ersten Maschinenkatalog in Web 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.

Anwendungsgruppe erstellen (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.

Bekannte Einschränkung

Wenn Sie die Citrix Workspace-App für Windows Version 1912 oder früher verwenden, wird die Sitzung nach einer Weile unterbrochen. Dieses Problem wurde in den neueren LTSR- und CR-Versionen der Citrix Workspace-App behoben.
Weitere Informationen zu den unterstützten Releaseversionen finden Sie unter Citrix Workspace-App für Windows/Citrix Receiver für Windows Long Term Service Releases.

Maschinenidentitäten

June 27, 2024

Jede Maschine muss eine eindeutige Maschinenidentität haben (“Computerkonto”). Maschinenidentitäten können lokal auf der Maschine oder in einem Verzeichnis (z. B. einem On-Premises-Active Directory oder Azure AD) erstellt und verwaltet werden. Citrix unterstützt das Hosten virtueller Anwendungen und Desktops auf in Active Directory oder Azure Active Directory eingebundenen Maschinen, Maschinen mit Azure AD-Hybrideinbindung oder auf Maschinen ohne Domänenbindung.

Maschinenidentitätstypen

Die folgenden Maschinenidentitätstypen werden unterstützt.

Maschinenidentitätstyp	Beschreibung
AD-Einbindung	Die Identitäten werden im On-Premises-Active Directory erstellt und verwaltet. Bereitgestellte Maschinen werden anhand der zugewiesenen Maschinenidentitäten mit dem On-Premises-Active Directory verbunden.
Azure AD-Hybrideinbindung	Die Identitäten werden im On-Premises-Active Directory erstellt und per Azure AD Connect mit Azure AD synchronisiert. Bereitgestellte Maschinen werden anhand der zugewiesenen Maschinenidentitäten mit dem On-Premises-Active Directory verbunden. Die Maschinen besitzen dann eine Azure AD-Hybrideinbindung. Beim Importieren einer VM mit Azure AD-Hybrideinbindung wird die VM von Citrix Virtual Apps and Desktops wie eine VM mit Active Directory-Einbindung behandelt.

Unterstützte Konfigurationen

Im Folgenden werden die unterstützten Konfigurationen für jedes Szenario erläutert.

Unterstützte Infrastruktur

Maschinenidentität	Citrix Virtual Apps and Desktops	Citrix Workspace	Citrix StoreFront	Citrix Gateway Service	Citrix Gateway
AD-Einbindung	Ja	Ja	Ja	Ja	Ja
In Azure AD eingebunden	Nein	Ja	Nein	Ja	Nein
Azure AD-Hybrideinbindung	Ja	Ja	Ja	Ja	Ja

Maschinenidentität	Citrix Virtual Apps and Desktops	Citrix Workspace	Citrix StoreFront	Citrix Gateway Service	Citrix Gateway
Nicht domänengebunden	Nein	Ja	Nein	Ja	Nein

Unterstützte Identitätsanbieter für die Workspace-Authentifizierung

Maschinenidentität	Azure Active Directory	Active Directory	Active Directory und Token	Okta	SAML	Citrix Gateway	Adaptive Authentifizierung
AD-Einbindung	Ja	Ja	Ja	Ja	Ja	Ja	Ja
In Azure AD eingebunden	Ja	Nein	Nein	Nein	Nein	Nein	Nein
Azure AD-Hybrideinbindung	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Nicht domänengebunden	Ja	Ja	Ja	Ja	Ja	Ja	Ja

Active Directory-Einbindung

June 27, 2024

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. Zum Verwenden der Richtlinienmodellierung muss der Domänencontroller unter Windows

Server 2003 bis Windows Server 2012 R2 ausgeführt werden. Dies hat keine Auswirkung auf die Domänenfunktionsebene.

Dieses Produkt unterstützt Folgendes:

- **Bereitstellungen, in denen die Benutzerkonten und Computerkonten in Domänen in einer einzigen Active Directory-Gesamtstruktur bestehen.** Benutzer- und Computerkonten können in beliebigen Domänen in einer Gesamtstruktur bestehen. Alle Domänen- und Gesamtstrukturebenen werden in diesem Bereitstellungstyp unterstützt.
- **Bereitstellungen, in denen die Benutzerkonten und die Computerkonten der Controller und virtuellen Desktops in unterschiedlichen Active Directory-Gesamtstrukturen bestehen.** Bei diesem Bereitstellungstyp muss eine Vertrauensstellung zwischen den Domänen mit den Computerkonten der Controller und virtuellen Desktops und den Domänen mit den Benutzerkonten bestehen. Sie können Gesamtstruktur- oder externe Vertrauensstellungen verwenden. Alle Domänen- und Gesamtstrukturebenen werden in diesem Bereitstellungstyp unterstützt.
- **Bereitstellungen, in denen die Computerkonten für Controller in einer Active Directory-Gesamtstruktur bestehen, die sich von den zusätzlichen Active Directory-Gesamtstrukturen mit den Computerkonten für die virtuellen Desktops unterscheidet.** Bei diesem Bereitstellungstyp muss eine bidirektionale Vertrauensstellung zwischen den Domänen mit den Computerkonten der Controller und allen Domänen mit den Computerkonten der virtuellen Desktops bestehen. Bei diesem Bereitstellungstyp müssen alle Domänen mit Computerkonten für Controller oder virtuelle Desktops mindestens auf der Funktionsebene “Windows 2000 native”sein. Alle Funktionsebenen der Gesamtstruktur werden unterstützt.
- **Beschreibbarer Domänencontroller.** Schreibgeschützte Domänencontroller werden nicht unterstützt.

Virtual Delivery Agents (VDAs) können mit in Active Directory veröffentlichten Informationen die Contoller ermitteln, bei denen sie sich registrieren können (Discovery). Diese Methode wird primär für Abwärtskompatibilität unterstützt und ist nur verfügbar, wenn die VDAs und die Controller in derselben Active Directory-Gesamtstruktur sind. Informationen über diese Discovery-Methode finden Sie unter Active Directory-basierte Discovery und CTX118976.

> **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

Bei einer Active Directory-Umgebung mit mehreren Gesamtstrukturen und unidirektionalen oder bidirektionalen Vertrauensstellungen können Sie DNS-Weiterleitungen oder bedingte Weiterleitun-

gen 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 zu VDA und Delivery Controllern 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.

Ein Registrierungseintrag wurde hinzugefügt, um das Aktivieren der NTLM-Authentifizierung in VDAs zu vermeiden, da dies weniger Sicherheit bietet als Kerberos. Dieser Eintrag kann anstelle des Eintrags `SupportMultipleForest` verwendet werden, der aus Gründen der Abwärtskompatibilität weiterhin verwendet werden kann.

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

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

Dieser Registrierungsschlüssel führt eine DDC-Suche in einer Umgebung mit mehreren Gesamtstrukturen und bidirektionaler Vertrauensstellung durch. Damit können Sie die NTLM-basierte Authentifizierung während der ersten Registrierung entfernen.

Wenn externe Vertrauensstellungen während des Setups vorhanden sind, ist der Registrierungsschlüssel ListOfSIDs erforderlich. Der Registrierungsschlüssel ListOfSIDs ist auch erforderlich, wenn Active Directory und DNS unterschiedliche vollqualifizierte Domänennamen (FQDN) verwenden, oder wenn 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 den Text allowNtlm="false" und ändern Sie ihn 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

Vertrauenstyp	Transitivität	Richtung	In diesem Release unterstützt
Extern	Nicht transitiv	Unidirektional oder bidirektional	Ja
Gesamtstruktur	Transitiv	Unidirektional oder bidirektional	Ja
Verknüpfung	Transitiv	Unidirektional oder bidirektional	Ja
Bereich	Transitiv oder nicht transitiv	Unidirektional oder bidirektional	Nein

Weitere Informationen über komplexe Active Directory-Umgebungen finden Sie unter CTX134971.

Azure Active Directory-Hybrideinbindung

June 27, 2024

> **Hinweis:**
>
> Seit Juli 2023 hat Microsoft Azure Active Directory (Azure AD) in Microsoft Entra ID umbenannt. In diesem Dokument bezieht sich jeder Verweis auf Azure Active Directory, Azure AD oder AAD jetzt auf Microsoft Entra ID.

Dieser Artikel enthält alle Anforderungen, die zusätzlich zu den Systemanforderungen für Citrix DaaS erforderlich sind, um Kataloge mit Azure Active Directory-Hybrideinbindung (HAAD) über Citrix DaaS zu erstellen.

Maschinen mit Azure AD-Hybrideinbindung verwenden das On-Premises-AD als Authentifizierungsanbieter. Sie können sie Domänenbenutzern oder Gruppen im On-Premises-AD zuweisen. Um eine nahtlose SSO-Erfahrung für Azure AD zu ermöglichen, müssen die Domänenbenutzer mit Azure AD synchronisiert werden.

> **Hinweis:**
>
> VMs mit Azure AD-Hybrideinbindung werden in Infrastrukturen mit Verbund- und verwalteter Identität unterstützt.

Anforderungen

- VDA-Typ: Einzelsitzung (nur Desktops) und Multisitzung (Apps und Desktops)

- VDA-Version: 2212 oder höher
- Provisioningtyp: Maschinenerstellungsdienste (MCS), persistent und nicht persistent
- Zuweisungstyp: dediziert und gepoolt
- Hostingplattform: Beliebiger Hypervisor oder Cloudservice

Einschränkungen

- Wenn Sie den Citrix Verbundauthentifizierungsdienst (FAS) verwenden, wird Single Sign-On an das On-Premises-AD und nicht an Azure AD weitergeleitet. In diesem Fall wird empfohlen, die zertifikatbasierte Azure AD-Authentifizierung zu konfigurieren. Der primäre Aktualisierungstoken (PRT) wird dann bei der Benutzeranmeldung generiert und ermöglicht einen Single Sign-On bei Azure AD-Ressourcen in der Sitzung. Andernfalls fehlt der primäre Aktualisierungstoken (PRT), und der Single Sign-On für Azure AD-Ressourcen funktioniert nicht. Informationen zum Erreichen von Azure AD Single Sign-On (SSO) bei VDAs mit Hybrideinbindung mithilfe des Citrix Verbundauthentifizierungsdiensts (FAS) finden Sie unter VDAs mit Hybrideinbindung.
- Überspringen Sie nicht die Imagevorbereitung, während Sie Maschinenkataloge erstellen oder aktualisieren. Wenn Sie die Imagevorbereitung überspringen möchten, dürfen die Master-VMs nicht in Azure AD oder Azure AD Hybrid eingebunden sein.

Überlegungen

- Zum Erstellen hybrider Maschinen mit Azure Active Directory-Einbindung ist die Berechtigung `Write userCertificate` in der Zieldomäne erforderlich. Stellen Sie sicher, dass Sie sich bei der Katalogerstellung als Administrator mit dieser Berechtigung anmelden.
- Der Prozess der Azure AD-Hybrideinbindung wird von Citrix verwaltet. Sie müssen das von Windows gesteuerte `autoWorkplaceJoin` auf den Master-VMs wie folgt deaktivieren. Die manuelle Deaktivierung von `autoWorkplaceJoin` ist nur für VDA-Version 2212 oder früher erforderlich.

  1. Führen Sie `gpedit.msc` aus.
  2. Gehen Sie zu **Computerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Geräteregistrierung**.
  3. Legen Sie für **In die Domäne eingebundene Computer als Geräte registrieren** die Option **Deaktiviert** fest.

- Wählen Sie die für die Synchronisierung mit Azure AD konfigurierte Organisationseinheit, wenn Sie die Maschinenidentitäten erstellen.
- Erstellen Sie auf Master-VMs mit Windows 11 22H2 einen geplanten Task, der die folgenden Befehle beim Systemstart mit dem SYSTEM-Konto ausführt. Das Planen eines Task in der Master-VM ist nur für VDA-Version 2212 oder früher erforderlich.


```
$VirtualDesktopKeyPath = 'HKLM:\Software\AzureAD\VirtualDesktop'
$WorkplaceJoinKeyPath = 'HKLM:\SOFTWARE\Policies\Microsoft\
    Windows\WorkplaceJoin'
$MaxCount = 60

for ($count = 1; $count -le $MaxCount; $count++)
{

  if ((Test-Path -Path $VirtualDesktopKeyPath) -eq $true)
  {

    $provider = (Get-Item -Path $VirtualDesktopKeyPath).GetValue(
        "Provider", $null)
    if ($provider -eq 'Citrix')
    {

        break;
     }


    if ($provider -eq 1)
    {

        Set-ItemProperty -Path $VirtualDesktopKeyPath -Name "
            Provider" -Value "Citrix" -Force
        Set-ItemProperty -Path $WorkplaceJoinKeyPath -Name "
            autoWorkplaceJoin" -Value 1 -Force
        Start-Sleep 5
        dsregcmd /join
        break
     }

   }


  Start-Sleep 1
 }

<!--NeedCopy-->
```

So geht es weiter

Weitere Informationen zum Erstellen von Katalogen mit Azure Active Directory-Hybrideinbindung finden Sie unter Kataloge mit Azure Active Directory-Hybrideinbindung erstellen.

Vorbereiten der Installation

June 27, 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 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 eine zusätzliche Komponente (z. B. Citrix Gateway) für Benutzer, die außerhalb Ihrer Firewall sind. Eine Einführung finden Sie unter Integrieren von Citrix Virtual Apps and Desktops und Citrix Gateway.

> **Hinweis:**
>
> Vergewissern Sie sich, dass die folgenden Microsoft-Voraussetzungen auf dem Serverbetriebssystem und dem Arbeitsstations-Betriebssystem erfüllt sind:
>
> - Die Microsoft-Dienste **Volumenschattenkopie** und **Microsoft-Softwareschattenkopie-Anbieter** werden ausgeführt. Weitere Informationen finden Sie unter Volumenschattenkopie-Dienst.
> - Die **MS-Defender**-Version muss höher als 4.18.2105.5 sein. Weitere Informationen finden Sie unter Microsoft Defender Antivirus Security Intelligence und Produktupdates.

Wenn Ihre Bereitstellung Windows Server-Workloads umfasst, konfigurieren Sie einen Microsoft RDS-Lizenzserver.

Mit dem Produktinstallationsprogramm auf dem ISO-Image können Sie viele Komponenten und Technologien installieren. VDAs können Sie mit dem eigenständigen VDA-Installationsprogramm installieren. Die dedizierten VDA-Installationspakete stehen auf den Citrix Downloadseiten zur Verfügung. 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 Images einsetzen, die von den Maschinenerstellungsdiensten und Citrix Provisioning (zuvor "Provisioning

Services") verwendet werden. Weitere Informationen finden Sie unter Installieren von VDAs mit Skripts.

Vor Installation zu lesende Informationen

- Technischer Überblick: Hier können Sie sich mit dem Produkt und seinen Komponenten vertraut machen.
- Sicherheit: Wenn Sie Ihre Bereitstellungsumgebung planen.
- Bekannte Probleme: Probleme, auf die Sie in dieser Version stoßen könnten.
- 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 einem anderen Dienst 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.
- **Hostverbindungen zur öffentlichen Cloud:** Wenn Sie eine Hybrid Rights-Lizenz haben, können Sie Hostverbindungen zur öffentlichen Cloud erstellen. Informationen zur Hybrid Rights-Lizenz finden Sie unter Hybrid Rights-Verlängerung. Informationen zum Anspruch für die öffentliche Cloud und den Gründen für diese Änderung finden Sie unter CTX270373.

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.

  Installieren Sie den Citrix Lizenzserver und die Lizenzen, bevor Sie andere Komponenten auf anderen Servern installieren.

- Das Installieren einer unterstützten Komponente auf einem Server-CoreOS (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.

Vergewissern Sie sich, dass für jedes Betriebssystem die neuesten Updates ausgeführt wurden.

Vergewissern Sie sich, dass bei allen Maschinen die Systemuhren synchronisiert sind. Die Kerberos-Infrastruktur, die die Kommunikation zwischen den Maschinen sichert, muss synchronisiert werden.

Bei XenServer kann der Energiezustand der virtuellen Maschine als unbekannt angezeigt werden, 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.

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.

Wenn Sie einen VDA in einem von dieser Produktversion nicht unterstützten Windows-Betriebssystem installieren oder aktualisieren, werden Sie 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 einem eigenständigen VDA-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. Active Directory-Einbindung enthält weitere Informationen.
- 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 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 eines Delivery Controllers, Lizenzservers oder von Studio oder Director, 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 von Citrix Analytics automatisch Analysedaten gesammelt. Standardmäßig werden die Daten automatisch an Citrix hochgeladen, wenn die Installation abgeschlossen ist. Bei der Installation von Komponenten werden Sie außerdem automatisch beim Citrix Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) angemeldet, in dessen Rahmen anonyme Daten hochgeladen werden.

  Während der Installation können Sie wahlweise auch die Teilnahme bei anderen Citrix Programmen 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 Microsoft Druckspoolerdienst muss aktiviert sein. Wenn dieser Dienst deaktiviert ist, können Sie keinen VDA installieren.
- Bei den meisten unterstützten Windows-Editionen ist Microsoft Media Foundation bereits installiert. Wenn Media Foundation nicht installiert ist (z. B. N-Editionen), werden mehrere Multimediafeatures nicht installiert und sind nicht funktionsfähig.

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

  Sie können diese Einschränkung bestätigen oder die VDA-Installation beenden und später, nach der Installation von Media Foundation neu beginnen. Diese Auswahl wird bei der grafischen Oberfläche per Meldung angeboten. In der Befehlszeile können Sie zum Bestätigen der Einschränkung die Option `/no_mediafoundation_ack` verwenden.
- 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. Weitere Informationen finden Sie unter VDA-Registrierung.

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.

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

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.

Wenn Sie ein Upgrade für eine VDA-Version einrichten, erfolgt während des Upgrades ein Neustart. Dies kann nicht vermieden werden.

Wiederherstellung bei Installations- oder Upgradefehler

> **Hinweis:**
>
> Dieses Feature ist für Einzelsitzungs- und Multisitzungs-VDAs verfügbar.

Wenn das Installieren oder Aktualisieren eines Einzelsitzungs-VDAs fehlschlägt und das Feature “Wiederherstellung bei Fehler”aktiviert ist, wird die Maschine auf einen zuvor festgelegten Wiederherstellungspunkt zurückgesetzt.

Wenn das Installieren oder Aktualisieren eines Multisitzungs-VDA fehlschlägt und das Feature "Wiederherstellung bei Fehler"aktiviert ist, wird die Maschine auf ein Backup zurückgesetzt, das vor dem Start der Installation oder des Upgrades erstellt wurde.

Wenn das Feature beim Start einer Installation oder eines Upgrades für Einzelsitzungs-VDAs aktiviert ist, erstellt das Installationsprogramm zunächst einen Systemwiederherstellungspunkt. Wenn die anschließende VDA-Installation oder das Upgrade fehlschlägt, wird die Maschine in den Zustand des Wiederherstellungspunkts zurückgesetzt. Der Ordner `%temp%/Citrix` enthält Bereitstellungsprotokolle und andere Informationen zur Wiederherstellung.

Wenn das Feature beim Start einer Installation oder eines Upgrades für Multisitzungs-VDAs aktiviert ist, erstellt das Installationsprogramm vor Beginn der Installation oder des Upgrades ein Serverbackup. Wenn die anschließende VDA-Installation oder das Upgrade fehlschlägt, wird die Maschine auf den Backupzustand zurückgesetzt. Der Ordner `%temp%/Citrix` enthält Bereitstellungsprotokolle und andere Informationen zur Wiederherstellung. Der für die Erstellung des Serverbackups erforderliche Zeitraum basiert auf der Größe des benötigten Backups und der Menge an Ressourcen, die dem Server zur Verfügung stehen. Das Backup wird unter *C:\WindowsImageBackup\servername* gespeichert.

Standardmäßig ist dieses Feature deaktiviert.

Wenn Sie dieses Feature aktivieren möchten, müssen Sie sicherstellen, dass die Systemwiederherstellung nicht über eine GPO-Einstellung deaktiviert ist (`Computer Configuration` > `Administrative Templates` > `System` > `System Restore`).

> **Hinweis:**
>
> Diese GPO-Einstellung gilt nicht für die Wiederherstellung von Multisitzungs-VDAs.

Aktivieren des Features beim Installieren oder Aktualisieren eines Einzelsitzungs- oder Multisitzungs-VDA:

- Wenn Sie die grafische Benutzeroberfläche eines VDA-Installationsprogramms (z. B. **Autostart** oder den Befehl `XenDesktopVDASetup.exe` ohne Optionen für Wiederherstellung und stillen Modus) verwenden, aktivieren Sie auf der Seite **Zusammenfassung** das Kontrollkästchen **Wiederherstellung bei Fehler aktivieren**.

  Nach dem erfolgreichen Abschluss der Installation oder des Upgrades wird der Wiederherstellungspunkt/das Backup nicht verwendet, aber beibehalten.

- Führen Sie ein VDA-Installationsprogramm mit der Option `/enablerestore` oder `/enablerestorecleanup` über die Befehlszeile aus.

  - Wenn Sie die Option `/enablerestorecleanup` verwenden, wird der Wiederherstellungspunkt/das Serverbackup nach dem erfolgreichen Abschluss der Installation oder des Upgrades automatisch entfernt.

- Wenn Sie die Option `/enablerestore` verwenden, wird der Wiederherstellungspunkt nach dem erfolgreichem Abschluss der Installation oder des Upgrades nicht verwendet, aber beibehalten.

Installationsprogramme

Komplettinstallationsprogramm

Mit dem im ISO-Image enthaltenen Komplettinstallationsprogramm:

- Installieren, aktualisieren oder entfernen Sie Kernkomponenten (Delivery Controller, Studio, Director und Lizenzserver).
- Installieren oder aktualisieren Sie StoreFront.
- Installieren oder aktualisieren Sie Windows-VDAs für Einzelsitzungs-OS oder Multisitzungs-OS.
- Installieren Sie den universellen Druckserver `UpsServer` auf den Druckservern.
- Verbundauthentifizierungsdienst installieren
- Installieren Sie die Sitzungsaufzeichnung.
- Installieren Sie Workspace Environment Management.

> **Hinweis:**
>
> Das Installationsprogramm für Workspace Environment Management Agents ist nicht lokalisiert. Es ist nur in englischer Sprache verfügbar.

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. (Sie sind nicht auf dem Produktinstallationsmedium verfügbar.) Die eigenständigen VDA-Installationsprogramme sind wesentlich kleiner als das vollständige ISO-Image. Sie eignen sich besser für Bereitstellungen, auf die Folgendes zutrifft:

- Verwenden lokal bereitgestellte oder kopierte ESD-Pakete (Electronic Software Distribution)
- Umfassen physische Maschinen
- Umfassen Remotestandorte

Standardmäßig werden die Dateien im selbstextrahierenden Paket für VDAs in den Ordner **Temp** extrahiert. Zum Extrahieren in den Ordner **Temp** wird auf der Maschine mehr Speicherplatz beansprucht, als wenn Sie das Produktinstallationsprogramm verwenden. In den Ordner **Temp** extrahierte Dateien werden allerdings automatisch gelöscht, wenn die Installation abgeschlossen ist. Alternativ können Sie den Befehl `/extract` mit einem absoluten Pfad verwenden.

Drei eigenständige VDA-Installationsprogramme stehen zum Herunterladen zur Verfügung.

VDAServerSetup.exe:

Installiert einen VDA für 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 Image verwendet werden. Es werden nur die für VDA-Verbindungen erforderlichen Kerndienste installiert. Daher unterstützt es nur einen Teil der Optionen des Produktinstallationsprogramms bzw. von `VDAWorkstationSetup.exe`.

Dieses Installationsprogramm installiert keine Komponenten für Folgendes:

- App-V.
- Profilverwaltung. Das Ausschließen der Citrix Profilverwaltung bei der Installation hat Auswirkungen auf die Anzeigen von Citrix Director. Weitere Informationen finden Sie unter Installieren von VDAs.
- Maschinenidentitätsdienst.
- 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. `VDAWorkstationSetup` 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` plus Option `/exclude` zum Auflisten aller gültigen zusätzlichen Komponenten.

Sie können die ausgelassenen Komponenten/Features später mit dem Produktinstallationsprogramm installieren. Diese Aktion ermöglicht die Installation aller fehlenden Komponenten.

Die Browserinhaltsumleitung-MSI wird vom Installationsprogramm `VDAWorkstationCoreSetup.exe` automatisch installiert. Die automatische Installation erfolgt in unterstützten VDA-Releases ab Release 2003.

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 RDS-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.

Konfigurieren eines Microsoft RDS-Lizenzservers für Windows Server-Workloads

Dieses Produkt greift bei der Bereitstellung einer Windows Server-Workload (z. B. Windows 2016) auf Windows Server-Remotesitzungsfunktionen zu. Dies erfordert in der Regel eine Clientzugriffslizenz für Remotedesktopdienste (RDS CAL). Der VDA muss in der Lage sein, RDS-CALs von einem RDS-Lizenzserver anzufordern. Installieren und aktivieren Sie den Lizenzserver. Weitere Informationen finden Sie in der Microsoft-Dokumentation unter Aktivieren des Remotedesktopdienste-Lizenzservers. Für Machbarkeitsstudien können Sie den von Microsoft bereitgestellten Kulanzzeitraum verwenden.

Mit dieser Methode können Sie die Lizenzservereinstellungen mithilfe dieses Service anwenden. Sie können den Lizenzserver und den "Pro-Benutzer"-Lizenzmodus in der RDS-Konsole auf dem Image konfigurieren. Sie können den Lizenzserver auch über die Microsoft-Gruppenrichtlinieneinstellungen konfigurieren. Weitere Informationen finden Sie in der Microsoft-Dokumentation unter License your RDS deployment with client access licenses (CALs).

Konfigurieren des RDS-Lizenzservers über die Gruppenrichtlinieneinstellungen:

1. Installieren Sie einen Lizenzserver für die Remotedesktopdienste auf einer verfügbaren Maschine. Die Maschine muss immer verfügbar sein. Die Citrix Produktworkloads müssen auf diesen Lizenzserver zugreifen können.
2. Geben Sie über die Microsoft-Gruppenrichtlinie die Lizenzserveradresse ein und legen Sie den "Pro-Benutzer"-Lizenzmodus fest. Weitere Informationen finden Sie in der Microsoft-Dokumentation unter Specify the Remote Desktop Licensing Mode for an RD Session Host Server.

Windows 10-Workloads erfordern eine Windows 10-Lizenzaktivierung. Wir empfehlen, dass Sie zum Aktivieren von Windows 10-Workloads der Microsoft-Dokumentation folgen.

Weitere Informationen

Einrichten des Ressourcenstandorts für bestimmte Hosttypen:

- AWS-Cloudumgebungen
- XenServer-Virtualisierungsumgebungen
- Google Cloud-Umgebungen
- Microsoft Azure Resource Manager-Cloudumgebungen
- Microsoft System Center Configuration Manager-Umgebungen
- Microsoft System Center Virtual Machine Manager-Virtualisierungsumgebungen
- Nutanix-Virtualisierungsumgebungen
- Nutanix-Cloud und Partnerlösungen
- VMware-Virtualisierungsumgebungen

- Cloud- und Partnerlösungen von VMware

AWS-Cloudumgebungen

June 28, 2024

Dieser Artikel erläutert das Einrichten eines AWS-Kontos als Ressourcenstandort für Citrix Virtual Apps and Desktops. Der Ressourcenstandort enthält eine Reihe grundlegender Komponenten, die sich ideal für Machbarkeitsstudien oder andere Bereitstellungen eignen, bei denen keine Ressourcenverteilung über mehrere Verfügbarkeitszonen erforderlich ist. Nachdem Sie die hier aufgeführten Aufgaben ausgeführt haben, können Sie VDAs installieren, Maschinen bereitstellen und Maschinenkataloge sowie Bereitstellungsgruppen erstellen.

Mit den im vorliegenden Artikel aufgeführten Aufgaben wird ein Ressourcenstandort mit folgenden Komponenten erstellt:

- Eine virtuelle private Cloud (VPC) mit öffentlichen und privaten Subnetzen in einer einzelnen Verfügbarkeitszone.
- Eine Instanz, die sowohl als Active Directory-Domänencontroller als auch als DNS-Server ausgeführt wird und im privaten Subnetz der VPC residiert.
- Eine Instanz, die als Bastionshost im öffentlichen Subnetz der VPC fungiert. Mit dieser Instanz werden RDP-Verbindungen zu den Instanzen im privaten Subnetz für Verwaltungszwecke initiiert. Wenn Sie den Ressourcenstandort eingerichtet haben, können Sie diese Instanz herunterfahren, sodass sie nicht mehr ohne Weiteres verfügbar ist. Wenn Sie andere Instanzen im privaten Subnetz verwalten müssen, z. B. VDA-Instanzen, müssen Sie die Bastionshostinstanz neu starten.

Aufgabenüberblick

Einrichten einer virtuellen privaten Cloud (VPC) mit öffentlichen und privaten Subnetzen: Wenn Sie diese Aufgabe ausführen, stellt AWS ein NAT-Gateway mit einer Elastic IP Address im öffentlichen Subnetz bereit. Dadurch können Instanzen im privaten Subnetz auf das Internet zugreifen. Instanzen im öffentlichen Subnetz sind für eingehenden öffentlichen Datenverkehr zugänglich, Instanzen im privaten Subnetz dagegen nicht.

Konfigurieren von Sicherheitsgruppen. Sicherheitsgruppen fungieren als virtuelle Firewall und steuern den Datenverkehr für die Instanzen in der VPC. Sie fügen den Sicherheitsgruppen Regeln zur Kommunikation zwischen Instanzen im öffentlichen und im privaten Subnetz hinzu. Sie ordnen die Sicherheitsgruppen außerdem jeder Instanz in der VPC zu.

Erstellen eines DHCP-Optionssatzes. Bei Amazon-VPCs werden DHCP- und DNS-Dienste standardmäßig bereitgestellt, was sich auf Ihre Konfiguration von DNS auf dem Active Directory-Domänencontroller auswirkt. Amazon-DHCP kann nicht deaktiviert werden und das Amazon-DNS kann nur für die öffentliche DNS-Auflösung, nicht aber für die Active Directory-Namensauflösung verwendet werden. Um die Domänen- und Namenserver anzugeben, die Instanzen über DHCP übergeben werden, erstellen Sie einen DHCP-Optionssatz. Dieser weist das Active Directory-Domänensuffix zu und gibt den DNS-Server für alle Instanzen in der VPC an. Um sicherzustellen, dass Host- (A) und Reverse-Lookup-Datensätze (PTR-Datensätze) automatisch registriert werden, wenn Instanzen der Domäne beitreten, konfigurieren Sie die Netzwerkadaptereigenschaften für jede Instanz, die Sie dem privaten Subnetz hinzufügen.

Fügen Sie der VPC einen Bastionshost und einen Domänencontroller hinzu. Über den Bastionshost können Sie sich bei Instanzen im privaten Subnetz anmelden, um die Domäne einzurichten und der Domäne Instanzen anzufügen.

Aufgabe 1: Einrichten der VPC

1. Wählen Sie in der AWS-Verwaltungskonsole **VPC**.
2. Wählen Sie im VPC-Dashboard die Option **Create VPC**.
3. Wählen Sie **VPC and more**.
4. Wählen Sie unter "NAT gateways ($)"**In 1 AZ**oder **1 per AZ**.
5. Lassen Sie unter "DNS Options"die Option **Enable DNS hostnames** aktiviert.
6. Wählen Sie **Create VPC**. AWS erstellt das öffentliche und private Subnetz, das Internetgateway, die Routingtabellen und die Standardsicherheitsgruppe.

Aufgabe 2: Konfigurieren von Sicherheitsgruppen

Bei diesem Vorgang werden die folgenden Sicherheitsgruppen für die VPC erstellt und konfiguriert:

- Eine öffentliche Sicherheitsgruppe, die den Instanzen in Ihrem öffentlichen Subnetz zugeordnet werden.
- Eine private Sicherheitsgruppe, die den Instanzen in Ihrem privaten Subnetz zugeordnet werden.

So erstellen Sie die Sicherheitsgruppen:

1. Wählen Sie im VPC-Dashboard **Sicherheitsgruppen**.
2. Erstellen Sie eine Sicherheitsgruppe für die öffentliche Sicherheitsgruppe. Wählen Sie **Create Security Group** und geben Sie einen Namen und eine Beschreibung für die Gruppe ein. Wählen Sie unter "VPC"die VPC aus, die Sie zuvor erstellt haben. Wählen Sie **Yes, Create**.

Öffentliche Sicherheitsgruppe konfigurieren

1. Wählen Sie in der Liste der Sicherheitsgruppen die private Sicherheitsgruppe aus.
2. Wählen Sie die Registerkarte **Inbound Rules** und dann **Edit**, um die folgenden Regeln zu erstellen:

Typ	Quelle
ALL Traffic	Wählen Sie die private Sicherheitsgruppe.
ALL Traffic	Wählen Sie die öffentliche Sicherheitsgruppe.
ICMP	0.0.0.0/0
22 (SSH)	0.0.0.0/0
80 (HTTP)	0.0.0.0/0
443 (HTTPS)	0.0.0.0/0
1494 (ICA/HDX)	0.0.0.0/0
2598 (Sitzungszuverlässigkeit)	0.0.0.0/0
3389 (RDP)	0.0.0.0/0

3. Wenn Sie fertig sind, wählen Sie **Save**.
4. Wählen Sie die Registerkarte **Inbound Rules** und dann **Edit**, um die folgenden Regeln zu erstellen:

Typ	Ziel
ALL Traffic	Wählen Sie die private Sicherheitsgruppe.
ALL Traffic	0.0.0.0/0
ICMP	0.0.0.0/0

5. Wenn Sie fertig sind, wählen Sie **Save**.

Private Sicherheitsgruppe konfigurieren

1. Wählen Sie in der Liste der Sicherheitsgruppen die private Sicherheitsgruppe aus.
2. Wenn Sie keinen Datenverkehr von der öffentlichen Sicherheitsgruppe eingerichtet haben, müssen Sie TCP-Ports festlegen. Wählen Sie die Registerkarte **Inbound Rules** und dann **Edit** aus, um die folgenden Regeln zu erstellen:

Typ	Quelle
ALL Traffic	Wählen Sie die private Sicherheitsgruppe.
ALL Traffic	Wählen Sie die öffentliche Sicherheitsgruppe.
ICMP	Wählen Sie die öffentliche Sicherheitsgruppe.
TCP 53 (DNS)	Wählen Sie die öffentliche Sicherheitsgruppe.
UDP 53 (DNS)	Wählen Sie die öffentliche Sicherheitsgruppe.
80 (HTTP)	Wählen Sie die öffentliche Sicherheitsgruppe.
TCP 135	Wählen Sie die öffentliche Sicherheitsgruppe.
TCP 389	Wählen Sie die öffentliche Sicherheitsgruppe.
UDP 389	Wählen Sie die öffentliche Sicherheitsgruppe.
443 (HTTPS)	Wählen Sie die öffentliche Sicherheitsgruppe.
TCP 1494 (ICA/HDX)	Wählen Sie die öffentliche Sicherheitsgruppe.
TCP 2598 (Sitzungszuverlässigkeit)	Wählen Sie die öffentliche Sicherheitsgruppe.
3389 (RDP)	Wählen Sie die öffentliche Sicherheitsgruppe.
TCP 49152–65535	Wählen Sie die öffentliche Sicherheitsgruppe.

3. Wenn Sie fertig sind, wählen Sie **Save**.
4. Wählen Sie die Registerkarte **Inbound Rules** und dann **Edit**, um die folgenden Regeln zu erstellen:

Typ	Ziel
ALL Traffic	Wählen Sie die private Sicherheitsgruppe.
ALL Traffic	0.0.0.0/0
ICMP	0.0.0.0/0
UDP 53 (DNS)	0.0.0.0/0

5. Wenn Sie fertig sind, wählen Sie **Save**.

Aufgabe 3: Starten von Instanzen

Führen Sie die folgenden Schritte aus, um zwei EC2-Instanzen zu erstellen und das von Amazon generierte Standardadministratorkennwort zu entschlüsseln:

1. Wählen Sie in der AWS-Verwaltungskonsole **EC2**.
2. Wählen Sie im EC2-Dashboard **Launch Instance**.
3. Wählen Sie ein Windows Server-Maschinenimage und einen Instanztyp.
4. Geben Sie auf der Seite **Configure Instance Details** einen Namen für die Instanz ein und wählen Sie die zuvor eingerichtete VPC aus.
5. Treffen Sie unter **Subnet** für jede Instanz folgende Auswahl:
   - Bastion host: Wählen Sie das öffentliche Subnetz
   - Domain Controller: Wählen Sie das private Subnetz
6. Treffen Sie unter **Auto-assign Public IP address** für jede Instanz folgende Auswahl:
   - Bastion host: Wählen Sie **Enable**.
   - Domain Controller: Wählen Sie **Use default setting** oder **Disable**.
7. Geben Sie für **Network Interfaces** eine primäre IP-Adresse innerhalb des IP-Bereichs des privaten Subnetzes für den Domänencontroller ein.
8. Ändern Sie auf der Seite **Add Storage** bei Bedarf die Datenträgergröße.
9. Geben Sie auf der Seite **Tag Instance** einen Anzeigenamen für jede Instanz ein.
10. Wählen Sie auf der Seite **Configure Security Groups** die Option **Select an existing security group** und treffen Sie dann für jede Instanz die folgende Auswahl:
    - Bastion host: Wählen Sie die öffentliche Sicherheitsgruppe.
    - Domain Controller: Wählen Sie die private Sicherheitsgruppe aus.
11. Überprüfen Sie Ihre Auswahl und wählen Sie **Launch**.
12. Erstellen Sie ein neues Schlüsselpaar oder wählen Sie ein vorhandenes aus. Wenn Sie ein neues Schlüsselpaar erstellen, laden Sie die private Schlüsseldatei (.pem) herunter und bewahren Sie sie an einem sicheren Ort auf. Sie müssen den privaten Schlüssel angeben, wenn Sie das Standardadministratorkennwort für die Instanz beschaffen.
13. Wählen Sie **Launch Instances**. Wählen Sie **View Instances**, um eine Liste Ihrer Instanzen anzuzeigen. Warten Sie, bis die neu gestartete Instanz alle Statusprüfungen bestanden hat, bevor Sie darauf zugreifen.
14. Beschaffen Sie das Standardadministratorkennwort für jede Instanz:
    a) Wählen Sie die Instanz aus der Liste aus und wählen Sie **Connect**.
    b) Gehen Sie zur Registerkarte **RDP client**, wählen Sie **Get Password** und laden Sie Ihre private Schlüsseldatei (`.pem`) hoch, wenn Sie dazu aufgefordert werden.
    c) Wählen Sie **Decrypt Password**, um das menschenlesbare Kennwort zu erhalten. AWS zeigt das Standardkennwort an.

15. Wiederholen Sie die Schritte ab Schritt 2, bis Sie zwei Instanzen erstellt haben:

    - Eine Bastionshostinstanz in Ihrem öffentlichen Subnetz
    - Eine Instanz in Ihrem privaten Subnetz, die als Domänencontroller verwendet werden soll.

Aufgabe 4: Erstellen eines DHCP-Optionssatzes

1. Wählen Sie im VPC-Dashboard **DHCP Options Sets**.
2. Geben Sie die folgenden Informationen ein:

    - Name tag: Geben Sie einen Anzeigenamen für den Satz ein.
    - Domain name: Geben Sie den vollqualifizierten Domänennamen ein, den Sie beim Konfigurieren der Domänencontrollerinstanz verwenden möchten.
    - Domain name servers: Geben Sie die private IP-Adresse, die Sie der Domänencontrollerinstanz zugewiesen haben, und die Zeichenfolge **AmazonProvidedDNS** getrennt durch Kommas ein.
    - NTP servers: Lassen Sie dieses Feld leer.
    - NetBIOS name servers: Geben Sie die private IP-Adresse der Domänencontrollerinstanz ein.
    - NetBIOS node type: Geben Sie **2** ein.

3. Wählen Sie **Yes, Create**.
4. Verknüpfen des neuen Satzes mit der VPC:

    a) Wählen Sie im VPC-Dashboard **Your VPCs** und dann die VPC, die Sie zuvor eingerichtet haben.
    b) Wählen Sie **Actions > Edit DHCP Options Set**.
    c) Wenn Sie dazu aufgefordert werden, wählen Sie den neuen Satz, den Sie erstellt haben, und wählen Sie **Save**.

Aufgabe 5: Konfigurieren der Instanzen

1. Stellen Sie mit einem RDP-Clients eine Verbindung mit der öffentlichen IP-Adresse der Bastionhostinstanz her. Geben Sie die Anmeldeinformationen für das Administratorkonto ein, wenn Sie dazu aufgefordert werden.
2. Starten Sie Remote Desktop Connection auf der Bastionshostinstanz und stellen Sie eine Verbindung zur privaten IP-Adresse der Instanz her, die Sie konfigurieren möchten. Geben Sie die Anmeldeinformationen für die Instanz ein, wenn Sie dazu aufgefordert werden.
3. Konfigurieren Sie für alle Instanzen im privaten Subnetz folgende DNS-Einstellungen:

a) Wählen Sie **Start > Control Panel > Network and Internet > Network and Sharing Center > Change adapter settings**. Doppelklicken Sie auf die angezeigte Netzwerkverbindung.

b) Wählen Sie **Properties > Internet Protocol Version 4 (TCP/IPv4) > Properties**.

c) Wählen Sie **Advanced > DNS**. Vergewissern Sie sich, dass die folgenden Einstellungen aktiviert sind, und wählen Sie **OK**:

- Register this connection's addresses in DNS
- Use this connection's DNS suffix in DNS registration

4. Konfigurieren des Domänencontrollers:

a) Fügen Sie mit Server-Manager die Active Directory-Domänendiensterolle mit allen Standardfeatures hinzu.

b) Stufen Sie die Instanz auf einen Domänencontroller hoch. Aktivieren Sie im Rahmen der Heraufstufung DNS und verwenden Sie den Domänennamen, den Sie beim Erstellen des DHCP-Optionssatzes festgelegt haben. Starten Sie die Instanz neu, wenn Sie dazu aufgefordert werden.

So geht es weiter

- Kernkomponenten installieren
- VDAs installieren
- Site erstellen
- Informationen zum Erstellen und Verwalten einer Verbindung in AWS finden Sie unter Verbindung zu AWS.

Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Maschinenkataloge erstellen

XenServer-Virtualisierungsumgebungen

June 27, 2024

XenServer vereinfacht Ihr Betriebsmanagement und gewährleistet ein hochauflösendes Benutzererlebnis für intensive Workloads.

Informationen zum Einrichten von XenServer finden Sie unter Installation vorbereiten.

So geht es weiter

- Kernkomponenten installieren
- VDAs installieren
- Site erstellen
- Weitere Informationen zum Erstellen und Verwalten einer Verbindung in XenServer finden Sie unter Verbindung zu XenServer

Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Maschinenkataloge erstellen

Google Cloud-Umgebungen

June 27, 2024

Citrix Virtual Apps and Desktops ermöglicht das Provisioning und Verwalten von Maschinen in Google Cloud.

Anforderungen

- Citrix Cloud-Konto. Das in diesem Artikel beschriebene Feature ist nur in Citrix Cloud verfügbar.
- Ein Google Cloud-Projekt. Das Projekt umfasst alle Rechenressourcen, die dem Maschinenkatalog zugeordnet sind. Dies kann ein bestehendes oder ein neues Projekt sein.
- Aktivieren Sie vier APIs in Ihrem Google Cloud-Projekt. Weitere Informationen finden Sie im Abschnitt Aktivieren von Google Cloud-APIs.
- Google Cloud-Dienstkonto. Das Dienstkonto dient zur Authentifizierung bei Google Cloud, um Zugriff auf das Projekt zu erhalten. Weitere Informationen finden Sie unter Dienstkonten konfigurieren und aktualisieren.
- Aktivieren des privaten Google-Zugriffs Einzelheiten finden Sie unter Enable-private-google-access.

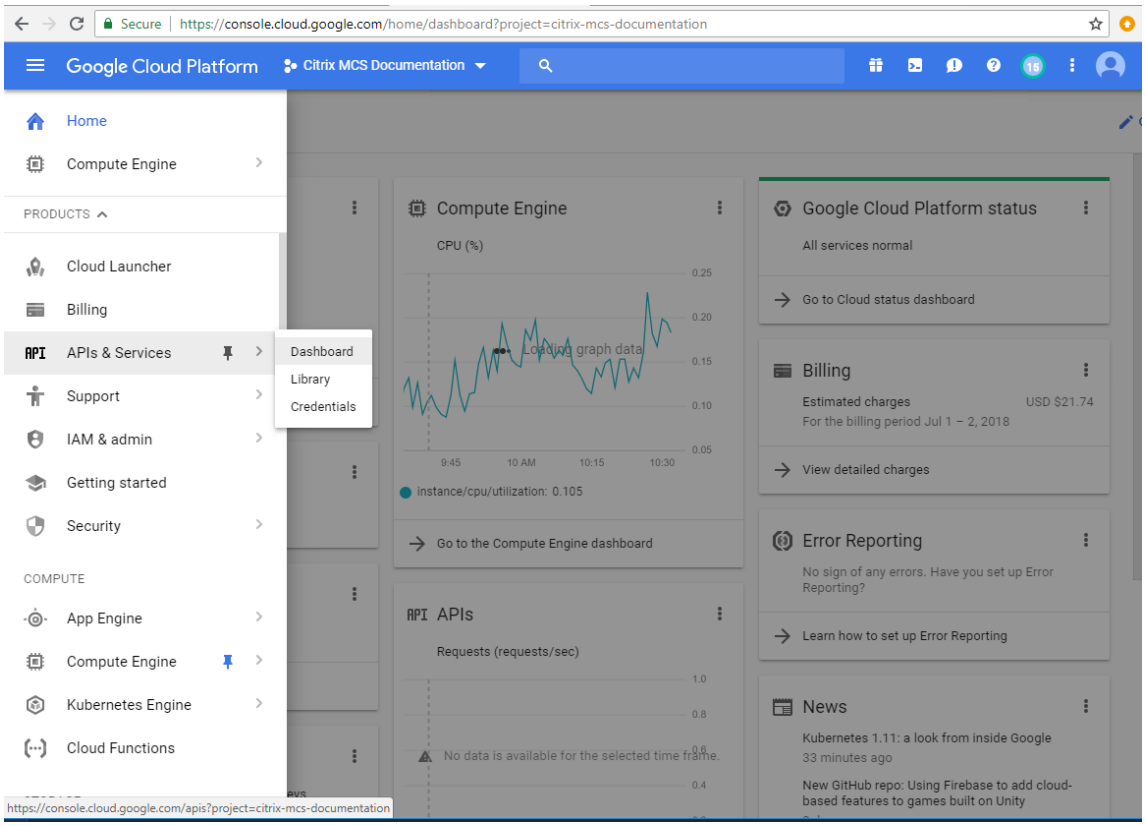
Aktivieren von Google Cloud-APIs

Um die Google Cloud-Funktionalität mit Web Studio zu verwenden, müssen Sie diese APIs in Ihrem Google Cloud-Projekt aktivieren:

- Compute Engine-API
- Cloud Resource Manager-API
- Identitäts- und Zugriffsverwaltung (IAM)-API
- Cloud Build-API
- Cloud-Schlüsselverwaltungsdienst (KMS)

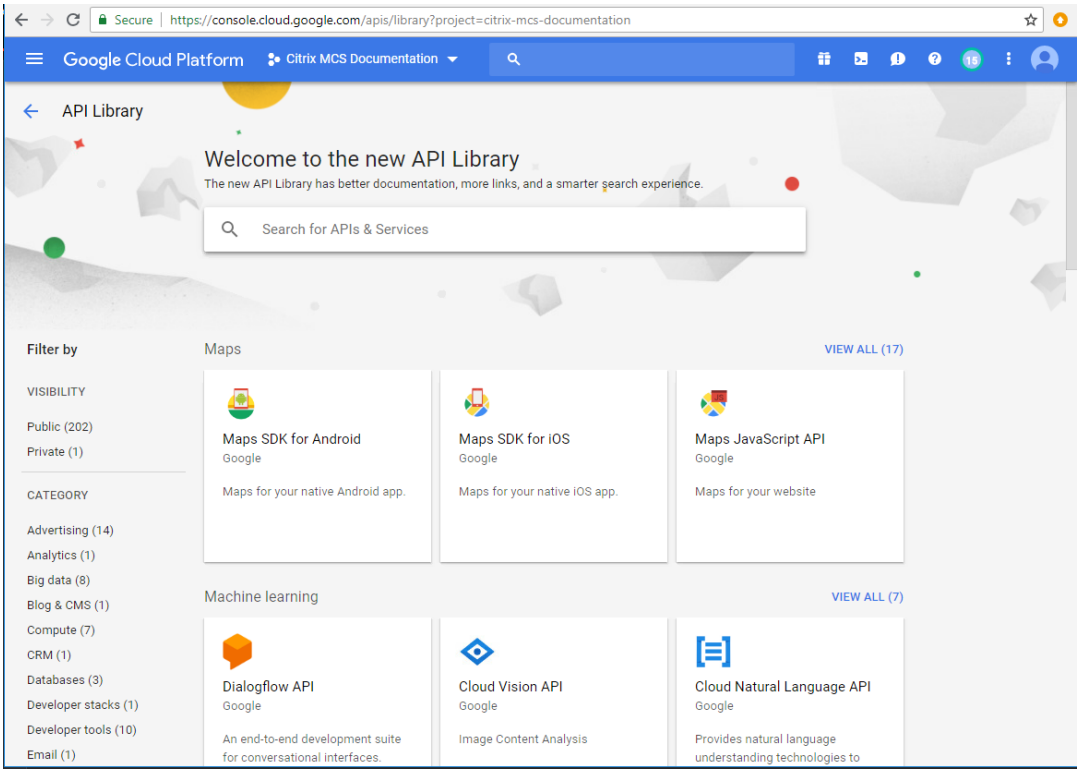
Führen Sie in der Google Cloud-Konsole die folgenden Schritte aus:

1. Wählen Sie im oberen linken Menü **APIs and Services > Dashboard**.



2. Stellen Sie im **Dashboard**-Bildschirm sicher, dass die Compute Engine-API aktiviert ist. Wenn nicht, führen Sie folgende Schritte aus:

   a) Gehen Sie zu **APIs & Services > Library**.



b) Geben Sie im Suchfeld den Begriff *Compute Engine* ein.

c) Wählen Sie in den Suchergebnissen **Compute Engine API**.

d) Wählen Sie **Enable** auf der Seite **Compute Engine API**.

3. Aktivieren Sie die Cloud Resource Manager-API.

   a) Gehen Sie zu **APIs & Services > Library**.

   b) Geben Sie im Suchfeld den Begriff *Cloud Resource Manager* ein.

   c) Wählen Sie in den Suchergebnissen **Cloud Resource Manager API**.

   d) Wählen Sie **Enable** auf der Seite **Cloud Resource Manager-API**. Der Status der API wird angezeigt.

4. Aktivieren Sie auch **IAM-API** und **Cloud Build-API** auf diese Weise.

Sie können die APIs auch mit Google Cloud Shell aktivieren. Gehen Sie hierzu folgendermaßen vor:

1. Öffnen Sie die Google-Konsole und laden Sie die Cloud Shell.
2. Führen Sie in der Cloud Shell folgende vier Befehle aus:

   - gcloud services enable compute.googleapis.com
   - gcloud services enable cloudresourcemanager.googleapis.com
   - gcloud services enable iam.googleapis.com

- gcloud services enable cloudbuild.googleapis.com

3. Klicken Sie auf **Authorize**, wenn Sie die Cloud Shell dazu auffordert.

Dienstkonten konfigurieren und aktualisieren

> **Hinweis:**
>
> Ab dem 29. April 2024 führt GCP Änderungen am Standardverhalten von Cloud Build Services und der Verwendung von Dienstkonten ein. Weitere Informationen finden Sie unter Änderungen des Cloud Build-Dienstkontos. Ihre bestehenden Google-Projekte mit aktivierter Cloud Build API vor dem 29. April 2024 sind von dieser Änderung nicht betroffen. Wenn Sie jedoch das bestehende Cloud Build Service-Verhalten nach dem 29. April beibehalten möchten, können Sie die Organisationsrichtlinie erstellen oder anwenden, um die Durchsetzung der Einschränkungen zu deaktivieren, bevor Sie die Cloud Build API aktivieren. Daher ist der folgende Inhalt zweigeteilt: Vor dem 29. April 2024 und Nach dem 29. April 2024. Wenn Sie die neue Organisationsrichtlinie festlegen, folgen Sie dem Abschnitt Vor dem 29. April 2024.

Vor dem 29. April 2024

Citrix Cloud verwendet drei separate Dienstkonten im Google Cloud-Projekt:

- *Citrix Cloud-Dienstkonto:* Dieses Dienstkonto ermöglicht Citrix Cloud den Zugriff auf das Google-Projekt, sowie Provisioning und Verwaltung von Maschinen. Dieses Dienstkonto authentifiziert sich bei Google Cloud mit einem von Google Cloud generierten Schlüssels.

  Sie müssen dieses Dienstkonto manuell erstellen, wie hier beschrieben. Weitere Informationen finden Sie unter Citrix Cloud-Dienstkonto erstellen.

  Sie können dieses Dienstkonto mit einer E-Mail-Adresse identifizieren. Beispiel: `<my-service-account>@<project-id>.iam.gserviceaccount.com`.

- *Cloud Build-Dienstkonto:* Dieses Dienstkonto wird automatisch bereitgestellt, nachdem Sie alle unter Enable Google Cloud APIs aufgeführten APIs aktiviert haben. Um alle automatisch erstellten Dienstkonten anzuzeigen, navigieren Sie in der **Google Cloud**-Konsole zu **IAM & Admin > IAM** und aktivieren Sie das Kontrollkästchen **Include Google-provided role grants**.

  Sie können dieses Dienstkonto durch eine E-Mail-Adresse identifizieren, die mit der **Projekt-ID** und dem Wort **cloudbuild** beginnt. Beispiel:`<project-id>@cloudbuild.gserviceaccount.com`

  Überprüfen Sie, ob dem Dienstkonto die folgenden Rollen gewährt wurden. Wenn Sie Rollen hinzufügen müssen, folgen Sie den Schritten unter Cloud Build-Dienstkonto Rollen hinzufügen.

  - Cloud Build-Dienstkonto

  - Compute Instance-Administrator
  - Dienstkontobenutzer

- *Cloud Compute-Dienstkonto*: Dieses Dienstkonto wird von Google Cloud zu Instanzen hinzugefügt, die in Google Cloud erstellt wurden, sobald die Compute-API aktiviert wird. Dieses Konto hat die einfache IAM-Bearbeiterrolle, um die Operationen auszuführen. Wenn Sie jedoch die Standardberechtigung löschen, um eine präzisere Kontrolle zu haben, müssen Sie die **Speicheradministratorrolle** hinzufügen, für die die folgenden Berechtigungen erforderlich sind:

  - resourcemanager.projects.get
  - storage.objects.create
  - storage.objects.get
  - storage.objects.list

Sie können dieses Dienstkonto durch eine E-Mail-Adresse identifizieren, die mit der **Projekt-ID** und dem Wort **compute** beginnt. Beispiel: `<project-id>-compute@developer.gserviceaccount.com`.

Citrix Cloud-Dienstkonto erstellen Führen Sie folgende Schritte aus, um ein Citrix Cloud-Dienstkonto zu erstellen:

1. Gehen Sie in der Google Cloud-Konsole zu **IAM & Admin > Service accounts**.
2. Wählen Sie auf der Seite **Service accounts CREATE SERVICE ACCOUNT**.
3. Geben Sie auf der Seite **Create service account** die erforderlichen Informationen ein und wählen Sie dann **CREATE AND CONTINUE**.
4. Klicken Sie auf der Seite **Grant this service account access to project** auf das Dropdownmenü **Select a role** und wählen Sie die erforderlichen Rollen aus. Klicken Sie auf **+ADD ANOTHER ROLE**, wenn Sie weitere Rollen hinzufügen möchten.

   Jedes Konto (persönlich oder Service) hat verschiedene Rollen, die das Management des Projekts definieren. Gewähren Sie diesem Dienstkonto die folgenden Rollen:

   - Compute Admin
   - Speicher-Administrator
   - Cloud Build-Editor
   - Dienstkontobenutzer
   - Cloud Datastore User
   - Cloud KMS Crypto Operator

   Der Cloud KMS Crypto Operator benötigt die folgenden Berechtigungen:

   - cloudkms.cryptoKeys.get

- cloudkms.cryptoKeys.list
- cloudkms.keyRings.get
- cloudkms.keyRings.list

> **Hinweis:**
>
> Aktivieren Sie alle APIs, um die vollständige Liste der beim Erstellen eines neuen Dienstkontos verfügbaren Rollen abzurufen.

5. Klicken Sie auf **CONTINUE**
6. Fügen Sie auf der Seite **Grant users access to this service account** Benutzer oder Gruppen hinzu, um ihnen Zugriff auf Aktionen in diesem Dienstkonto zu gewähren.
7. Klicken Sie auf **DONE**.
8. Navigieren Sie zur IAM-Hauptkonsole.
9. Identifizieren Sie das erstellte Dienstkonto.
10. Überprüfen Sie, ob die Rollen erfolgreich zugewiesen wurden.

Überlegungen:

Beachten Sie beim Erstellen des Servicekontos Folgendes:

- Die Schritte **Grant this service account access to project** und **Grant users access to this service account** sind optional. Wenn Sie diese optionalen Konfigurationsschritte überspringen, wird das neu erstellte Servicekonto nicht auf der Seite **IAM & Admin > IAM** angezeigt.
- Um die mit dem Servicekonto verknüpften Rollen anzuzeigen, fügen Sie die Rollen hinzu, ohne die optionalen Schritte zu überspringen. Dadurch wird sichergestellt, dass Rollen für das konfigurierte Servicekonto angezeigt werden.

Citrix Cloud-Dienstkontoschlüssel Der Citrix Cloud-Dienstkontoschlüssel ist erforderlich, um eine Verbindung in Citrix DaaS herzustellen. Der Schlüssel ist in einer Anmeldeinformationsdatei (.json) enthalten. Nachdem Sie den Schlüssel erstellt haben, wird die Datei automatisch heruntergeladen und im Ordner **Downloads** gespeichert. Stellen Sie beim Erstellen des Schlüssels sicher, dass der Schlüsseltyp auf JSON festgelegt wird. Andernfalls kann die Citrix Oberfläche "Vollständige Konfiguration" sie nicht analysieren.

Um einen Dienstkontoschlüssel zu erstellen, navigieren Sie zu **IAM & Admin > Dienstkonten** und klicken Sie auf die E-Mail-Adresse des Citrix Cloud-Dienstkontos. Wechseln Sie zur Registerkarte **Schlüssel** und wählen Sie **Schlüssel hinzufügen > Neuen Schlüssel erstellen**. Achten Sie darauf, **JSON** als Schlüsseltyp auszuwählen.

> **Tipp:**
>
> Erstellen Sie Schlüssel auf der Seite **Service accounts** in der Google Cloud-Konsole. Es wird empfohlen, Schlüssel aus Sicherheitsgründen regelmäßig zu ändern. Sie stellen der Citrix Virtual Apps and Desktops-Anwendung neue Schlüssel durch Bearbeiten einer vorhandenen Google Cloud-Verbindung bereit.

Citrix Cloud-Dienstkonto Rollen hinzufügen So fügen Sie einem Citrix Cloud-Dienstkonto Rollen hinzu:

1. Gehen Sie in der Google Cloud-Konsole zu **IAM & Admin > IAM**.
2. Suchen Sie auf der Seite **IAM > PERMISSIONS** das erstellte Dienstkonto, erkennbar an der E-Mail-Adresse.

   Beispiel:`<my-service-account>@<project-id>.iam.gserviceaccount.com`
3. Wählen Sie das Bleistiftsymbol, um den Zugriff auf den Prinzipal des Dienstkontos zu bearbeiten.
4. Wählen Sie auf der Seite **Edit access to "project-id"** für den ausgewählten Prinzipal **ADD ANOTHER ROLE**, um Ihrem Dienstkonto die erforderlichen Rollen nacheinander hinzuzufügen, und wählen Sie **SAVE**.

Cloud Build-Dienstkonto Rollen hinzufügen So fügen Sie einem Cloud Build-Dienstkonto Rollen hinzu:

1. Gehen Sie in der Google Cloud-Konsole zu **IAM & Admin > IAM**.
2. Suchen Sie auf der Seite **IAM** das Cloud Build-Dienstkonto, erkennbar an einer E-Mail-Adresse, die mit der **Projekt-ID** und dem Wort **cloudbuild** beginnt.

   Beispiel:`<project-id>@cloudbuild.gserviceaccount.com`
3. Wählen Sie das Bleistiftsymbol, um die Cloud Build-Kontorollen zu bearbeiten.
4. Wählen Sie auf der Seite **Edit access to "project-id"** für den ausgewählten Prinzipal **ADD ANOTHER ROLE**, um Ihrem Cloud Build-Dienstkonto die erforderlichen Rollen nacheinander hinzuzufügen, und wählen Sie **SAVE**.

   > **Hinweis:**
   >
   > Aktivieren Sie alle APIs, um die vollständige Liste der Rollen abzurufen.

Nach dem 29. April 2024

Citrix Cloud verwendet zwei separate Dienstkonten im Google Cloud-Projekt:

- *Citrix Cloud-Dienstkonto:* Dieses Dienstkonto ermöglicht Citrix Cloud den Zugriff auf das Google-Projekt, sowie Provisioning und Verwaltung von Maschinen. Dieses Dienstkonto authentifiziert sich bei Google Cloud mit einem von Google Cloud generierten Schlüssels.

  Sie müssen dieses Dienstkonto manuell erstellen.

  Sie können dieses Dienstkonto mit einer E-Mail-Adresse identifizieren. Beispiel: `<my-service-account>@<project-id>.iam.gserviceaccount.com`.

- *Cloud Compute-Dienstkonto*: Dieses Dienstkonto wird automatisch bereitgestellt, nachdem Sie alle unter Enable Google Cloud APIs aufgeführten APIs aktiviert haben. Um alle automatisch erstellten Dienstkonten anzuzeigen, navigieren Sie in der **Google Cloud**-Konsole zu **IAM & Admin > IAM** und aktivieren Sie das Kontrollkästchen **Include Google-provided role grants**. Dieses Konto hat die einfache IAM-Bearbeiterrolle, um die Operationen auszuführen. Wenn Sie jedoch die Standardberechtigung löschen, um eine präzisere Kontrolle zu haben, müssen Sie die **Speicheradministratorrolle** hinzufügen, für die die folgenden Berechtigungen erforderlich sind:

  - resourcemanager.projects.get
  - storage.objects.create
  - storage.objects.get
  - storage.objects.list

  Sie können dieses Dienstkonto durch eine E-Mail-Adresse identifizieren, die mit der **Projekt-ID** und dem Wort **compute** beginnt. Beispiel:`<project-id>-compute@developer.gserviceaccount.com`.

  Überprüfen Sie, ob dem Dienstkonto die folgenden Rollen gewährt wurden.

  - Cloud Build-Dienstkonto
  - Compute Instance-Administrator
  - Dienstkontobenutzer

Citrix Cloud-Dienstkonto erstellen Führen Sie folgende Schritte aus, um ein Citrix Cloud-Dienstkonto zu erstellen:

1. Gehen Sie in der Google Cloud-Konsole zu **IAM & Admin > Service accounts**.
2. Wählen Sie auf der Seite **Service accounts CREATE SERVICE ACCOUNT**.
3. Geben Sie auf der Seite **Create service account** die erforderlichen Informationen ein und wählen Sie dann **CREATE AND CONTINUE**.

4. Klicken Sie auf der Seite **Grant this service account access to project** auf das Dropdownmenü **Select a role** und wählen Sie die erforderlichen Rollen aus. Klicken Sie auf **+ADD ANOTHER ROLE**, wenn Sie weitere Rollen hinzufügen möchten.

   Jedes Konto (persönlich oder Service) hat verschiedene Rollen, die das Management des Projekts definieren. Gewähren Sie diesem Dienstkonto die folgenden Rollen:

   - Compute Admin
   - Speicher-Administrator
   - Cloud Build-Editor
   - Dienstkontobenutzer
   - Cloud Datastore User
   - Cloud KMS Crypto Operator

   Der Cloud KMS Crypto Operator benötigt die folgenden Berechtigungen:

   - cloudkms.cryptoKeys.get
   - cloudkms.cryptoKeys.list
   - cloudkms.keyRings.get
   - cloudkms.keyRings.list

   > **Hinweis:**
   >
   > Aktivieren Sie alle APIs, um die vollständige Liste der beim Erstellen eines neuen Dienstkontos verfügbaren Rollen abzurufen.

5. Klicken Sie auf **CONTINUE**
6. Fügen Sie auf der Seite **Grant users access to this service account** Benutzer oder Gruppen hinzu, um ihnen Zugriff auf Aktionen in diesem Dienstkonto zu gewähren.
7. Klicken Sie auf **DONE**.
8. Navigieren Sie zur IAM-Hauptkonsole.
9. Identifizieren Sie das erstellte Dienstkonto.
10. Überprüfen Sie, ob die Rollen erfolgreich zugewiesen wurden.

Überlegungen:

Beachten Sie beim Erstellen des Servicekontos Folgendes:

- Die Schritte **Grant this service account access to project** und **Grant users access to this service account** sind optional. Wenn Sie diese optionalen Konfigurationsschritte überspringen, wird das neu erstellte Servicekonto nicht auf der Seite **IAM & Admin > IAM** angezeigt.
- Um die mit dem Servicekonto verknüpften Rollen anzuzeigen, fügen Sie die Rollen hinzu, ohne die optionalen Schritte zu überspringen. Dadurch wird sichergestellt, dass Rollen für das konfigurierte Servicekonto angezeigt werden.

Citrix Cloud-Dienstkontoschlüssel Der Citrix Cloud-Dienstkontoschlüssel ist erforderlich, um eine Verbindung in Citrix DaaS herzustellen. Der Schlüssel ist in einer Anmeldeinformationsdatei (.json) enthalten. Nachdem Sie den Schlüssel erstellt haben, wird die Datei automatisch heruntergeladen und im Ordner **Downloads** gespeichert. Stellen Sie beim Erstellen des Schlüssels sicher, dass der Schlüsseltyp auf JSON festgelegt wird. Andernfalls kann die Citrix Oberfläche "Vollständige Konfiguration" sie nicht analysieren.

Um einen Dienstkontoschlüssel zu erstellen, navigieren Sie zu **IAM & Admin > Dienstkonten** und klicken Sie auf die E-Mail-Adresse des Citrix Cloud-Dienstkontos. Wechseln Sie zur Registerkarte **Schlüssel** und wählen Sie **Schlüssel hinzufügen > Neuen Schlüssel erstellen**. Achten Sie darauf, **JSON** als Schlüsseltyp auszuwählen.

> **Tipp:**
>
> Erstellen Sie Schlüssel auf der Seite **Service accounts** in der Google Cloud-Konsole. Es wird empfohlen, Schlüssel aus Sicherheitsgründen regelmäßig zu ändern. Sie stellen der Citrix Virtual Apps and Desktops-Anwendung neue Schlüssel durch Bearbeiten einer vorhandenen Google Cloud-Verbindung bereit.

Citrix Cloud-Dienstkonto Rollen hinzufügen So fügen Sie einem Citrix Cloud-Dienstkonto Rollen hinzu:

1. Gehen Sie in der Google Cloud-Konsole zu **IAM & Admin > IAM**.
2. Suchen Sie auf der Seite **IAM > PERMISSIONS** das erstellte Dienstkonto, erkennbar an der E-Mail-Adresse.

   Beispiel:`<my-service-account>@<project-id>.iam.gserviceaccount.com`
3. Wählen Sie das Bleistiftsymbol, um den Zugriff auf den Prinzipal des Dienstkontos zu bearbeiten.
4. Wählen Sie auf der Seite **Edit access to "project-id"** für den ausgewählten Prinzipal **ADD ANOTHER ROLE**, um Ihrem Dienstkonto die erforderlichen Rollen nacheinander hinzuzufügen, und wählen Sie **SAVE**.

Rollen zum Cloud Compute-Dienstkonto hinzufügen So fügen Sie Rollen zum Cloud Compute-Dienstkonto hinzu:

1. Gehen Sie in der Google Cloud-Konsole zu **IAM & Admin > IAM**.
2. Suchen Sie auf der Seite **IAM** das Cloud Build-Dienstkonto, erkennbar an einer E-Mail-Adresse, die mit der **Projekt-ID** und dem Wort **compute** beginnt.

   Beispiel:`<project-id>-compute@developer.gserviceaccount.com`

3. Wählen Sie das Bleistiftsymbol, um die Cloud Build-Kontorollen zu bearbeiten.
4. Wählen Sie auf der Seite **Edit access to "project-id"** für den ausgewählten Prinzipal **ADD ANOTHER ROLE**, um Ihrem Cloud Build-Dienstkonto die erforderlichen Rollen nacheinander hinzuzufügen, und wählen Sie **SAVE**.

   > **Hinweis:**
   >
   > Aktivieren Sie alle APIs, um die vollständige Liste der Rollen abzurufen.

Speicherberechtigungen und Bucket-Verwaltung

Citrix Virtual Apps and Desktops verbessert die Meldung von Cloud Build-Fehlern für den Google Cloud-Dienst. Der Dienst führt Builds in Google Cloud aus. Citrix Virtual Apps and Desktops erstellt ein Speicher-Bucket unter dem Namen `citrix-mcs-cloud-build-logs-{ region } -{ 5 random characters }`, in dem die Google Cloud-Dienste Build-Protokollinformationen erfassen. Für das Bucket ist festgelegt, dass dessen Inhalt nach 30 Tagen gelöscht wird. Für diesen Vorgang muss die Google Cloud-Berechtigung des für die Verbindung verwendeten Dienstkontos auf `storage.buckets.update` festgelegt sein. Hat das Dienstkonto diese Berechtigung nicht, ignoriert Citrix Virtual Apps and Desktops Fehler und setzt die Katalogerstellung fort. Ohne diese Berechtigung werden Build-Protokolle immer größer und erfordern eine manuelle Bereinigung.

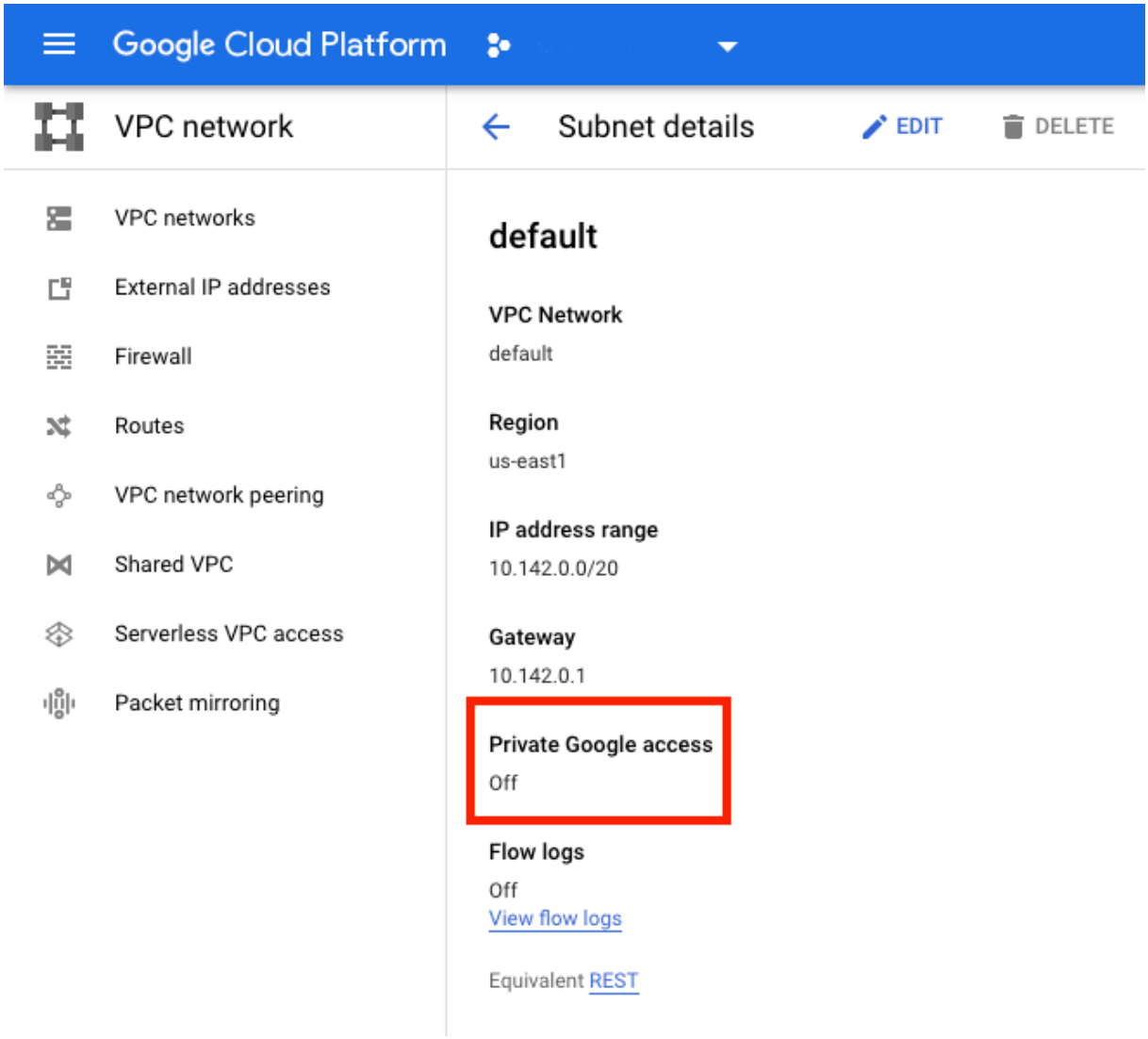
Aktivieren des privaten Google-Zugriffs

Wenn der Netzwerkschnittstelle einer VM keine externe IP-Adresse zugewiesen ist, werden Pakete nur an andere interne IP-Adressenziele gesendet. Wenn Sie den privaten Zugriff aktivieren, stellt die VM eine Verbindung zu den von der Google-API und den zugehörigen Diensten verwendeten externen IP-Adressen her.

> **Hinweis:**
>
> Unabhängig davon, ob der private Google-Zugriff aktiviert ist, müssen alle VMs mit und ohne öffentliche IP-Adresse auf öffentliche Google-APIs zugreifen können, vor allem dann, wenn Netzwerkgeräte von Drittanbietern in der Umgebung installiert sind.

Damit eine VM im Subnetz ohne öffentliche IP-Adresse für das MCS-Provisioning auf die Google-APIs zugreifen kann, führen Sie folgende Schritte aus:

1. Rufen Sie in Google Cloud **VPC network configuration** auf.
2. Aktivieren Sie im Fenster "Subnet details"die Option **Private Google access**.



Weitere Informationen finden Sie unter Konfigurieren des privaten Google-Zugriffs.

> **Wichtig:**
>
> Wenn Ihr Netzwerk so konfiguriert ist, dass der VM-Zugriff auf das Internet unterbunden wird, vergewissern Sie sich, dass Ihre Organisation das mit der Aktivierung des privaten Google-Zugriffs für das Subnetz der VMs verbundene Risiko einzugehen bereit ist.

So geht es weiter

- Kernkomponenten installieren
- VDAs installieren
- Site erstellen
- Informationen zum Erstellen und Verwalten einer Verbindung in Google Cloud-Umgebungen finden Sie unter Verbindung zu Google-Cloudumgebungen.

Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Maschinenkataloge erstellen

HPE Moonshot-Virtualisierungsumgebungen

June 27, 2024

Citrix Virtual Apps and Desktops verwaltet Ihre HPE Moonshot-Workloads über ein vorhandenes, von Citrix verwaltetes HPE Moonshot-Plug-In. Mit diesem Plug-In können Sie Verbindungen zu Ihrem HPE Moonshot Chassis herstellen, Kataloge erstellen und die Energieverwaltung von Maschinen im Katalog steuern.

Voraussetzung

Installieren Sie das von Citrix verwaltete HPE Moonshot Plug-In auf dem Delivery Controller.

> **Hinweis:**
>
> - Wenn sowohl von Citrix verwaltete als auch von HPE verwaltete HPE Moonshot Plug-Ins installiert sind, verwendet der Delivery Controller das von Citrix verwaltete HPE Moonshot Plug-In.
> - Wenn sowohl das von Citrix verwaltete als auch das von HPE verwaltete HPE Moonshot Plug-In installiert sind und Sie das HPE Managed Moonshot Plug-In verwenden möchten, deinstallieren Sie das von Citrix verwaltete HPE Moonshot Plug-In und aktualisieren Sie den `RegisterPlugin`-Cache.

Das von Citrix verwaltete HPE Moonshot Plug-In installieren

Gehen Sie wie folgt vor, um das von Citrix verwaltete HPE Moonshot Plug-In zu installieren:

1. Installieren Sie `E:\x64\Citrix Desktop Delivery Controller\MoonshotPlugin.msi`. `E:\` ist die ISO.
2. Öffnen Sie die PowerShell als Administrator und führen Sie den folgenden Befehl aus.

```
C:\Program Files\Common Files\Citrix\HCLPlugins> .\RegisterPlugins.exe -pluginsroot .\CitrixMachineCreation\v1.0.0.0\
<!--NeedCopy-->
```


3. Nachdem die Plug-In-Registrierung erfolgreich war, starten Sie die folgenden Dienste vom **Task-Manager** aus neu:

    a) CitrixBrokerService
    b) CitrixHostService
    c) CitrixMachineCreationService

4. Führen Sie `Get-HypHypervisorPlugins` aus, um zu überprüfen, ob das Plug-In auf dem Delivery Controller installiert ist. Das **DisplayName**-Feld in der Ausgabe muss als **HPE Moonshot** angezeigt werden.

Das von Citrix verwaltete HPE Moonshot Plug-In deinstallieren und den RegisterPlugin-Cache aktualisieren

Wenn sowohl das von Citrix verwaltete als auch das von HPE verwaltete HPE Moonshot Plug-In installiert sind und Sie das HPE Managed Moonshot Plug-In verwenden möchten, müssen Sie das von Citrix verwaltete HPE Moonshot Plug-In deinstallieren und den `RegisterPlugin`-Cache aktualisieren. Vorgehensweise:

1. Deinstallieren Sie das von Citrix verwaltete HPE Moonshot-Plug-In.
2. Öffnen Sie die PowerShell als Administrator und führen Sie den folgenden Befehl aus:

```
cd `C:\Program Files\Common Files\Citrix\HCLPlugins`
C:\Program Files\Common Files\Citrix\HCLPlugins> .\RegisterPlugins
    .exe -PluginsRoot ` C:\Program Files\Common Files\Citrix\
    HCLPlugins\ManagedMachine\v2.5.0.0`
<!--NeedCopy-->
```

3. Nachdem die Plug-In-Registrierung erfolgreich war, starten Sie die folgenden Dienste vom **Task-Manager** aus neu:

    a) CitrixBrokerService
    b) CitrixHostService
    c) CitrixMachineCreationService

4. Führen Sie `Get-HypHypervisorPlugins` aus, um zu überprüfen, ob das Plug-In auf dem Delivery Controller installiert ist. Das **DisplayName**-Feld in der Ausgabe muss als **HPE Moonshot Machine Manager** angezeigt werden.

Wichtige Schritte

1. Richten Sie Ihre HPE-Umgebungen ein.
2. Stellen Sie eine Verbindung zum HPE Moonshot Chassis her.

3. Erstellen Sie einen Maschinenkatalog.

> **Hinweis:**
>
> Stellen Sie vor dem Erstellen eines Katalogs sicher, dass Sie über einen oder mehrere HPE Moonshot Cartridge-Knoten verfügen, und installieren Sie VDAs auf diesen Knoten. Sie können das HPE Moonshot Chassis als Hypervisor und die Cartridge-Knoten als VMs betrachten.

4. Erstellen Sie eine Bereitstellungsgruppe.
5. Migrieren Sie die übrigen nicht verwalteten HPE Moonshot-Knoten in den verwalteten Katalog oder die Bereitstellungsgruppe.

So geht es weiter

- Kernkomponenten installieren
- VDAs installieren
- Site erstellen
- Informationen zum Erstellen und Verwalten einer Verbindung in HPE Moonshot finden Sie unter Verbindung zu HPE Moonshot

Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Maschinenkataloge erstellen

Microsoft Azure Resource Manager-Cloudumgebungen

June 27, 2024

Wenn Sie mit Microsoft Azure Resource Manager virtuelle Maschinen in Ihrer Citrix Virtual Apps and Desktops-Umgebung bereitstellen, sollten Sie mit Folgendem vertraut sein:

- Azure Active Directory: https://docs.microsoft.com/en-in/azure/active-directory/fundamentals/active-directory-whatis/
- Einverständniserklärung: https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/plan-an-application-integration
- Dienstprinzipal: https://docs.microsoft.com/en-us/azure/active-directory/develop/app-objects-and-service-principals/

Informationen zum Einrichten von Microsoft Azure Resource Manager finden Sie unter Installation vorbereiten.

So geht es weiter

- Kernkomponenten installieren
- VDAs installieren
- Site erstellen
- Informationen zum Erstellen und Verwalten einer Verbindung in Azure-Umgebungen finden Sie unter Verbindung zu Microsoft Azure.

Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- 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 Configuration Manager-Umgebungen

June 27, 2024

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:** Das Wake-On-LAN-Feature für den Remote-PC-Zugriff wird durch Configuration Manager unterstützt. Weitere Informationen finden Sie unter Wake-On-LAN —SCCM-integriert.
- **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 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)
`BrokerSiteName`	Gibt den gleichen Wert zurück wie `HostIdentifier`
`DesktopCatalogName`	Dem Desktop zugewiesener Maschinenkatalog
`DesktopGroupName`	Dem Desktop zugewiesene Bereitstellungsgruppe
`HostIdentifier`	Gibt den gleichen Wert zurück wie `BrokerSiteName`
`IsAssigned`	`True` = Desktop wird einem Benutzer zugewiesen; `False` = zufälliger Desktop
`IsMasterImage`	Ermöglicht Entscheidungen bezüglich der Umgebung. Installieren Sie beispielsweise Anwendungen auf dem Image und nicht auf den bereitgestellten Maschinen. Gültige Werte sind: `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

Eigenschaft	Beschreibung
`OSChangesPersist`	`False`, wenn das Betriebssystemimage des Desktops bei jedem Neustart in einen fehlerfreien Zustand versetzt wird, andernfalls **`true`**
`PersistentDataLocation`	Der Speicherort, an dem Configuration Manager persistente Daten speichert. Benutzer haben hierauf keinen Zugriff.
`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 Leerzeichen oder weichen vom Eigenschaftsnamen geringfügig ab. `BrokerSiteName` wird zum Beispiel als `Broker Site Name` angezeigt.

- 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 Microsoft-Dokumentation.

Microsoft System Center Virtual Machine Manager-Virtualisierungsumgebungen

June 27, 2024

Folgen Sie den 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.

> **Hinweis:**
>
> Hyper-V-Cluster mit verschiedenen Hyper-V-Versionen werden nicht unterstützt.

Verwenden Sie Citrix Provisioning (zuvor "Provisioning Services") und Maschinenerstellungsdienste zum Bereitstellen folgender Elemente:

- Unterstützte Desktop- oder Serverbetriebssystem-VMs der ersten Generation.
- Unterstützte Desktop- oder Serverbetriebssystem-VMs der zweiten Generation, mit Secure Boot-Unterstützung.

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. Diese Konfiguration unterstützt die VM-Lebenszyklusverwaltung (z. B. VM erstellen, aktualisieren und löschen).

   Die direkte Installation eines Controllers auf einem Server, auf dem Hyper-V ausgeführt wird, wird nicht unterstützt.

In großen Bereitstellungen, in denen ein SCVMM mehrere Cluster in verschiedenen Datencentern verwaltet, können Sie den Hostgruppenbereich für delegierte Administratoren beschränken.

Verwenden Sie zum Beschränken des Hostgruppenbereichs die Rolle "Delegierter Administrator"in der Konsole des Microsoft System Center Virtual Machine Manager (SCVMM):

1. Wählen Sie im **Assistenten zum Erstellen von Benutzerrollen** die Benutzerrolle "Fabric-Administrator (Delegierter Administrator)".

2. Fügen Sie unter **Mitglieder** das Benutzerkonto im Active Directory hinzu, das Sie als delegierten Administrator verwenden möchten.
3. Wählen Sie in **Geltungsbereich** die Hostgruppen aus, auf die der delegierte Administrator Zugriff erhalten soll.
4. Erstellen Sie ein neues **Ausführendes Konto** mit den Benutzeranmeldeinformationen des delegierten Administrators. Verwenden Sie diese Anmeldeinformationen, um später eine Hypervisor-Verbindung herzustellen. Verwenden Sie nicht die Konten der Rolle "Hauptadministrator".

Azure Stack HCI-Provisioning über SCVMM

Azure Stack HCI ist eine Clusterlösung mit hyperkonvergenter Infrastruktur (HCI), die virtualisierte Windows- und Linux-Workloads und deren Speicher in einer hybriden On-Premises-Umgebung hostet.

Azure-Hybriddienste erweitern den Cluster durch Funktionen wie Cloud-basierte Überwachung, Site-Wiederherstellung und VM-Backups. Sie können auch eine zentrale Ansicht aller Azure Stack HCI-Bereitstellungen im Azure-Portal einrichten.

Integration von Azure Stack HCI mit SCVMM

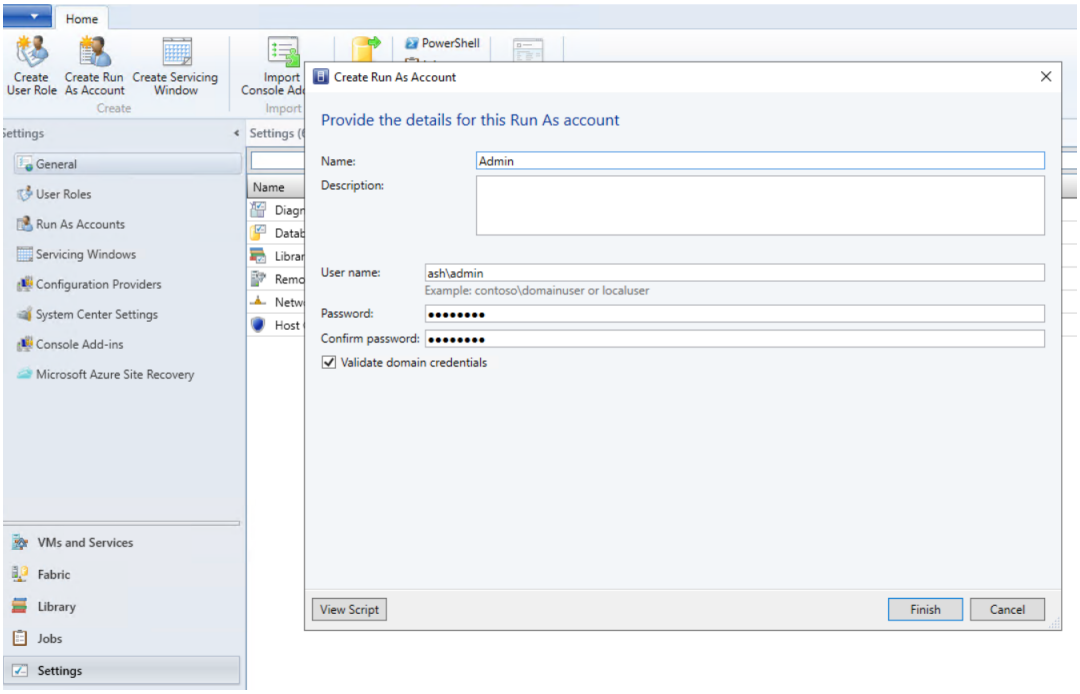
Um Azure Stack HCI mit SCVMM zu integrieren, müssen Sie zuerst einen Azure Stack HCI-Cluster erstellen und diesen Cluster dann mit SCVMM integrieren.

1. Informationen zum Erstellen des Azure Stack HCI-Clusters finden Sie im Microsoft-Dokument Herstellen einer Verbindung von Azure Stack HCI mit Azure.
2. Schrittfolge zum Integrieren von Azure Stack HCI-Cluster mit SCVMM:

    a) Melden Sie sich bei der Maschine an, die für das Hosten des SCVMM-Servers vorbereitet wurde, und installieren Sie SCVMM 2019 UR3 oder höher.

    > **Hinweis:**
    >
    > Installieren Sie die Administratorkonsole von SCVMM 2019 UR3 oder höher auf allen Controllern.

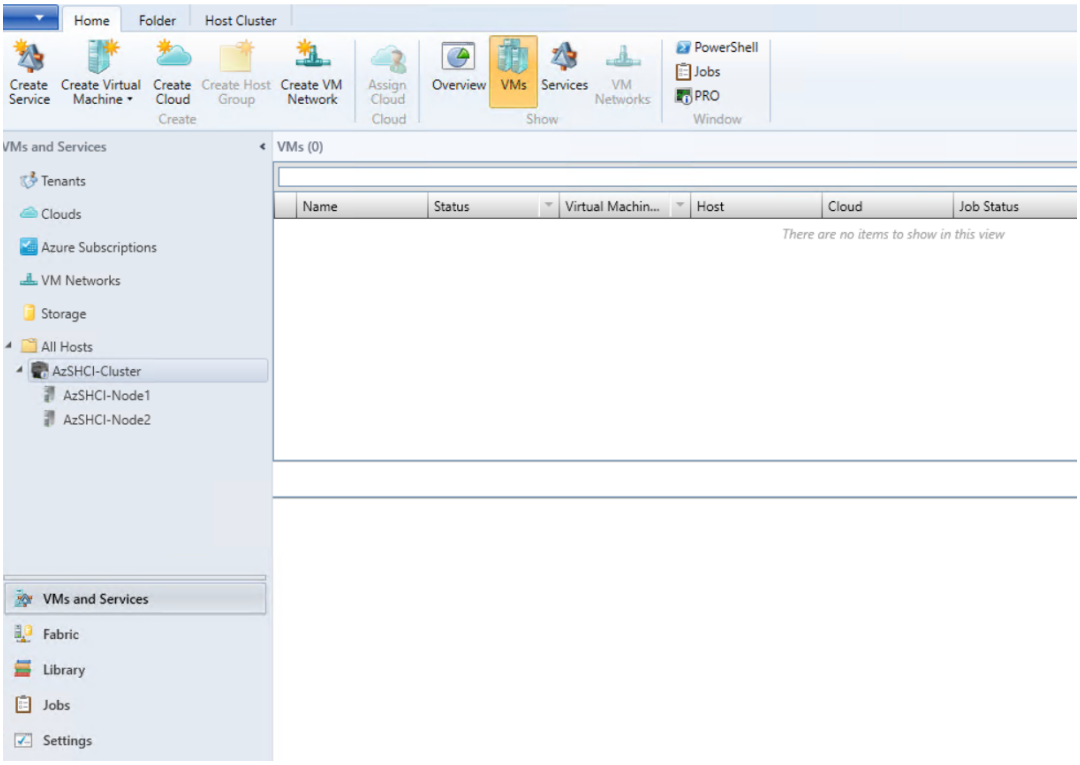
    b) Erstellen Sie auf der Seite **Einstellungen** der VMM-Konsole ein ausführendes Konto.



c) Führen Sie die folgenden PowerShell-Befehle mit Administratorrechten auf dem SCVMM-Server aus, um den Azure Stack HCI-Cluster als Host hinzuzufügen:

```
$runAsAccountName = 'Admin'
$runAsAccount = Get-SCRunAsAccount -Name $runAsAccountName
$hostGroupName = 'All Hosts'
$hostGroup = Get-SCVMHostGroup -Name $hostGroupName
$hostCluster = 'FQDN of Azure Stack HCI cluster'
Add-SCVMHostCluster -Name $hostCluster -RunAsynchronously -
    VMHostGroup
$hostGroup -Credential $runAsAccount -RemoteConnectEnabled
    $true
<!--NeedCopy-->
```

d) Sie können jetzt den Azure Stack HCI-Cluster samt Knoten in der VMM-Konsole sehen.



e) Erstellen Sie die SCVMM-Hostingverbindung in Web Studio.

So geht es weiter

- Kernkomponenten installieren
- VDAs installieren
- Site erstellen
- Informationen zum Erstellen und Verwalten einer Verbindung in SCVMM finden Sie unter Verbindung zu Microsoft System Center Virtual Machine Manager.

Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Maschinenkataloge erstellen

Nutanix-Virtualisierungsumgebungen

June 27, 2024

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, verfügbar im Nutanix Support Portal.

Installieren und Registrieren des Nutanix-Plug-Ins

Führen Sie die folgenden Schritte aus, um das Nutanix-Plug-In bei allen Delivery Controllern zu installieren und zu registrieren. Erstellen Sie mit Citrix Studio eine Verbindung mit Nutanix Erstellen Sie dann einen Maschinenkatalog mit dem Snapshot eines Masterimages, das Sie in der Nutanix-Umgebung erstellt haben.

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

Informationen zur Installation des Nutanix-Plug-Ins finden Sie in der Nutanix-Dokumentation.

So geht es weiter

- Kernkomponenten installieren
- VDAs installieren
- Site erstellen
- Informationen zum Erstellen und Verwalten einer Verbindung in Nuntanix-Umgebungen finden Sie unter Verbindung zu Nutanix.

Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Maschinenkataloge erstellen

Nutanix-Cloud und Partnerlösungen

June 27, 2024

Citrix Virtual Apps and Desktops unterstützt die folgende Nutanix-Cloud und Partnerlösung:

- Nutanix Cloud Clusters in AWS

Nutanix Cloud Clusters in AWS

Citrix Virtual Apps and Desktops unterstützt Nutanix Cloud-Cluster auf AWS. Nutanix-Cluster vereinfachen das Ausführen von Anwendungen in privaten oder mehreren öffentlichen Clouds. Weitere Informationen zu Nutanix Cloud Clusters auf AWS finden Sie unter Nutanix Cloud Clusters on AWS Deployment and User Guide.

> **Tipp:**
>
> Diese Unterstützung bietet dieselbe Funktionalität wie ein on-premises bereitgestellter Nutanix-Cluster. Es wird nur ein einziger Cluster unterstützt: *Prism Element*. Weitere Informationen finden Sie hier.

Anforderungen

Sie benötigen Folgendes, um Nutanix-Cluster auf AWS zu verwenden:

- Ein Nutanix-Konto.
- Ein AWS-Konto mit den folgenden Berechtigungen:
  - IAMFullAccess
  - AWSConfigRole
  - AWSCloudFormationFullAccess

Erstellen eines Nutanix-Clusters

Schrittfolge zum Erstellen eines Nutanix-Clusters:

1. Melden Sie sich bei Ihrem Nutanix-Konto an.
2. Suchen Sie die Option **Nutanix cluster** und klicken Sie auf **Launch**. Die **Nutanix-Konsole** wird geöffnet. Weitere Informationen finden Sie unter Get Started with Nutanix Cluster on AWS.
3. Erstellen Sie eine **neue virtuelle private Cloud (VPC)**.

Das Erstellen des Clusters schlägt möglicherweise fehl, wobei folgende Fehlermeldungen angezeigt werden:

- Cluster konnte nicht innerhalb der vorgegebenen Zeit erstellt werden. Der Cluster wird gelöscht.
- Host-Nutanix-Cluster –Knoten `XXXXXXXXXXX: Instance i-xxxxxxxxxxxxx: disable network interface source/dest check error.`
- Host-Nutanix-Cluster –Knoten `XXXXXXXXXXX: Unable to obtain instance i-xxxxxxxxxxxxxx network interface info.`

Wenn der Cluster nicht erstellt werden konnte:

- Versuchen Sie, den Cluster in einer anderen Region neu zu erstellen.
- Löschen Sie den Nutanix-CloudFormation-Stack (CFS), bevor Sie den Versuch wiederholen.

Zusätzlich zu anderen Ressourcen erstellt der Nutanix-CFS Folgendes:

- 1 virtuelle private Cloud mit dem Namen *Nutanix Cluster xxxxxxxxxxxx* 10.0.0.0/16
- 2 Subnetze: 10.0.128.0/24 und 10.0.129.0/24
- 1 Internetgateway
- 1 NAT-Gateway

Rufen Sie nach dem Erstellen des Clusters die Adresse von **Nutanix Prism** ab:

1. Wechseln Sie zur **Nutanix-Konsole**.
2. Zeigen Sie mit der Maus auf den Link **Launch Prism Element** rechts oben auf der Konsole und kopieren Sie die URL.

So geht es weiter

- Kernkomponenten installieren
- VDAs installieren
- Site erstellen
- Informationen zum Erstellen und Verwalten einer Verbindung zu Nutanix-Cloud und Partnerlösungen finden Sie unter Verbindung zu Nutanix-Cloud und Partnerlösungen.

Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Maschinenkataloge erstellen

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.

So geht es weiter

- Kernkomponenten installieren
- VDAs installieren
- Site erstellen
- Informationen zum Erstellen und Verwalten einer Verbindung zu VMware-Umgebungen finden Sie unter Verbindung zu VMware.

Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Maschinenkataloge erstellen

Cloud- und Partnerlösungen von VMware

June 27, 2024

Citrix Virtual Apps and Desktops unterstützt die folgende VMware Cloud samt Partnerlösungen:

- Azure VMware-Lösung (AVS)
- Google Cloud VMware Engine
- VMware-Cloud auf Amazon Web Services (AWS)

Integration von Azure VMware Solution (AVS)

Citrix Virtual Apps and Desktops Service unterstützt AVS. AVS bietet Cloudinfrastruktur mit vSphere-Clustern, die von der Azure-Infrastruktur erstellt wurden. Nutzen Sie den Citrix Virtual Apps and Desktop Service, um AVS für das Provisioning der VDA-Workload auf die gleiche Weise zu verwenden, in der Sie vSphere in On-Premises-Umgebungen verwenden würden.

AVS-Cluster einrichten

Führen Sie die folgenden Schritte in Azure aus, um Citrix Virtual Apps and Desktop Service die Verwendung von AVS zu ermöglichen:

- Hostkontingent anfordern
- Registrieren des Microsoft.AVS-Ressourcenanbieters
- Netzwerk-Checkliste
- Erstellen einer privaten Azure VMware Solution-Cloud
- Zugreifen auf eine private Azure VMware Solution-Cloud
- Konfigurieren des Netzwerks für Ihre private VMware-Cloud in Azure
- Konfigurieren von DHCP für Azure VMware Solution
- Hinzufügen eines Netzwerksegments in Azure VMware Solution
- Überprüfen der Azure VMware Solution-Umgebung

Hostkontingent für Kunden von Azure Enterprise Agreement anfordern Wählen Sie auf der Seite **Hilfe + Support** des Azure-Portals **Neue Supportanfrage** aus und fügen Sie die folgenden Informationen hinzu:

- Problemtyp:Technisch
- Abonnement:Wählen Sie ein Abonnement aus
- Dienst:Alle Dienste > Azure VMware Solution
- Ressource:Allgemeine Frage
- Zusammenfassung:Kapazität erforderlich
- Problemtyp:Capacity Management Issues (Kapazitätsverwaltungsprobleme)
- Problemuntertyp:Customer Request for Additional Host Quota/Capacity (Kundenanfrage für zusätzliches Hostkontingent/zusätzliche Hostkapazität)

Geben Sie in der **Beschreibung** des Supporttickets auf der Registerkarte **Details** die folgenden Informationen an:

- Proof of Concept oder Produktion
- Name der Region
- Anzahl von Hosts

- Weitere Details

> **Hinweis:**
>
> AVS erfordert mindestens drei Hosts und empfiehlt eine Redundanz von N+1 Hosts.

Wenn Sie die Details für das Supportticket angegeben haben, wählen Sie **Überprüfen und erstellen** aus, um die Anforderung an Azure zu senden.

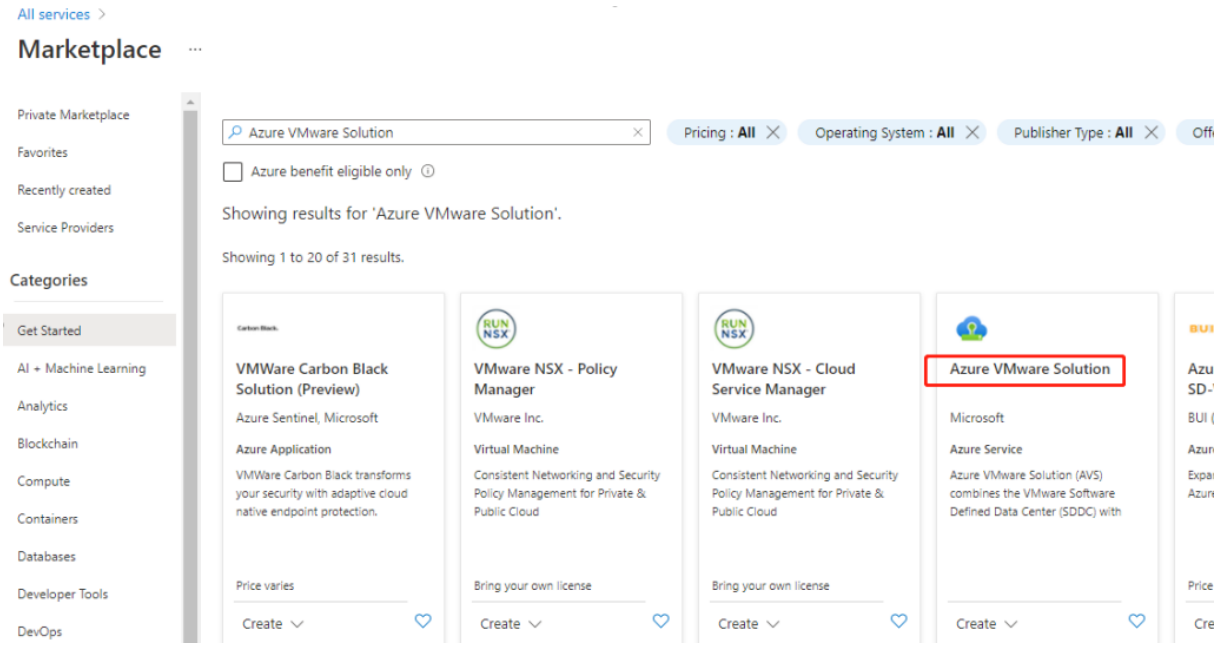
Registrieren des Microsoft.AVS-Ressourcenanbieters Nach Anforderung des Hostkontingents müssen Sie den Ressourcenanbieter registrieren:

1. Melden Sie sich beim Azure-Portal an.
2. Wählen Sie im Menü des Azure-Portals **Alle Dienste** aus.
3. Geben Sie im Menü **Alle Dienste** das Abonnement ein und wählen Sie **Abonnements** aus.
4. Wählen Sie das Abonnement aus der Abonnementliste aus.
5. Wählen Sie **Ressourcenanbieter** aus und geben Sie **Microsoft.AVS** als Suchbegriff in die Suchleiste ein.
6. Wählen Sie **Registrieren** aus, falls der Ressourcenanbieter nicht registriert ist.

Überlegungen zum Netzwerk AVS bietet Netzwerkdienste an, die bestimmte Netzwerkadressbereiche und Firewallports erfordern. Weitere Informationen finden Sie unter Checkliste für die Netzwerkplanung für Azure VMware Solution.

Erstellen einer privaten Azure VMware Solution-Cloud Erstellen Sie nach Prüfung der Netzwerkanforderungen für Ihre Umgebung eine private ASV-Cloud:

1. Melden Sie sich beim Azure-Portal an.
2. Wählen Sie **Neue Ressource erstellen** aus.
3. Geben Sie im Textfeld **Marketplace durchsuchen** den Text *Azure VMware Solution* ein und wählen Sie **Azure VMware Solution** in der Liste aus.



Abbildung

Im Fenster **Azure VMware Solution**:

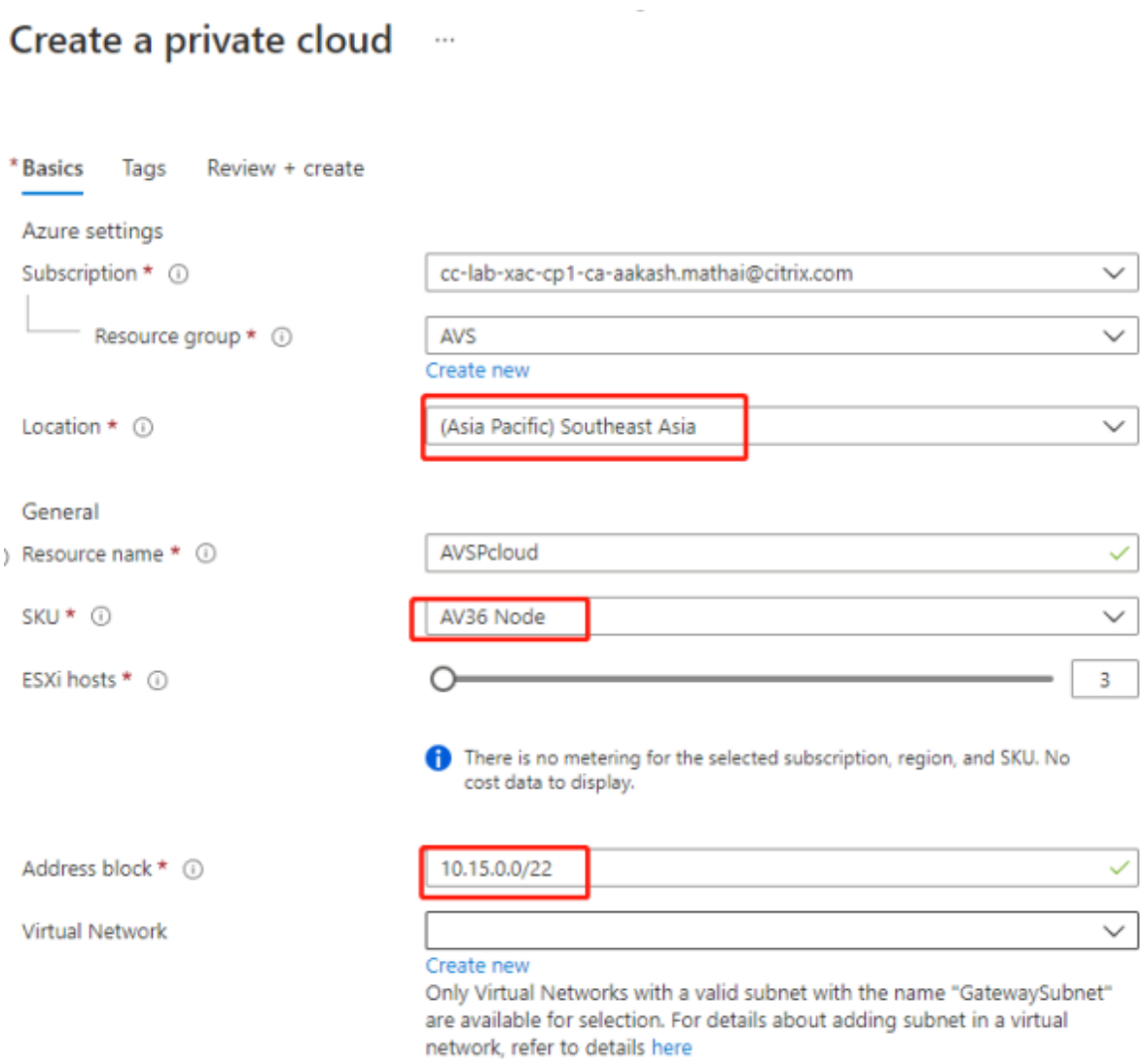
1. Wählen Sie **Create**.
2. Klicken Sie auf die Registerkarte **Grundlagen**.
3. Geben Sie Werte für die Felder ein. Verwenden Sie dazu die Informationen in der folgenden Tabelle:

Feld	Wert
Abonnement	Wählen Sie das Abonnement aus, das Sie für die Bereitstellung verwenden möchten. Alle Ressourcen in einem Azure-Abonnement werden gemeinsam abgerechnet.
Ressourcengruppe	Wählen Sie die Ressourcengruppe für Ihre private Cloud aus. Eine Azure-Ressourcengruppe ist ein logischer Container, in dem Azure-Ressourcen bereitgestellt und verwaltet werden. Alternativ können Sie eine neue Ressourcengruppe für Ihre private Cloud erstellen.
Standort	Wählen Sie einen Standort aus (beispielsweise USA, Osten). Dies ist die Region, die Sie während der Planungsphase definiert haben.

Feld	Wert
Ressourcenname	Geben Sie den Namen Ihrer privaten Azure VMware Solution-Cloud an.
SKU	Wählen Sie AV36 aus.
Hosts	Zeigt die Anzahl der Hosts an, die dem privaten Cloudcluster zugeordnet sind. Der Standardwert ist 3. Sie können den Wert nach der Bereitstellung erhöhen oder verringern.
Adressblock	Geben Sie einen IP-Adressblock für die private Cloud an. CIDR stellt das Verwaltungsnetzwerk der privaten Cloud dar und wird für die Clusterverwaltungsdienste wie vCenter Server und NSX-T Manager verwendet. Geben Sie einen /22-Adressraum an, beispielsweise 10.175.0.0/22. Die Adresse sollte eindeutig sein und sich nicht mit anderen Azure Virtual Networks und On-Premises-Netzwerken überschneiden.
Virtuelles Netzwerk	Lassen Sie dieses Feld leer, da die Azure VMware Solution ExpressRoute-Leitung als Schritt nach der Bereitstellung eingerichtet wird.

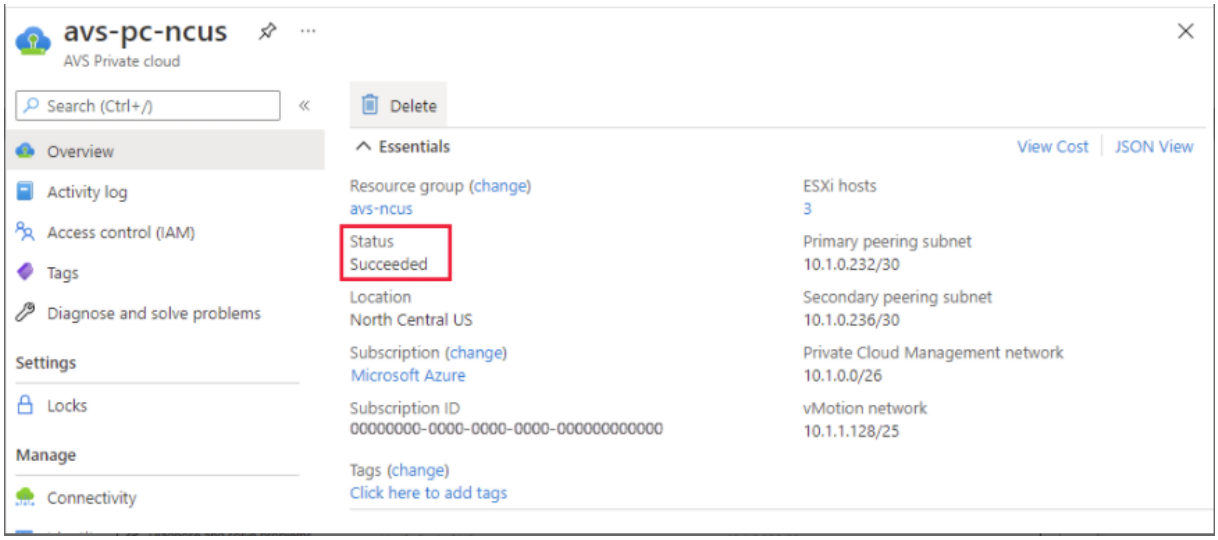
Auf dem Bildschirm **Erstellen einer privaten Cloud**:

1. Wählen Sie im Feld **Standort** die Region mit dem AVS aus. Die Region der Ressourcengruppe entspricht der AVS-Region.
2. Wählen Sie im Feld **SKU** den Knoten **AV36** aus.
3. Geben Sie im Feld **Adressblock** eine IP-Adresse an. Beispiel: 10.15.0.0/22.
4. Wählen Sie **Überprüfen und erstellen** aus.
5. Klicken Sie nach dem Überprüfen der Informationen auf **Erstellen**.



> **Tipp:**
>
> Das Erstellen einer privaten Cloud kann 3 bis 4 Stunden dauern. Das Hinzufügen eines einzelnen Hosts zum Cluster kann 30 bis 45 Minuten dauern.

Vergewissern Sie sich, dass die Bereitstellung erfolgreich war. Navigieren Sie zu der von Ihnen erstellten Ressourcengruppe und wählen Sie Ihre private Cloud aus. Wenn der **Status Erfolgreich** angezeigt wird, ist die Bereitstellung abgeschlossen.



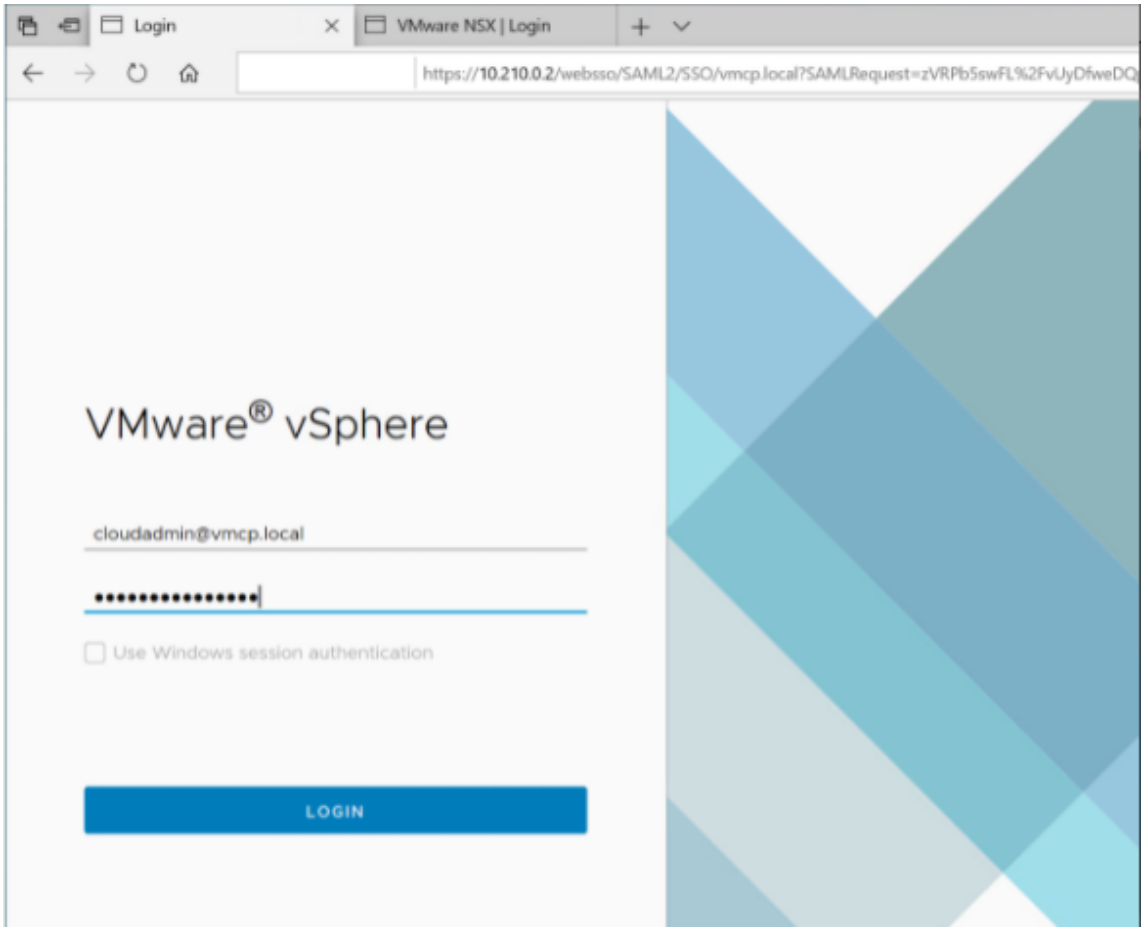
Zugreifen auf eine private Azure VMware Solution-Cloud Erstellen Sie nach dem Erstellen einer privaten Cloud eine Windows-VM und stellen Sie eine Verbindung zum lokalen vCenter Ihrer privaten Cloud her.

Erstellen einer neuen virtuellen Windows-Maschine

1. Wählen Sie in der Ressourcengruppe **+ Hinzufügen** aus, suchen Sie nach **Microsoft Windows 10/2016/2019** und wählen Sie es aus.
2. Klicken Sie auf **Erstellen**.
3. Geben Sie die erforderlichen Informationen ein und wählen Sie dann **Überprüfen + erstellen** aus.
4. Wählen Sie nach erfolgreicher Validierung **Erstellen** aus, um den Erstellungsprozess der virtuellen Maschine zu starten.

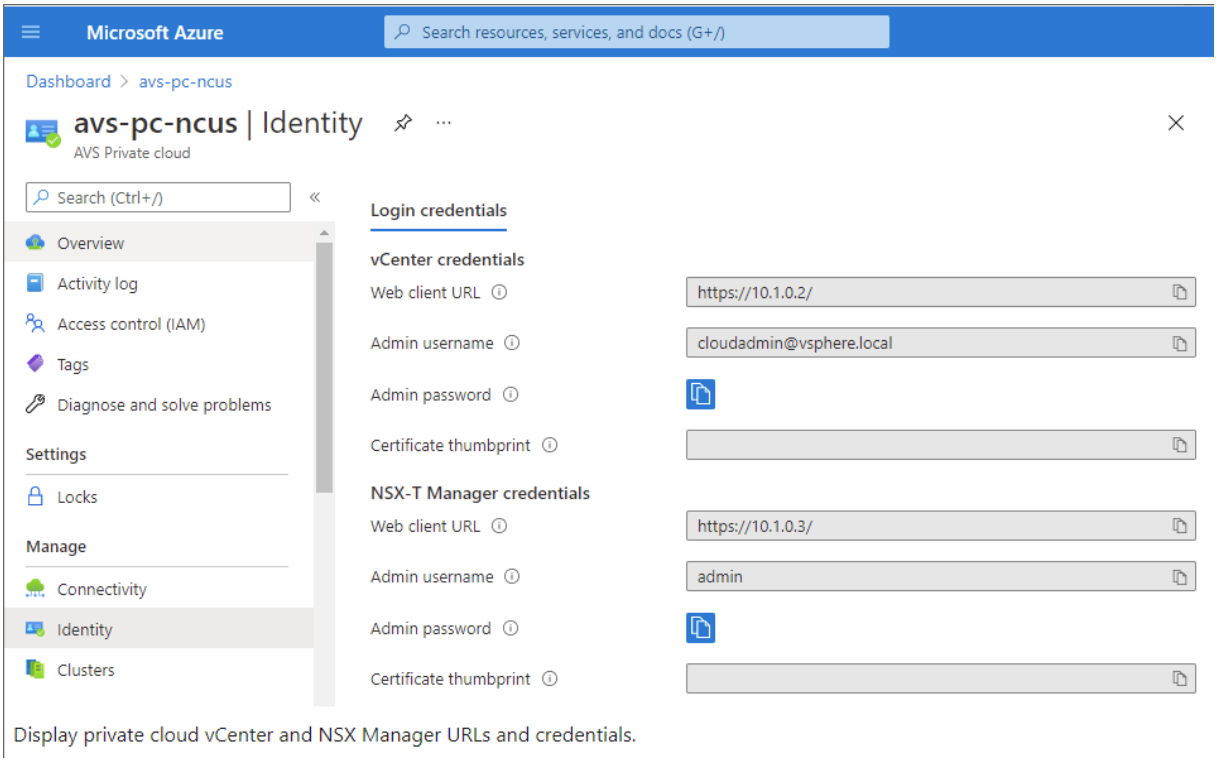
Herstellen einer Verbindung mit dem lokalen vCenter Ihrer privaten Cloud

1. Melden Sie sich als Cloudadministrator mit **VMware vCenter SSO beim vSphere-Client** an.



2. Wählen Sie im Azure-Portal Ihre private Cloud aus und wählen Sie dann **Verwalten > Identität**.

Die URLs und Benutzeranmeldeinformationen für vCenter und NSX-T Manager der privaten Cloud werden angezeigt:



Display private cloud vCenter and NSX Manager URLs and credentials.

Nach der Bestätigung der URLs und Benutzeranmeldeinformationen:

1. Navigieren Sie zu der VM, die Sie im vorherigen Schritt erstellt haben, und stellen Sie eine Verbindung zur virtuellen Maschine her.
2. Öffnen Sie in der Windows-VM einen Browser und navigieren Sie auf zwei Browserregisterkarten zu den URLs für vCenter- und NSX-T Manager. Geben Sie auf der Registerkarte "vCenter"die Benutzeranmeldeinformationen für *cloudadmin@vmcp.local* aus dem vorherigen Schritt ein.

Konfigurieren des Netzwerks für Ihre private VMware-Cloud in Azure Konfigurieren Sie nach dem Zugriff auf eine private ASV-Cloud das Netzwerk, indem Sie ein virtuelles Netzwerk und ein Gateway erstellen.

Erstellen eines virtuellen Netzwerks

1. Melden Sie sich beim Azure-Portal an.
2. Navigieren Sie zu der zuvor erstellten Ressourcengruppe.
3. Wählen Sie **+ Hinzufügen** aus, um eine neue Ressource zu definieren.
4. Geben Sie im Textfeld **Marketplace durchsuchen** den Text *Virtuelles Netzwerk* ein. Suchen Sie nach der Ressource für virtuelle Netzwerke und wählen Sie sie aus.
5. Wählen Sie auf der Seite **Virtuelles Netzwerk** die Option **Erstellen** aus, um das virtuelle Netzwerk für Ihre private Cloud einzurichten.

6. Geben Sie auf der Seite **Virtuelles Netzwerk erstellen** die Details für Ihr virtuelles Netzwerk ein.
7. Geben Sie auf der Registerkarte **Grundlagen** einen Namen für das virtuelle Netzwerk ein, wählen Sie die entsprechende Region aus und klicken Sie auf **Weiter: IP-Adressen**.
8. Geben Sie auf der Registerkarte **IP-Adressen** unter "IPv4-Adressraum"die zuvor erstellte Adresse ein.

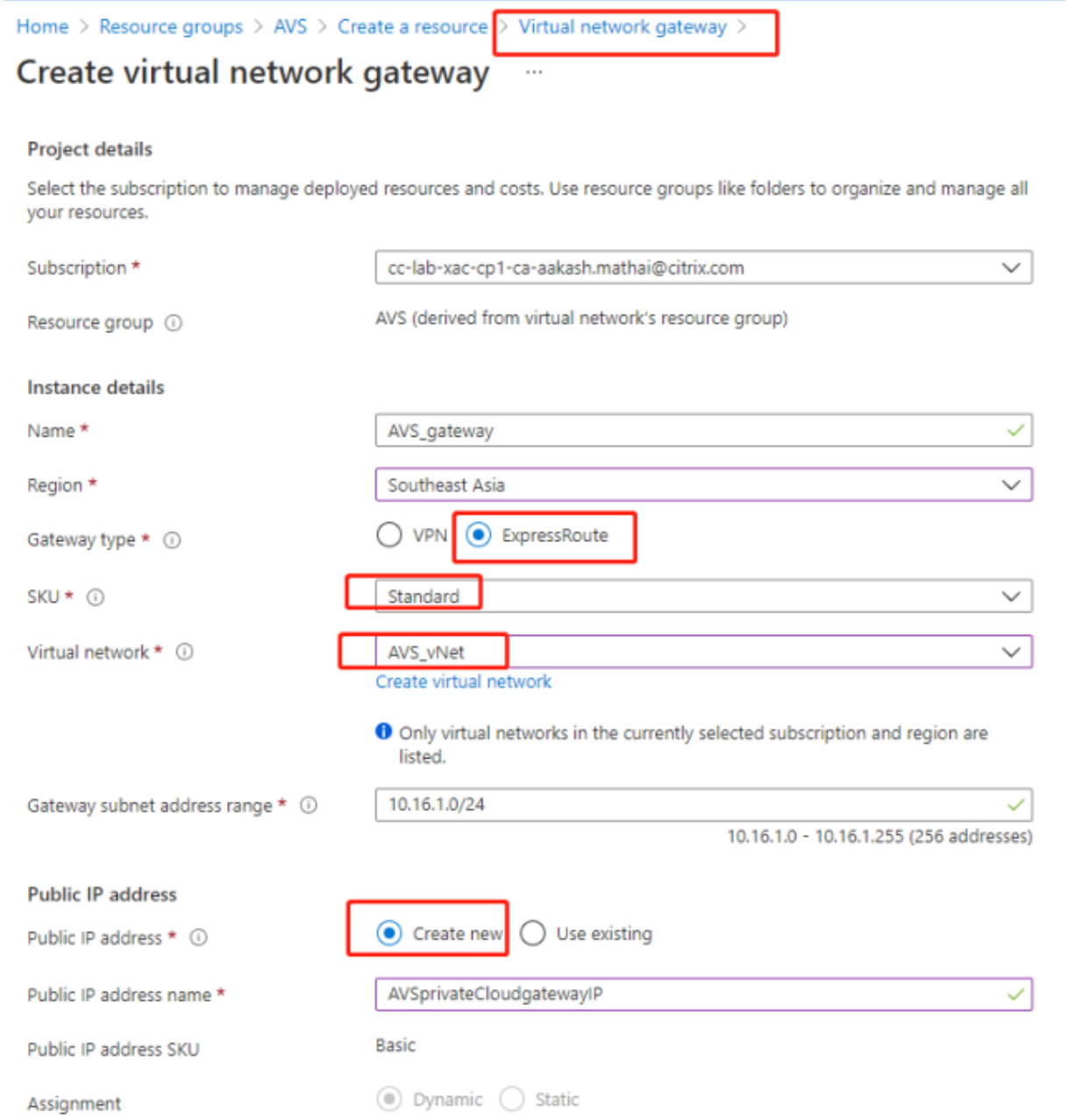
> **Wichtig:**
>
> Verwenden Sie eine Adresse, die sich nicht mit dem Adressraum überschneidet, den Sie bei der Erstellung Ihrer privaten Cloud verwendet haben.

Nach Eingabe des Adressraums:

1. Wählen Sie **+ Subnetz hinzufügen** aus.
2. Geben Sie auf der Seite **Subnetz hinzufügen** einen Namen und einen entsprechenden Adressbereich für das Subnetz an.
3. Klicken Sie auf **Hinzufügen**.
4. Wählen Sie **Überprüfen und erstellen** aus.
5. Überprüfen Sie die Angaben und klicken Sie auf **Erstellen**. Nach Abschluss der Bereitstellung wird das virtuelle Netzwerk in der Ressourcengruppe angezeigt.

Erstellen eines Gateways für das virtuelle Netzwerk Erstellen Sie nach dem Erstellen eines virtuellen Netzwerks ein Gateway für das virtuelle Netzwerk.

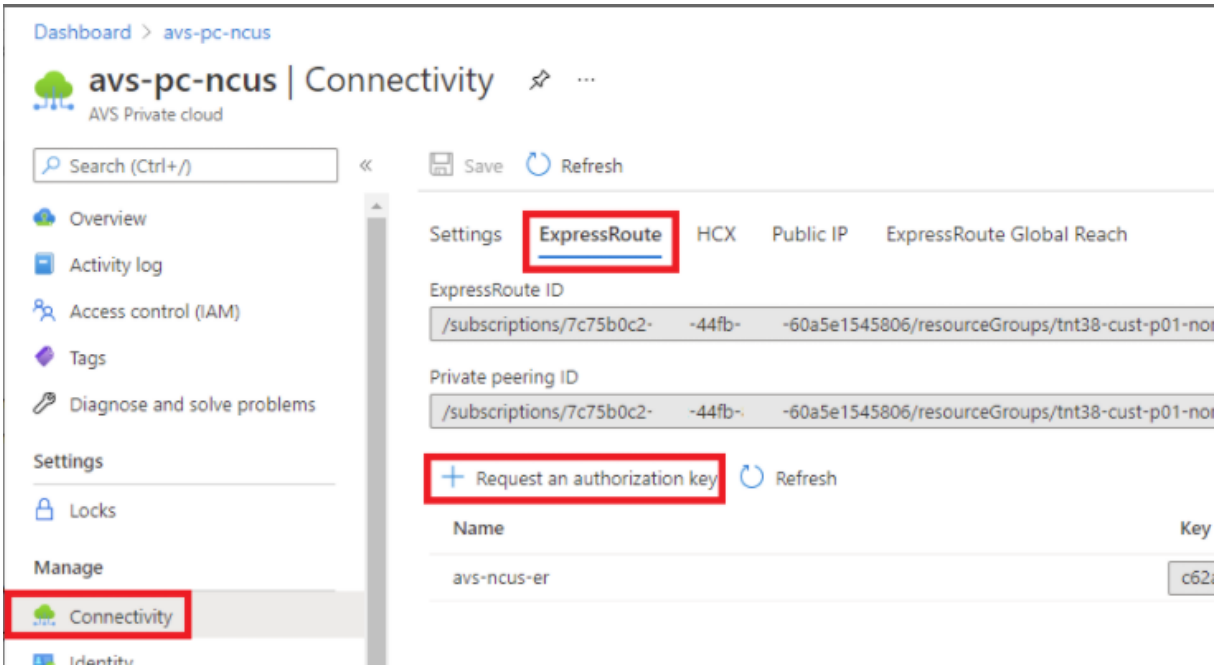
1. Wählen Sie in der Ressourcengruppe **+ Hinzufügen** aus, um eine neue Ressource hinzuzufügen.
2. Geben Sie im Textfeld **Marketplace durchsuchen** den Text *Gateway für virtuelle Netzwerke* ein. Suchen Sie nach der Ressource für virtuelle Netzwerke und wählen Sie sie aus.
3. Klicken Sie auf der Seite **Gateway für virtuelle Netzwerke** auf **Erstellen**.
4. Geben Sie auf der Registerkarte **Grundlagen** der Seite **Gateway für virtuelle Netzwerke erstellen** Werte für die Felder an.
5. Klicken Sie auf **Überprüfen und erstellen**.



Klicken Sie nach der Überprüfung der Konfiguration des Gateways für virtuelle Netzwerke auf **Erstellen**, um die Bereitstellung des Gateways für virtuelle Netzwerke zu starten.
Verbinden Sie nach Abschluss der Bereitstellung Ihre **ExpressRoute**-Verbindung mit dem Gateway für virtuelle Netzwerke, das Ihre private Azure AVS-Cloud enthält.

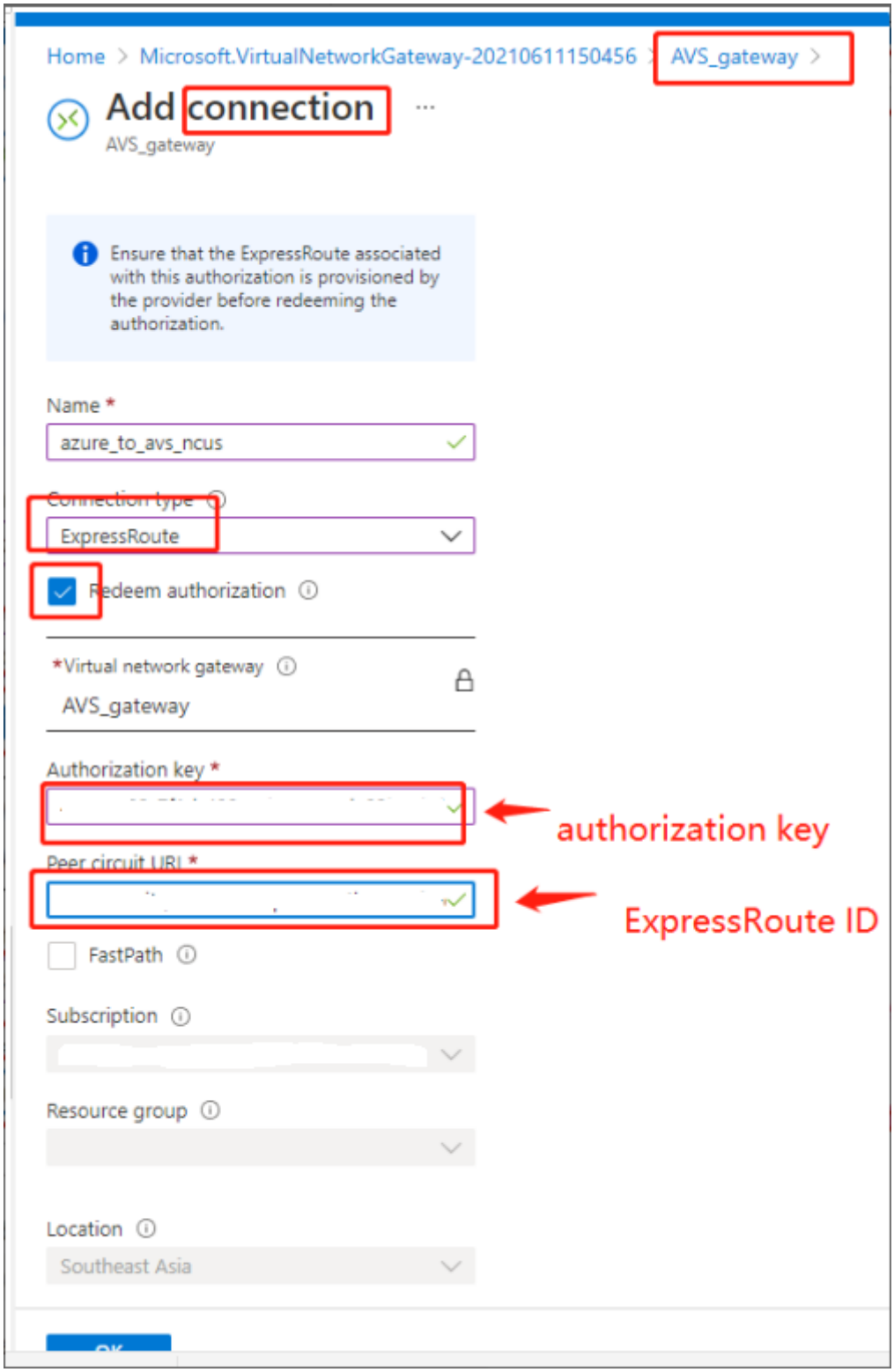
Verbinden von ExpressRoute mit dem Gateway für virtuelle Netzwerke Fügen Sie nach der Bereitstellung eines Gateways für virtuelle Netzwerke eine Verbindung zwischen dem Gateway und Ihrer privaten Azure AVS-Cloud hinzu:

1. Fordern Sie einen ExpressRoute-Autorisierungsschlüssel an.
2. Navigieren Sie im Azure-Portal zur **privaten Azure VMware Solution-Cloud**. Wählen Sie **Verwalten > Konnektivität > ExpressRoute** und anschließend **+ Autorisierungsschlüssel anfordern** aus.

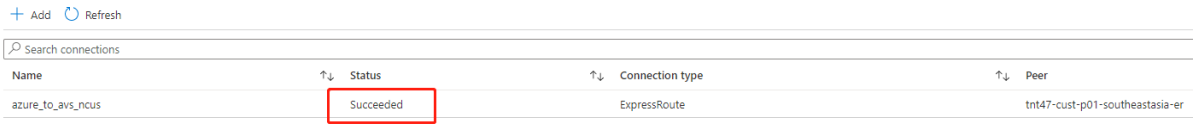


Nach dem Anfordern eines Autorisierungsschlüssels:

1. Geben Sie einen Namen für den Schlüssel ein und klicken Sie auf **Erstellen**. Das Erstellen des Schlüssels kann etwa 30 Sekunden dauern. Nach der Erstellung wird der neue Schlüssel in der Liste der Autorisierungsschlüssel für die private Cloud angezeigt.
2. Kopieren Sie den **Autorisierungsschlüssel** und die **ExpressRoute-ID**. Diese Angaben benötigen Sie, um den Peering-Prozess abzuschließen. Der Autorisierungsschlüssel wird nach einiger Zeit nicht mehr angezeigt. Kopieren Sie ihn daher, sobald er angezeigt wird.
3. Navigieren Sie zu dem **Gateway für virtuelle Netzwerke**, das Sie verwenden möchten, und wählen Sie **Verbindungen > + Hinzufügen** aus.
4. Geben Sie auf der Seite **Verbindung hinzufügen** Werte für die Felder ein und wählen Sie **OK** aus.



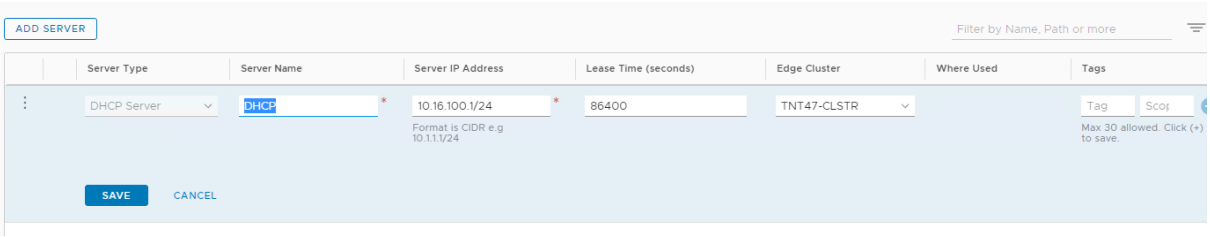
Die Verbindung zwischen Ihrer ExpressRoute-Leitung und Ihrem virtuellen Netzwerk wird hergestellt:



Konfigurieren von DHCP für Azure VMware Solution Konfigurieren Sie DHCP, nachdem Sie ExpressRoute mit dem virtuellen Gateway verbunden haben.

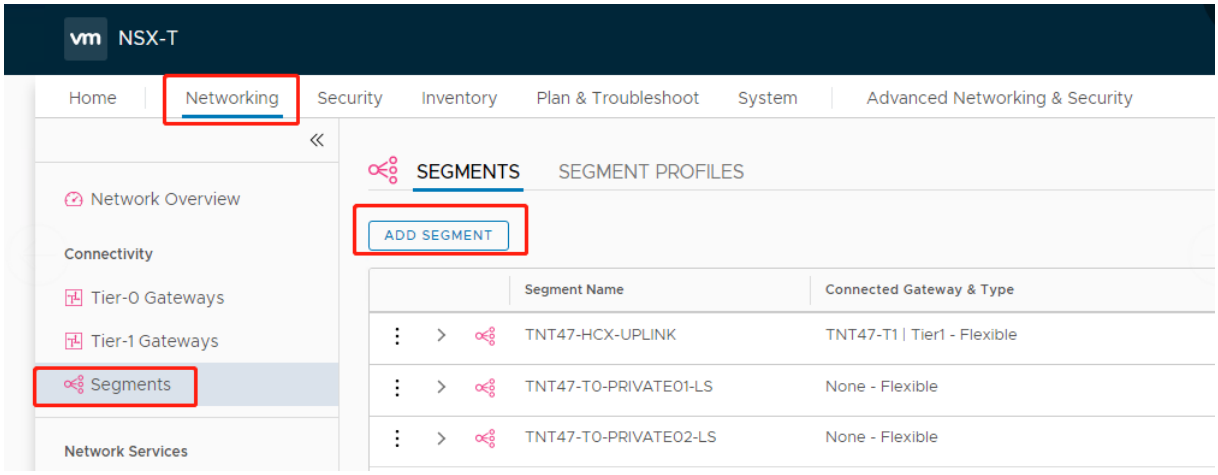
Verwenden von NSX-T zum Hosten Ihres DHCP-Servers In NSX-T Manager:

1. Wählen Sie **Networking > DHCP** und dann **Add Server** aus.
2. Wählen Sie **DHCP** unter **Server Type** aus und geben Sie den Servernamen und die IP-Adresse an.
3. Klicken Sie auf **Speichern**.
4. Wählen Sie **Tier-1 Gateways** aus. Wählen Sie dann die vertikalen Auslassungspunkte für das Tier-1-Gateway und anschließend **Edit** aus.
5. Wählen Sie **No IP Allocation Set** aus, um ein Subnetz hinzuzufügen.
6. Wählen Sie **DHCP Local Server** unter **Type** aus.
7. Wählen Sie für **DHCP Server** die Option **Default DHCP** aus und klicken Sie dann auf **Save**.
8. Klicken Sie erneut auf **Save** und wählen Sie dann **Close Editing** aus.



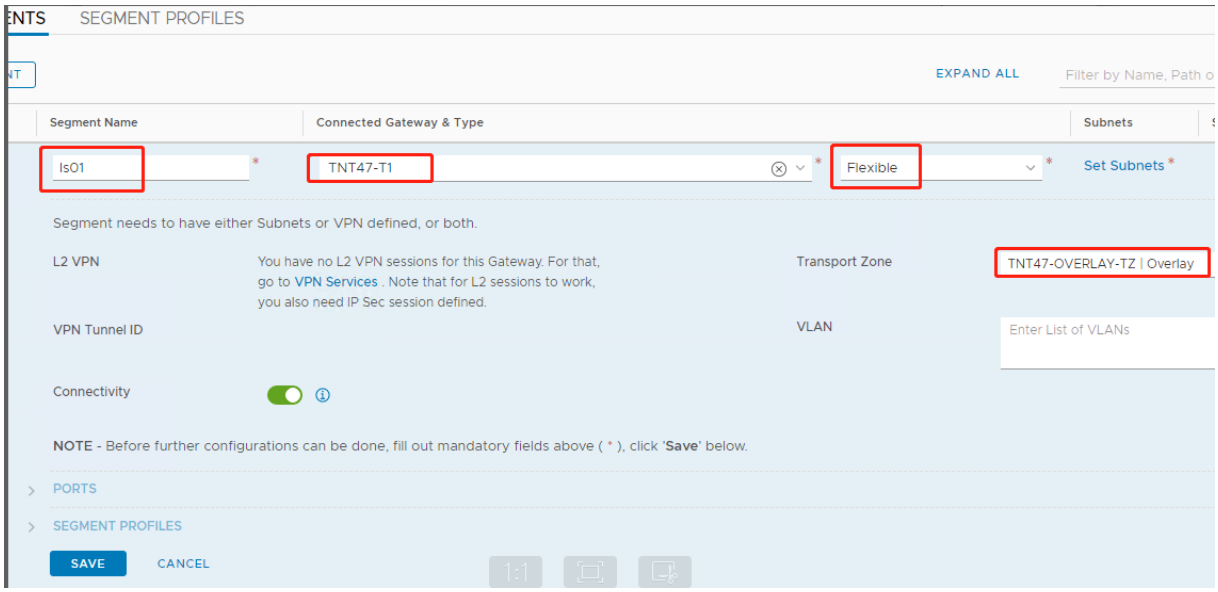
Hinzufügen eines Netzwerksegments in Azure VMware Solution Fügen Sie nach dem Einrichten von DHCP ein Netzwerksegment hinzu.

Zum Hinzufügen eines Netzwerksegments wählen Sie in NSX-T Manager **Networking > Segments** aus und klicken dann auf **Add Segment**.



Auf dem Bildschirm **Segment Profiles**:

1. Geben Sie einen **Namen** für das Segment ein.
2. Wählen Sie unter **Connected Gateway** das **Tier-1 Gateway (TNTxx-T1)** aus und übernehmen Sie für **Type** die Option **Flexible**.
3. Wählen Sie die vorkonfigurierte **Transport Zone(TNTxx-OVERLAY-TZ)** für die Überlagerung aus.
4. Klicken Sie auf **Set Subnets**.



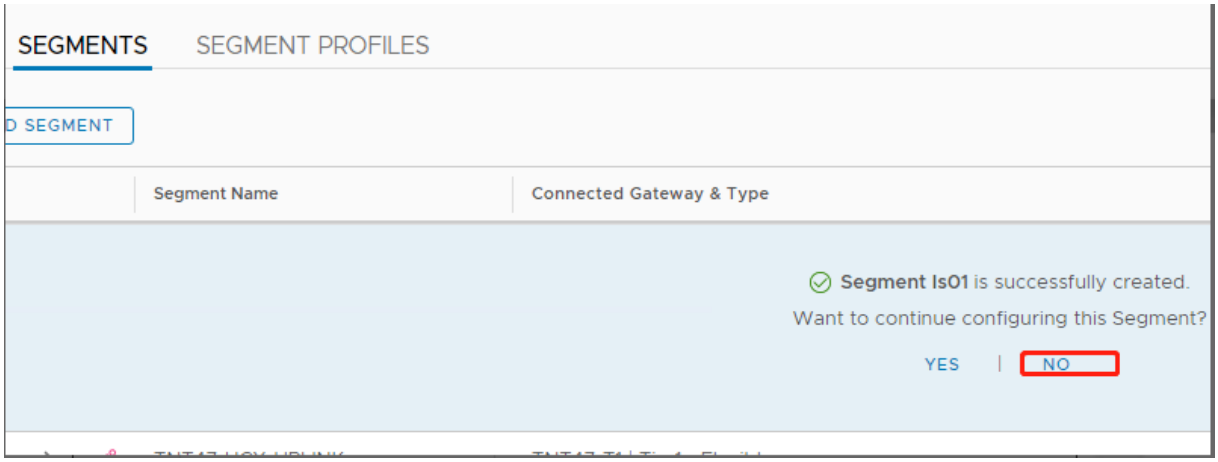
Im Abschnitt **Subnets**:

1. Geben Sie die IP-Adresse des Gateways ein.
2. Wählen Sie **Hinzufügen** aus.

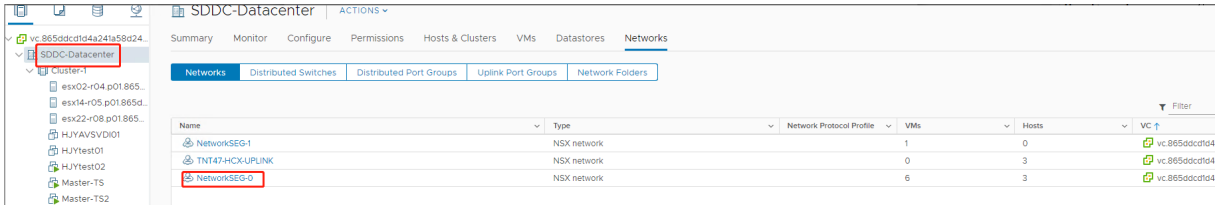
> **Wichtig:**
>
> Diese Segment-IP-Adresse muss Teil der Azure-Gateway-IP-Adresse 10.15.0.0/22 sein.

Der DHCP-Bereich sollte zur Segment-IP-Adresse gehören:

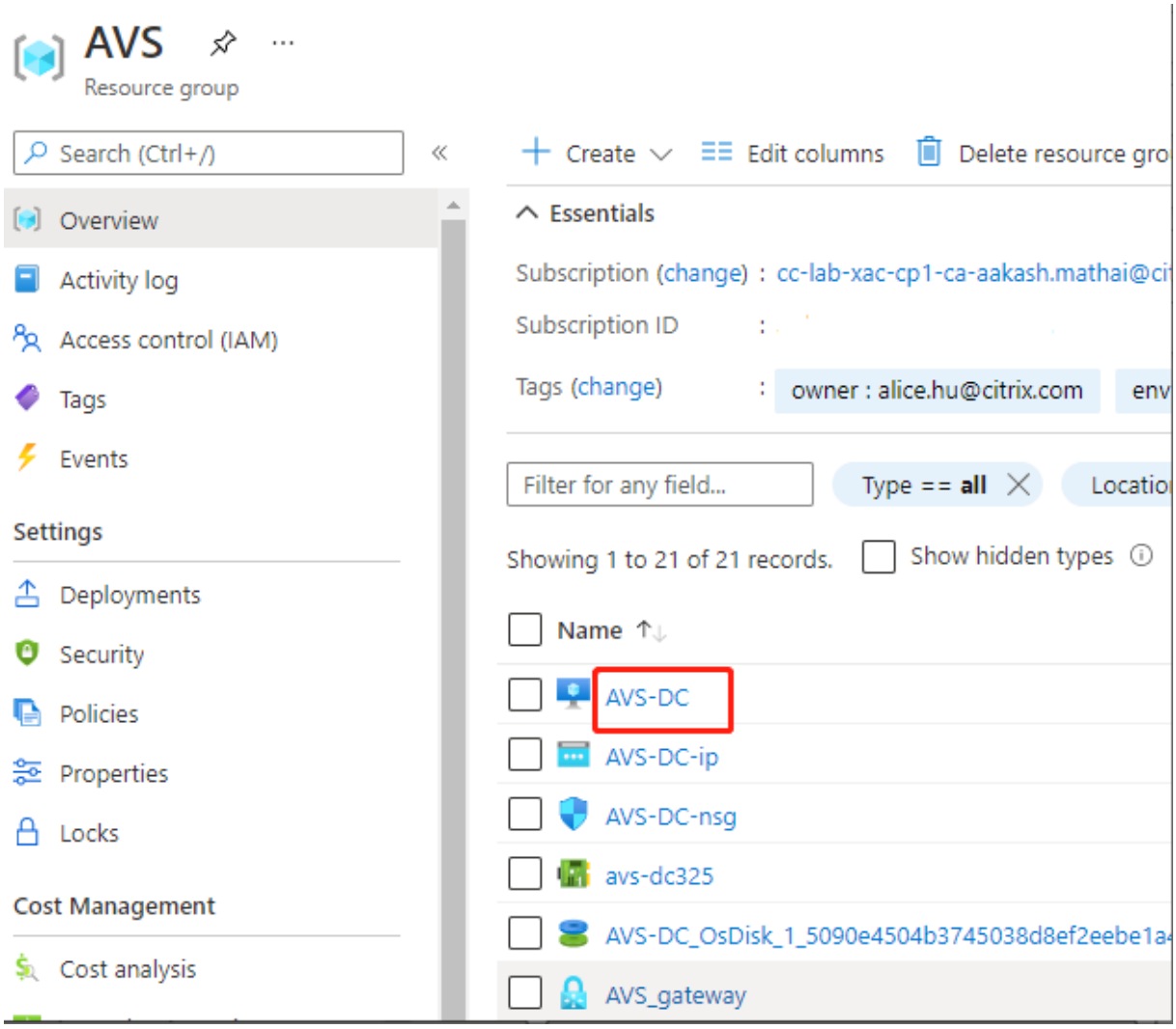
Wählen Sie **No** aus, um die Option zur weiteren Konfiguration des Segments abzulehnen:



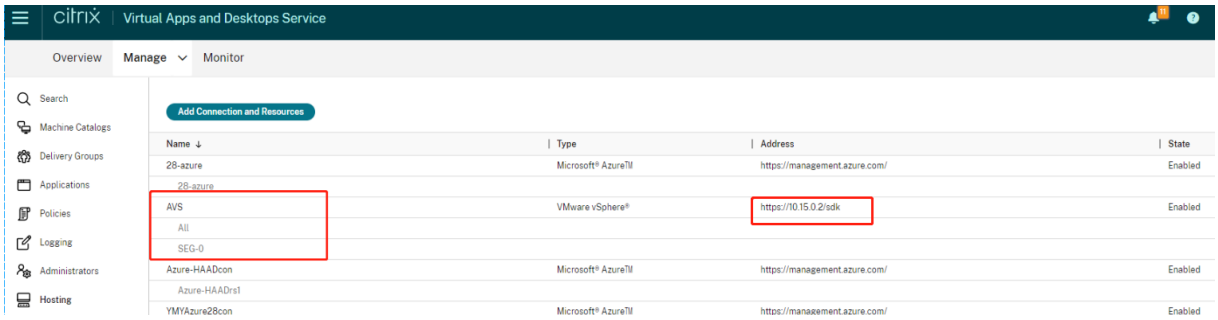
Wählen Sie in vCenter **Networking > SDDC-Datacenter** aus:



Überprüfen der Azure AVS-Umgebung Richten Sie eine direkte Verbindung und einen Connector in der Azure-Ressourcengruppe ein:



Verifizieren Sie die Verbindung mit vCenter-Anmeldeinformationen:



Google Cloud VMware Engine

Mit Citrix Virtual Apps and Desktops können Sie VMware-basierte Citrix On-Premises-Workloads nach Google Cloud VMware Engine migrieren.

Google Cloud VMware Engine konfigurieren

Nachfolgend wird beschrieben, wie Sie Cluster in Google Cloud VMware Engine erhalten und einrichten.

Zugriff auf das VMware Engine-Portal

1. Klicken Sie in der **Google Cloud-Konsole** auf das Navigationsmenü.
2. Klicken Sie im Abschnitt **Compute** auf **VMware Engine**, um VMware Engine in einer neuen Browserregisterkarte zu öffnen.

Anforderungen zum Erstellen der ersten privaten Cloud Sie benötigen Zugriff auf Google Cloud VMware Engine, verfügbares VMware Engine-Knotenkontingent und eine geeignete IAM-Rolle. Treffen Sie folgende Vorbereitungen, bevor Sie mit der Erstellung Ihrer privaten Cloud fortfahren:

1. Fordern Sie API-Zugriff und Knotenkontingent an. Weitere Informationen finden Sie unter Requesting API access and quota.
2. Notieren Sie die Adressbereiche, die Sie für VMware-Verwaltungsgeräte und das HCX-Bereitstellungsnetzwerk verwenden möchten. Weitere Informationen finden Sie unter Networking requirements.
3. Beschaffen Sie sich die IAM-Rolle eines VMware Engine Service-Administrators.

Erstellen der ersten privaten Cloud

1. Rufen Sie das VMware Engine-Portal auf.
2. Klicken Sie auf der VMware Engine-Homepage auf **Create a private cloud**. Der Hostingstandort und die Hardwareknotentypen werden aufgeführt.
3. Wählen Sie die Anzahl der Knoten für die private Cloud aus. Mindestens drei Knoten sind erforderlich.
4. Geben Sie einen CIDR-Bereich für das VMware-Verwaltungsnetzwerk ein.
5. Geben Sie einen CIDR-Bereich für das HCX-Bereitstellungsnetzwerk ein.

   > **Wichtig:**
   >
   > Der CIDR-Bereich darf sich mit keinem Ihrer On-Premises- oder Cloudsubnetze überschneiden. Der CIDR-Bereich muss /27 oder höher sein.

6. Wählen Sie **Review and create**.
7. Prüfen Sie die Einstellungen. Um Einstellungen zu ändern, klicken Sie auf **Back**.

8. Klicken Sie auf **Create**, um die private Cloud zu erstellen.

Beim Erstellen der privaten Cloud stellt VMware Engine VMware-Komponenten bereit und richtet erste Autoscale-Richtlinien für Cluster in der privaten Cloud ein. Die Erstellung einer privaten Cloud kann eine halbe bis zwei Stunden dauern. Nach Abschluss des Vorgangs erhalten Sie eine E-Mail.

Einrichten des Google Cloud VMware Engine-VPN-Gateways Um eine erste Verbindung zu Google Cloud VMware Engine herzustellen, können Sie ein VPN-Gateway verwenden. Es handelt sich um ein OpenVPN-basiertes Client-VPN, mit dem Sie eine Verbindung zu Ihrem VMware Software Defined Data Center vCenter herstellen und jede erforderliche Erstkonfiguration vornehmen können.

Konfigurieren Sie vor Bereitstellung des VPN-Gateways den **Edge Services**-Bereich für die Region, in der Ihr SDDC bereitgestellt wird. Gehen Sie hierzu folgendermaßen vor:

1. Melden Sie sich beim **Google Cloud VMware Engine**-Portal an und gehen Sie zu **Network > Regional Settings**. Klicken Sie auf **Add Region**.
2. Wählen Sie die Region, in der Ihr SDDC bereitgestellt wird, und aktivieren Sie **Internet Access** sowie **Public IP Service**.
3. Geben Sie den bei der Planung notierten Edge Services-Bereich an, und klicken Sie auf **Submit**. Die Aktivierung dieser Services dauert 10—15 Minuten.

   Sobald der Vorgang abgeschlossen ist, werden die Edge Services auf der Seite "Regional Settings"als **Enabled** angezeigt. Durch die Aktivierung dieser Einstellungen können Ihrem SDDC öffentliche IPs zugewiesen werden, was für die Bereitstellung eines VPN-Gateways erforderlich ist.

Gehen Sie zum Bereitstellen eines VPN-Gateways folgendermaßen vor:

1. Gehen Sie im **Google Cloud VMware Engine**-Portal zu **Network > VPN Gateways**. Klicken Sie auf **Create New VPN Gateway**.
2. Geben Sie den Namen für das VPN-Gateway und das bei der Planung reservierte Clientsubnetz an. Klicken Sie auf **Weiter**.
3. Wählen Sie Benutzer aus, die VPN-Zugriff erhalten sollen. Klicken Sie auf **Weiter**.
4. Geben Sie die Netzwerke an, die für das VPN zugänglich sein müssen. Klicken Sie auf **Weiter**.
5. Eine Zusammenfassung wird angezeigt. Überprüfen Sie die Auswahl und klicken Sie auf **Submit**, um das VPN-Gateway zu erstellen. Die Seite "VPN Gateways"wird angezeigt, der Status des neuen VPN-Gateways lautet **Creating**.
6. Wenn der Status in **Operational** wechselt, klicken Sie auf das neue VPN-Gateway.
7. Klicken Sie auf **Download my VPN configuration**, um eine ZIP-Datei mit vorkonfigurierten OpenVPN-Profilen für das VPN-Gateway herunterzuladen. Es stehen Profile für die Verbindung

über UDP/1194 und TCP/443 zur Verfügung. Importieren Sie die bevorzugte Option in Open VPN und stellen Sie eine Verbindung her.

8. Gehen Sie zu **Resources** und wählen Sie Ihr SDDC aus.

VPN verbinden

1. Stellen Sie über das VPN-Gateway-Setup eine Point-to-Site-Verbindung zwischen Ihrem On-Premises-Netzwerk und der privaten Cloud her. Siehe Einrichten des Google Cloud VMware Engine-VPN-Gateways.
2. Laden Sie die VPN-Konfiguration hoch, die Sie unter Einrichten des Google Cloud VMware Engine-VPN-Gateways heruntergeladen haben.
3. Importieren Sie sie in Ihren VPN-Client, zum Beispiel OpenVPN Connect.

Weitere Informationen finden Sie unter Verbindung über VPN herstellen.

Erstellen des ersten Subnetzes

Zugriff auf NSX-T Manager über das VMware Engine-Portal Das Subnetz wird in NSX-T erstellt, auf das Sie über VMware Engine zugreifen. Gehen Sie wie folgt vor, um auf NSX-T Manager zuzugreifen.

1. Melden Sie sich beim **Google Cloud VMware Engine**-Portal an.
2. Rufen Sie im Hauptmenü **Resources** auf.
3. Klicken Sie unter **Private cloud name** auf die private Cloud, in der Sie das Subnetz erstellen möchten.
4. Klicken Sie auf der Detailseite der privaten Cloud auf die Registerkarte **vSphere Management Network**.
5. Klicken Sie auf den **FQDN** des NSX-T Managers.
6. Wenn Sie dazu aufgefordert werden, geben Sie Ihre Anmeldeinformationen ein. Wenn Sie vIDM eingerichtet und mit einer Identitätsquelle wie Active Directory verbunden haben, verwenden Sie stattdessen Ihre Anmeldeinformationen für diese Identitätsquelle.

   > **Erinnerung:**
   >
   > Sie können generierte Anmeldeinformationen von der Detailseite der privaten Cloud abrufen.

Einrichten von DHCP für das Subnetz Bevor Sie ein Subnetz erstellen können, richten Sie einen DHCP-Dienst ein:

In NSX-T Manager:

1. Gehen Sie zu **Network > DHCP**. Das Netzwerkdashboard zeigt an, dass der DHCP-Dienst ein Tier-0- und ein Tier-1-Gateway erstellt.
2. Klicken Sie auf **Add Server**, um mit dem Provisioning des DHCP-Servers zu beginnen.
3. Wählen Sie **DHCP** unter **Server Type** aus und geben Sie den Servernamen und die IP-Adresse an.
4. Klicken Sie auf **Save**, um den DHCP-Dienst zu erstellen.

Gehen Sie wie folgt vor, um den DHCP-Dienst dem Tier-1-Gateway anzufügen. Ein standardmäßiges Tier-1-Gateway wurde bereits vom DHCP-Dienst bereitgestellt:

1. Wählen Sie **Tier-1 Gateways** aus. Wählen Sie dann die vertikalen Auslassungspunkte für das Tier-1-Gateway und anschließend **Edit** aus.
2. Wählen Sie im Feld **IP Address Management** die Option **No IP Allocation Set**.
3. Wählen Sie **DHCP Local Server** unter **Type** aus.
4. Wählen Sie den unter **DHCP Server** erstellten DHCP-Server.
5. Klicken Sie auf **Speichern**.
6. Klicken Sie auf **Close Editing**.

Sie können jetzt ein Netzwerksegment in NSX-T erstellen. Weitere Informationen zu DHCP in NSX-T finden Sie in der VMware-Dokumentation für DHCP.

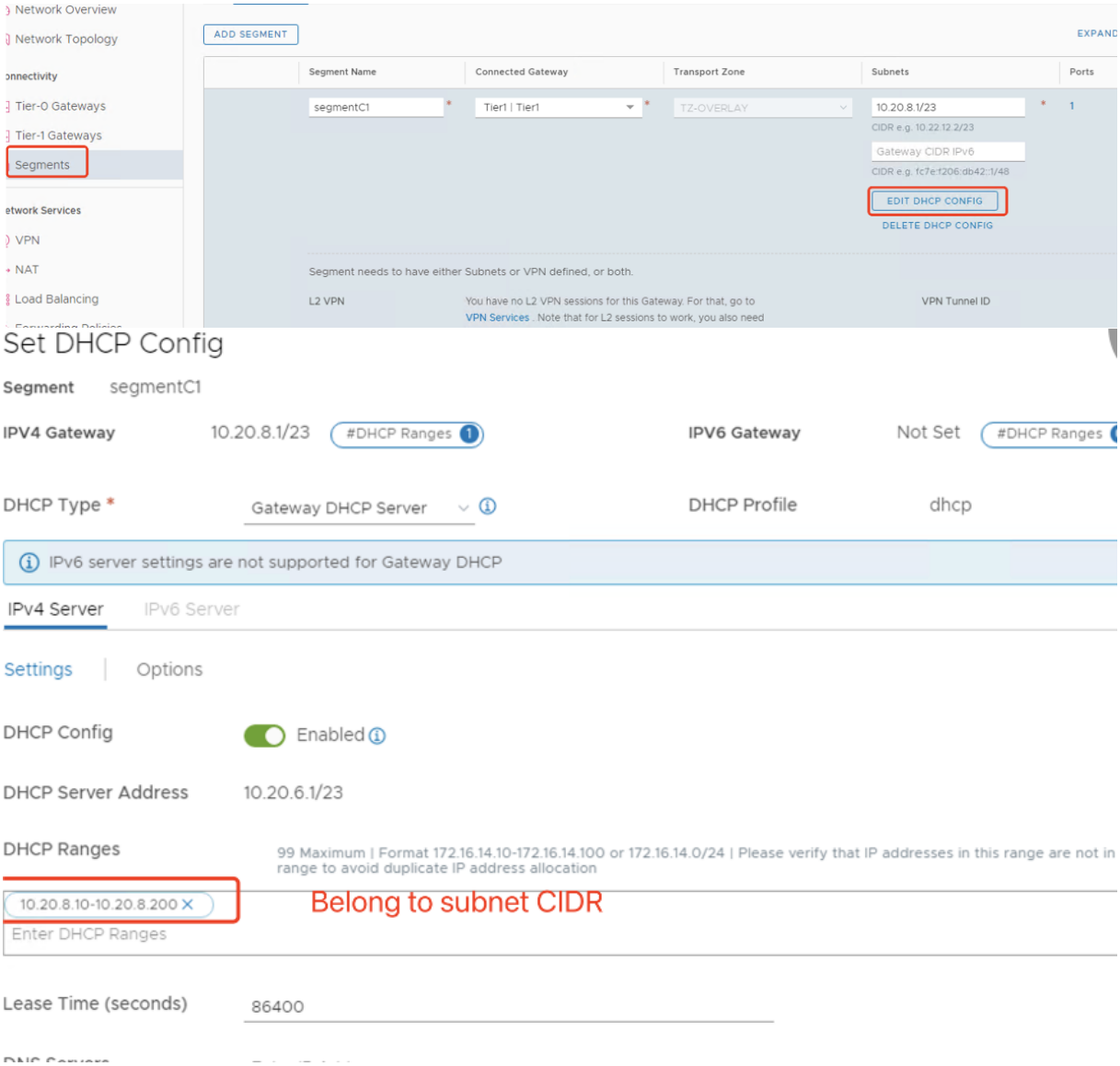
Erstellen eines Netzwerksegments in NSX-T Für Workload-VMs erstellen Sie Subnetze als NSX-T-Netzwerksegmente für Ihre private Cloud:

1. Gehen Sie in NSX-T Manager zu **Networking > Segments**.
2. Klicken Sie auf **Add Segment**.
3. Geben Sie einen Namen für das Segment ein.
4. Wählen Sie unter **Connected Gateway** die Option **Tier-1** und übernehmen Sie als Typ die Option **Flexible**.
5. Klicken Sie auf **Set Subnets**.
6. Klicken Sie auf **Add Subnets**.
7. Geben Sie unter **Gateway IP/Prefix Length** den Subnetzbereich ein. Geben Sie den Subnetzbereich mit **.1** als letztes Oktett an. Beispiel: **10.12.2.1/24**.
8. Geben Sie die DHCP-Bereiche ein und klicken Sie auf **ADD**.
9. Wählen Sie in **Transport Zone** in der Dropdownliste **TZ-OVERLAY**.
10. Klicken Sie auf **Speichern**. Sie können das Netzwerksegment jetzt in vCenter auswählen, wenn Sie eine VM erstellen.

Sie können pro Region maximal 100 einmalige Routen von VMware Engine zu Ihrem VPC-Netzwerk mit Zugriff auf private Dienste einrichten. Dazu gehören beispielsweise IP-Adressbereiche für die Verwal-

tung der privaten Cloud, NSX-T-Workload-Netzwerksegmente und HCX-Netzwerk-IP-Adressbereiche. Dieses Limit umfasst alle privaten Clouds in der Region.

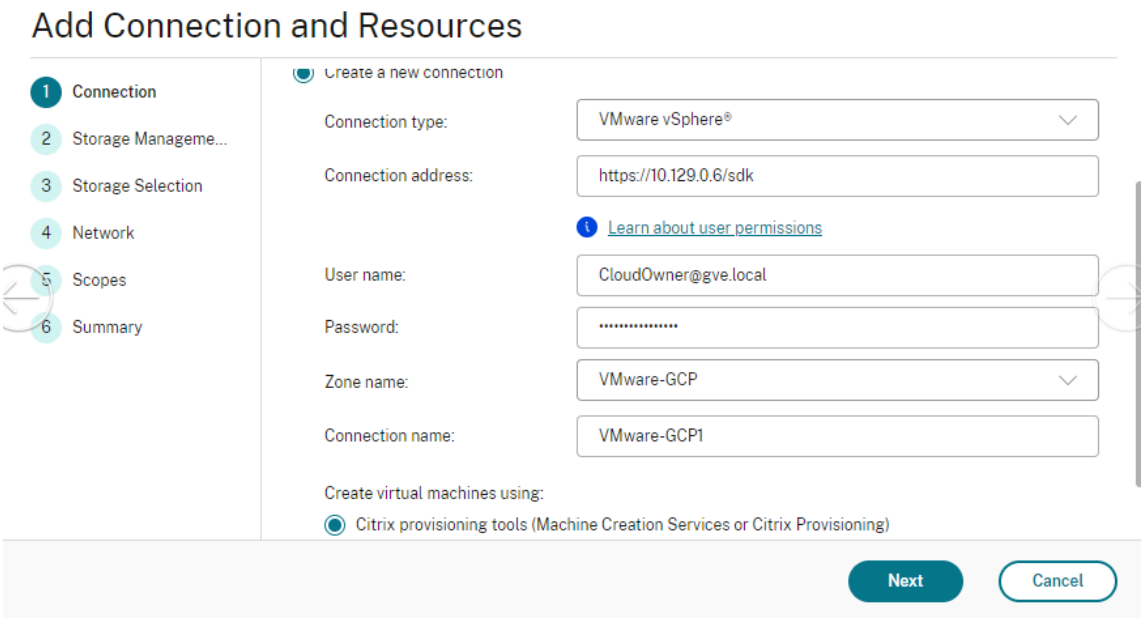
> **Hinweis:**
>
> Aufgrund eines Google Cloud-Konfigurationsproblems müssen Sie die DHCP-Bereiche mehrmals konfigurieren. Konfigurieren Sie daher die DHCP-Bereichseinstellung nach der Google Cloud-Konfiguration. Klicken Sie auf **EDIT DHCP CONFIG**, um die DHCP-Bereiche zu konfigurieren.



Erstellen der Google Cloud-VMware-Verbindung in Citrix Studio

1. Erstellen Sie eine Maschine in vCenter.
2. Starten Sie Citrix Studio.

3. Wählen Sie den Hostingknoten und klicken Sie auf **Verbindung und Ressourcen hinzufügen**.
4. Wählen Sie auf der Seite **Verbindung** die Option **Neue Verbindung erstellen** und machen Sie folgenden Eingaben:



   a) Wählen Sie für **Verbindungstyp** die Option **VMware vSphere**.
   b) Geben Sie unter **Verbindungsadresse** die private vCenter-IP-Adresse ein.
   c) Geben Sie die vCenter-Anmeldeinformationen ein.
   d) Geben Sie einen Verbindungsnamen ein.
   e) Wählen Sie das Tool zum Erstellen virtueller Maschinen aus.

5. Wählen Sie auf der Seite **Netzwerk** das auf dem NSX-T-Server erstellte Subnetz aus.
6. Schließen Sie den Assistenten ab.

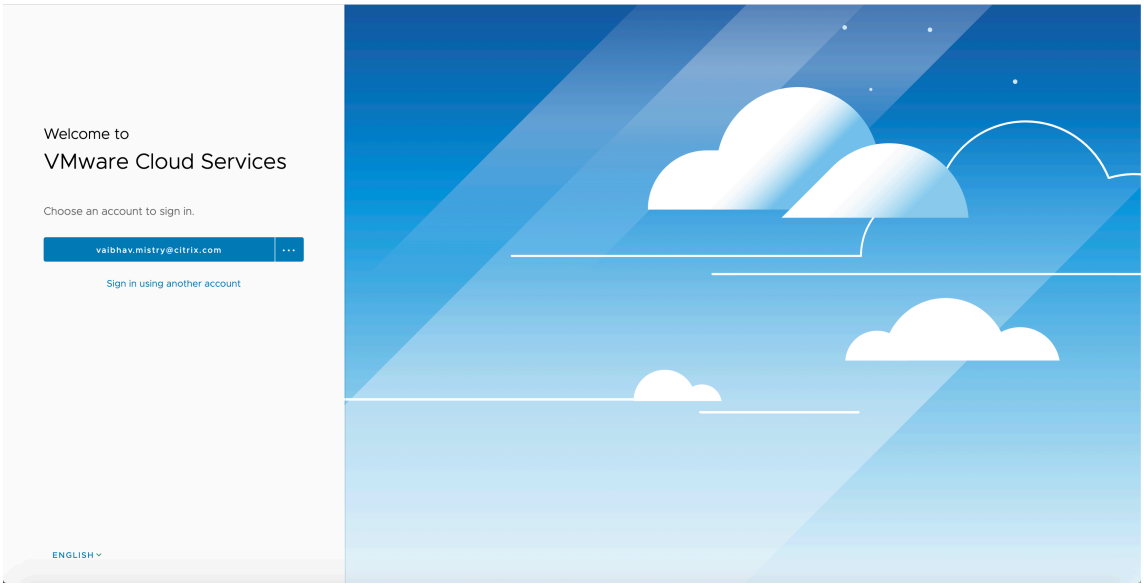
VMware-Cloud auf Amazon Web Services (AWS)

Mit VMware-Cloud auf Amazon Web Services (AWS) können Sie VMware-basierte, on-premises bereitgestellte Citrix Workloads zur AWS-Cloud migrieren.

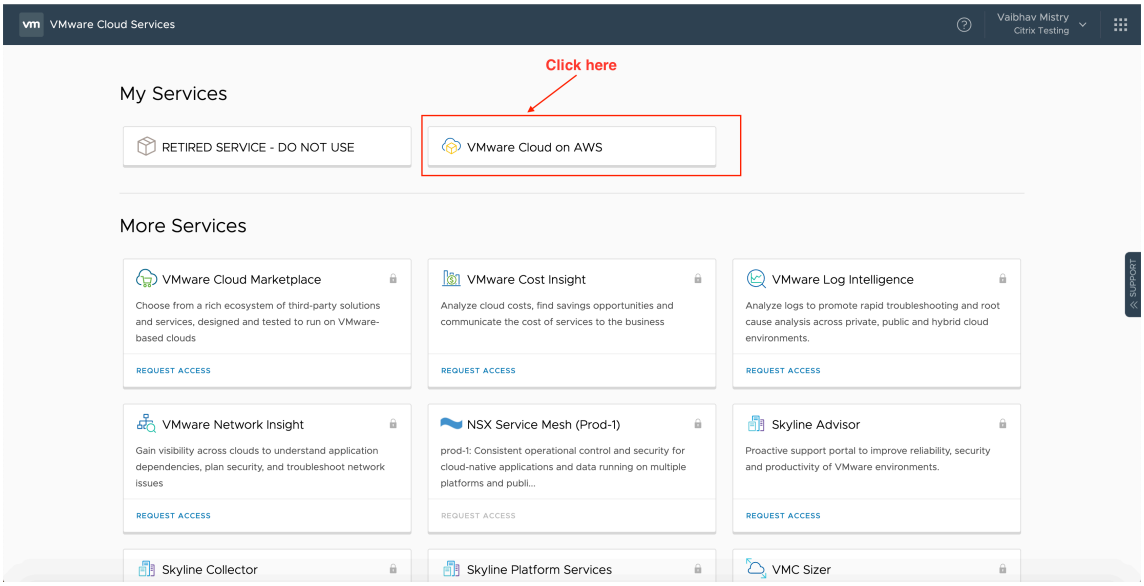
In diesem Artikel wird das Verfahren zum Einrichten einer VMware-Cloud auf AWS beschrieben.

Zugriff auf die VMware-Cloudumgebung

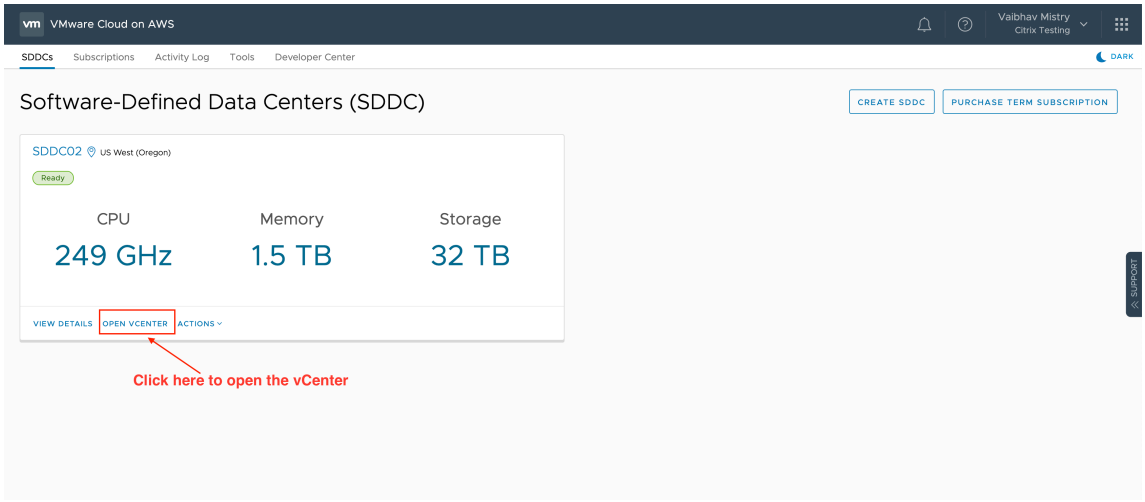
1. Melden Sie sich mit der URL https://console.cloud.vmware.com/ bei den VMware-Clouddiensten an.

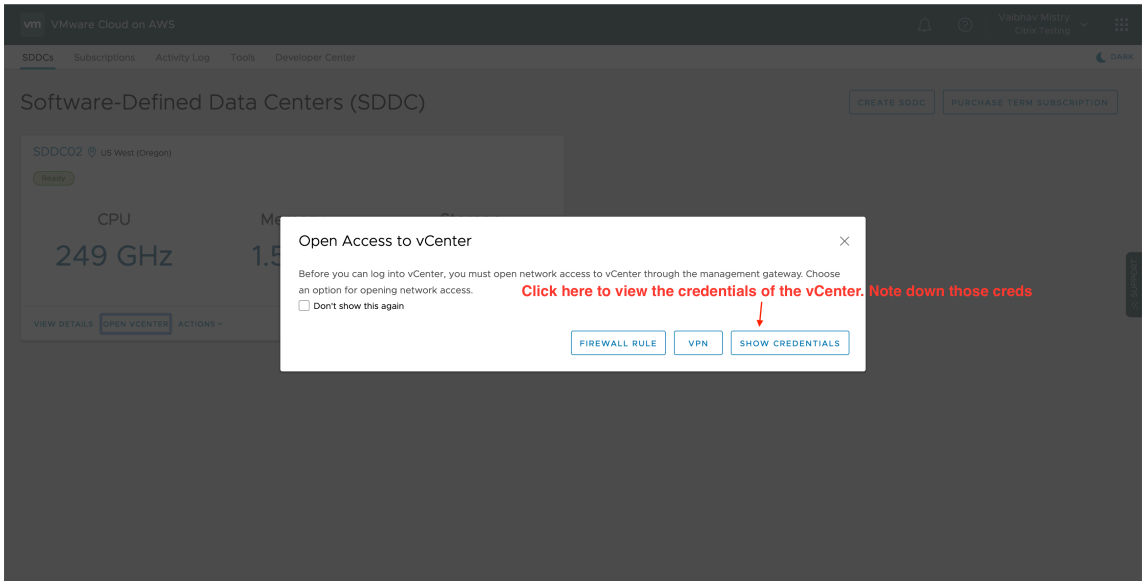


2. Klicken Sie auf **VMware Cloud on AWS**. Die Seite “Software-Defined Data Centers (SDDC)”wird angezeigt.

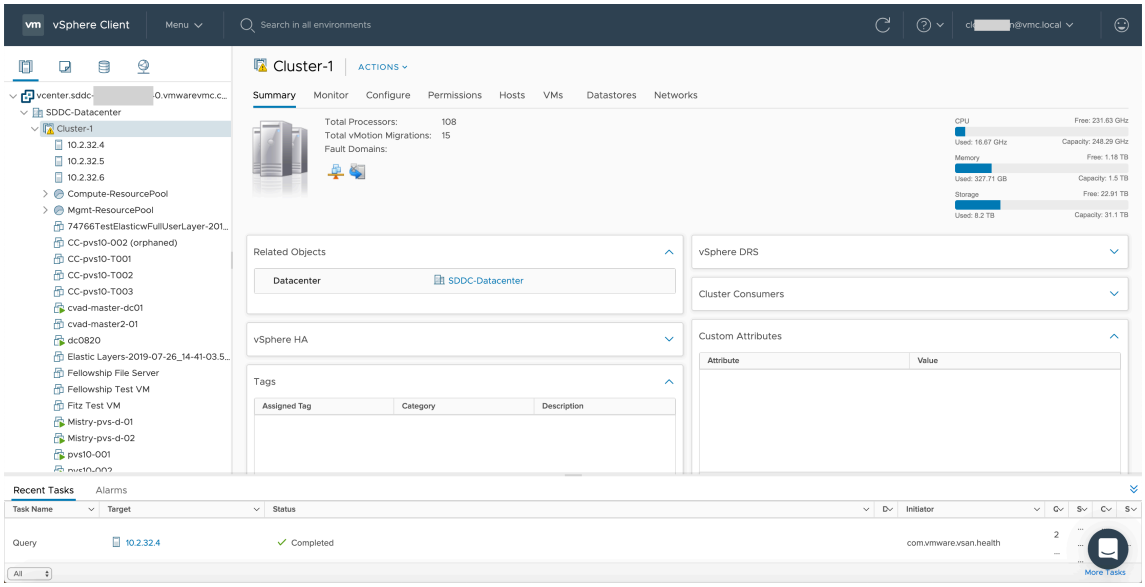


3. Klicken Sie auf **OPEN VCENTER** und dann auf **SHOW CREDENTIALS**. Notieren Sie sich die Anmeldeinformationen zur späteren Verwendung.





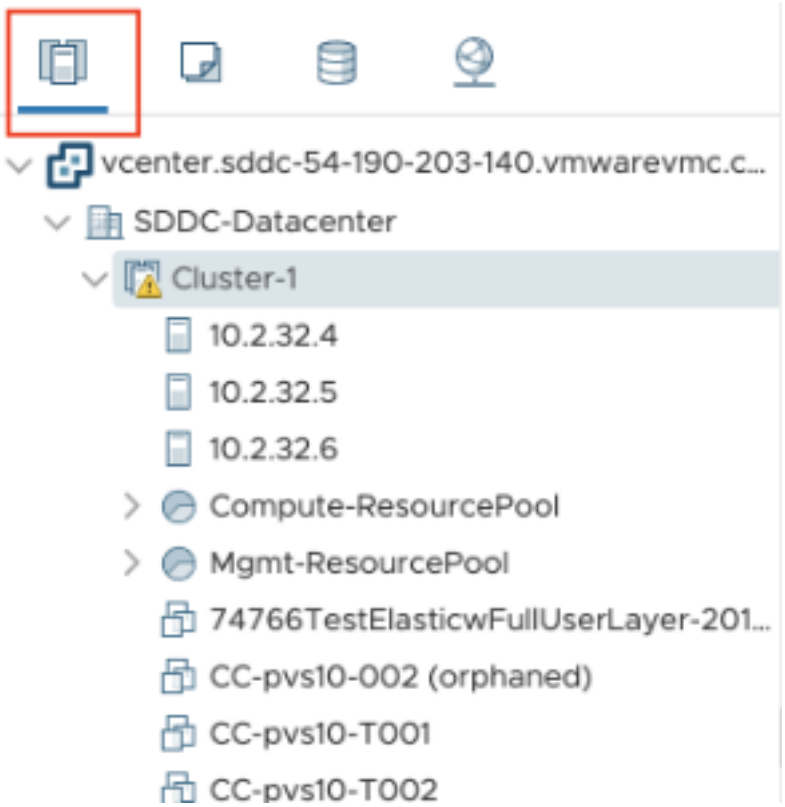
4. Öffnen Sie einen Webbrowser und geben Sie die URL für den vSphere Web Client ein.
5. Geben Sie die zuvor notierten Anmeldeinformationen ein und klicken Sie auf **Login**. Die Webseite des vSphere-Clients ähnelt der On-Premises-Umgebung.



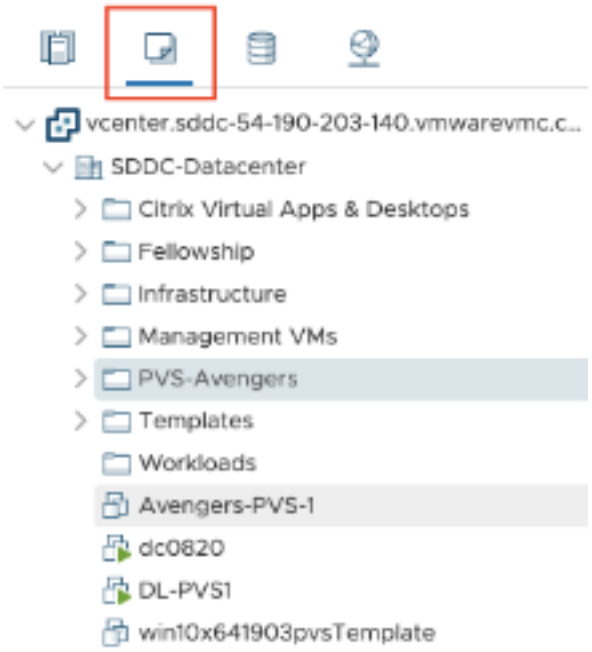
Informationen zur VMware-Cloudumgebung

Auf der Webseite des vSphere-Clients gibt es vier Ansichten.

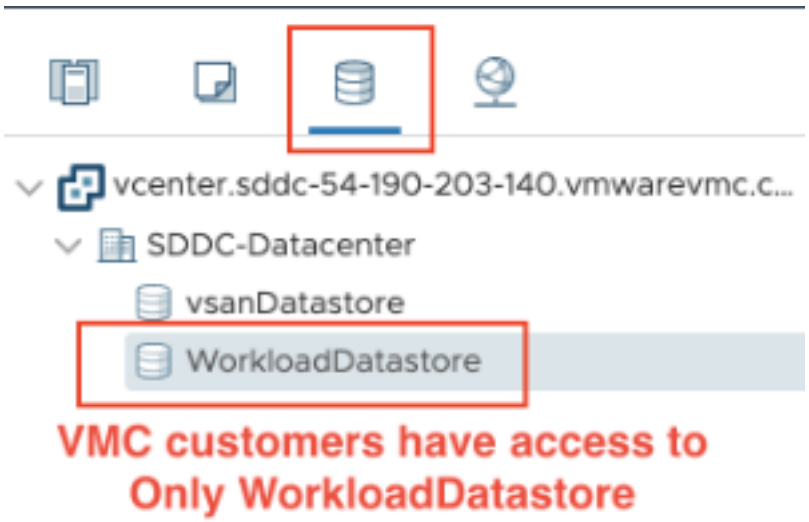
- Host- und Clusteransicht: Sie können keinen neuen Cluster erstellen, der Cloudadministrator kann jedoch mehrere Ressourcenpools erstellen.



- VM- und Vorlagenansicht: Der Cloudadministrator kann viele Ordner erstellen.



- Speicheransicht: Wählen Sie den Speicher **WorkloadDatastore**, wenn Sie eine Hosteinheit in Citrix Studio hinzufügen, da Sie nur Zugriff auf Workload Datastore haben.



- Netzwerkansicht: Die Symbole für VMware-Cloudnetzwerke und Opaque-Netzwerke sind unterschiedlich.

Nach dem Einrichten des Clusters finden Sie unter VMware-Virtualisierungsumgebungen weitere Informationen zum Hinzufügen von Verbindungen und Ressourcen.

So geht es weiter

- Kernkomponenten installieren
- VDAs installieren

- Site erstellen
- Informationen zum Erstellen und Verwalten einer Verbindung finden Sie unter Verbindung zu VMware-Cloud und Partnerlösungen.

Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Maschinenkataloge erstellen

Kernkomponenten installieren

June 27, 2024

> **Wichtig:**
>
> Citrix erfasst grundlegende Lizenzierungsdaten, soweit dies für Citrix' legitime Interessen, einschließlich Lizenz-Compliance, erforderlich ist. Weitere Informationen finden Sie unter Daten zur Citrix Lizenzierung.

Die Kernkomponenten sind der Citrix Delivery Controller, Citrix Studio, Web Studio, Citrix Director und Citrix Lizenzserver.

> **Hinweis:**
>
> Citrix Studio ist eine Windows-basierte Verwaltungskonsole, mit der Sie On-Premises-Bereitstellungen von Citrix Virtual Apps and Desktops konfigurieren und verwalten. Web Studio hebt Citrix Studio auf die nächste Stufe –als webbasierte Verwaltungskonsole, die sämtliche Funktionen von Citrix Studio bietet. Weitere Informationen zu Web Studio finden Sie unter Web Studio installieren.

(In Versionen vor 2003 gehört Citrix StoreFront zu den Kernkomponenten. Sie können StoreFront weiterhin installieren, indem Sie auf die Kachel **Citrix StoreFront** klicken 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: Produktsoftware herunterladen und Assistent starten

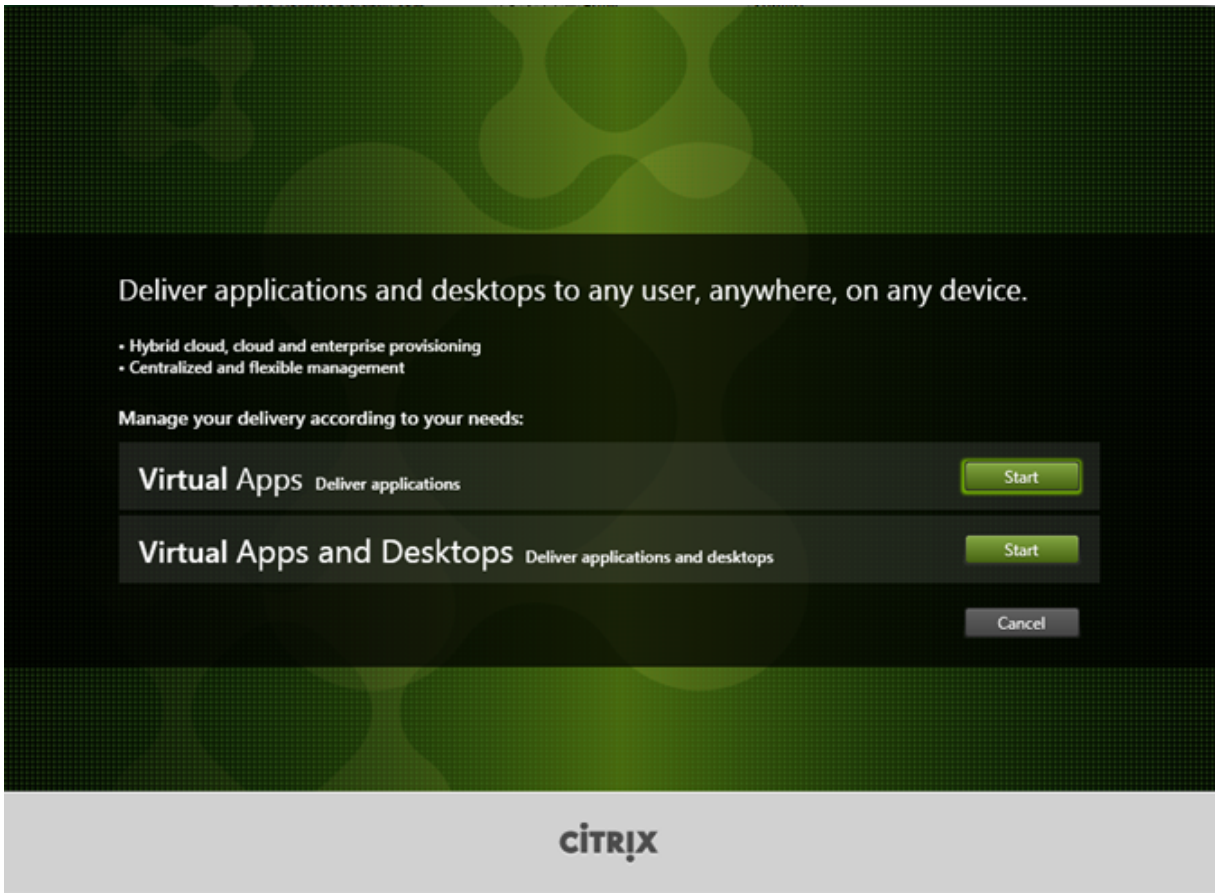
Rufen Sie unter Angabe Ihrer Citrix Anmeldeinformationen die Citrix Virtual Apps and Desktops-Downloadseite auf. Laden Sie die ISO-Datei für das Produkt herunter.

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: Zu installierendes Produkt auswählen

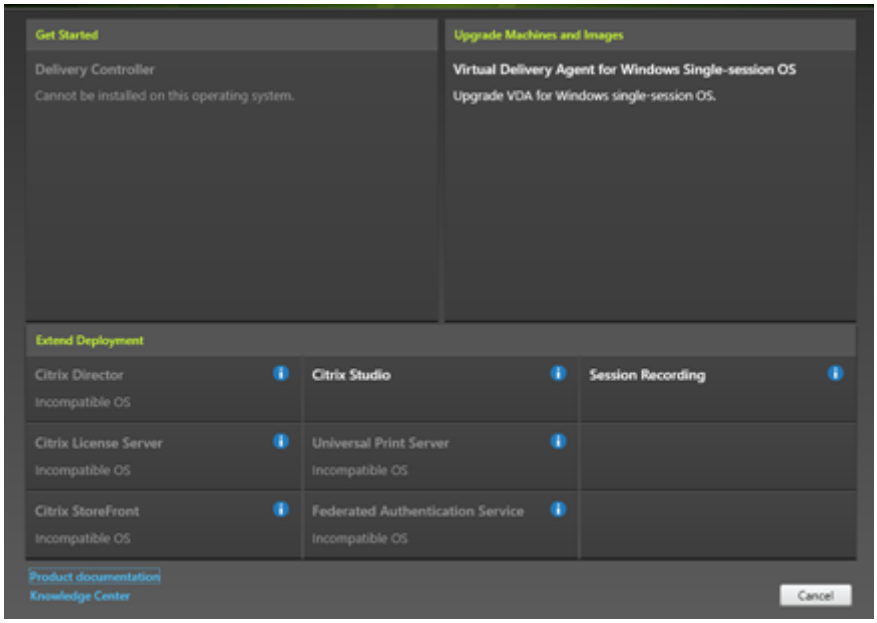


Klicken Sie auf **Start** neben dem zu installierenden Produkt: Virtual Apps oder Virtual Apps and Desktops.

(Wenn auf der Maschine bereits Citrix Virtual Apps and Desktops-Komponenten installiert sind, wird diese Seite nicht angezeigt.)

Befehlszeilenoption: `/xenapp` zum Installieren von Citrix Virtual Apps. Wenn diese Option ausgelassen wird, wird Citrix Virtual Apps and Desktops installiert.

Schritt 3: Auswählen der zu installierenden Komponente

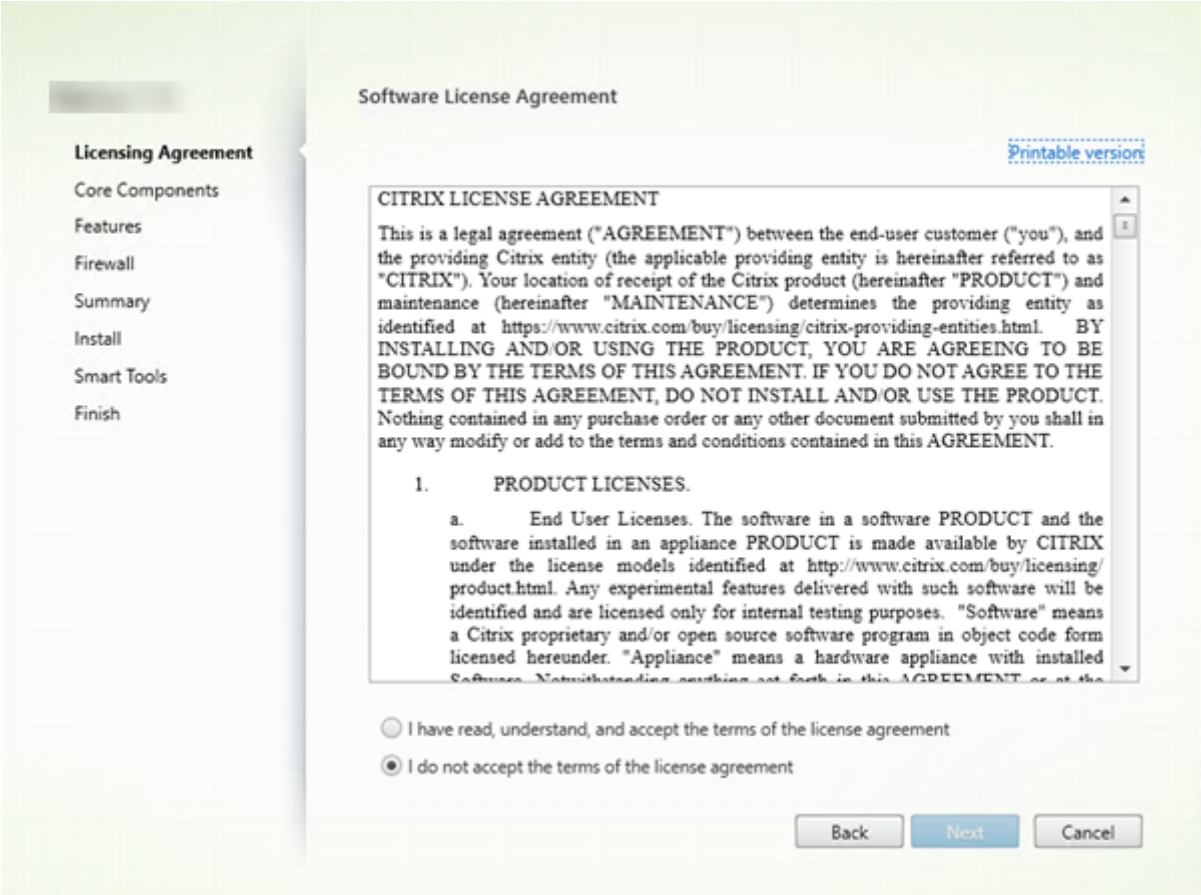


Wenn Sie ganz zu Beginn der Installation stehen, wählen Sie **Delivery Controller**. (Später wählen Sie die spezifischen Komponenten aus, die Sie auf dieser Maschine installieren.)

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.

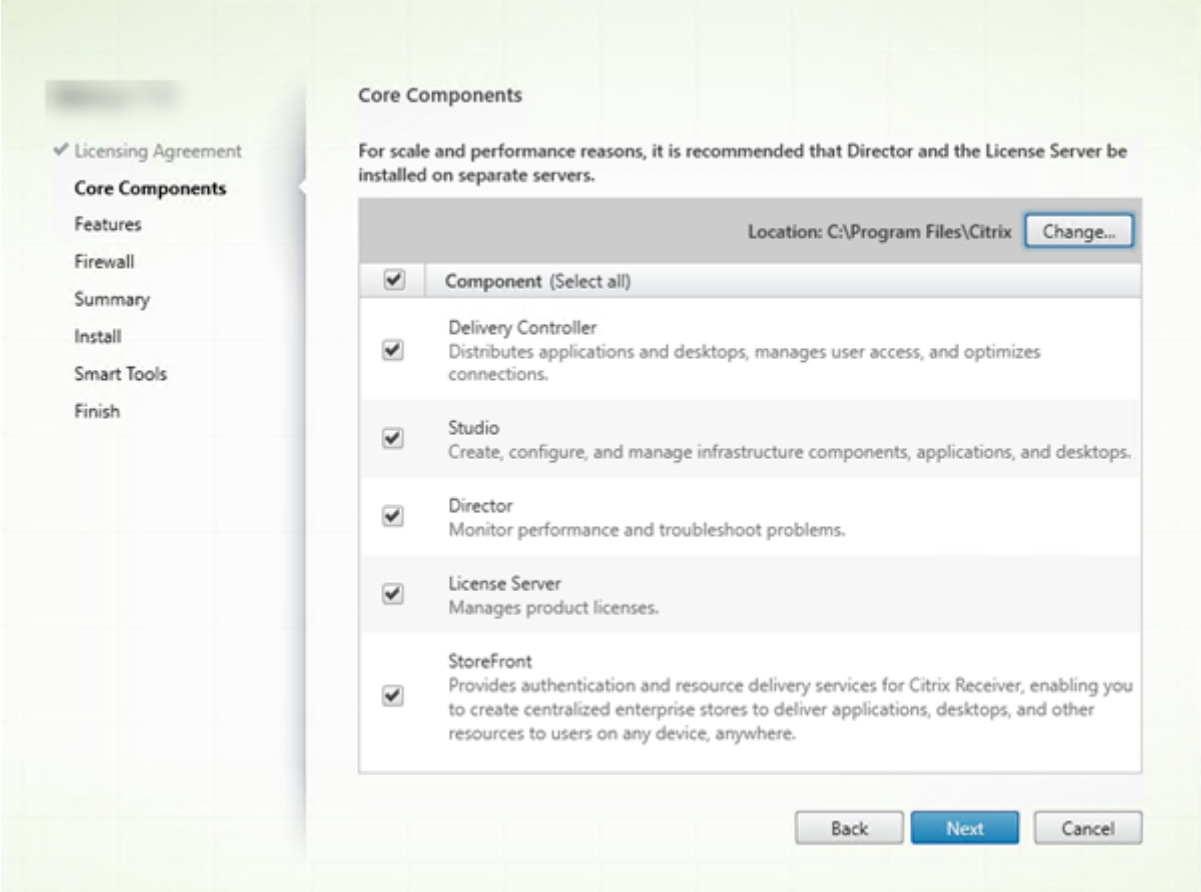
Befehlszeilenoption: `/components`

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:\Program Files\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, Secure Private Access und Lizenzserver auf eigenen Servern.

  > **Hinweis:**
  >
  > Wenn Sie Komponenten auf mehreren Servern installieren, installieren Sie zuerst den Citrix Lizenzserver und die Lizenzen, bevor Sie andere Komponenten auf anderen Servern installieren. Weitere Informationen finden Sie im Abschnitt “Automatische Installation”

> der Lizenzierungsdokumentation für Citrix Virtual Apps and Desktops.

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.

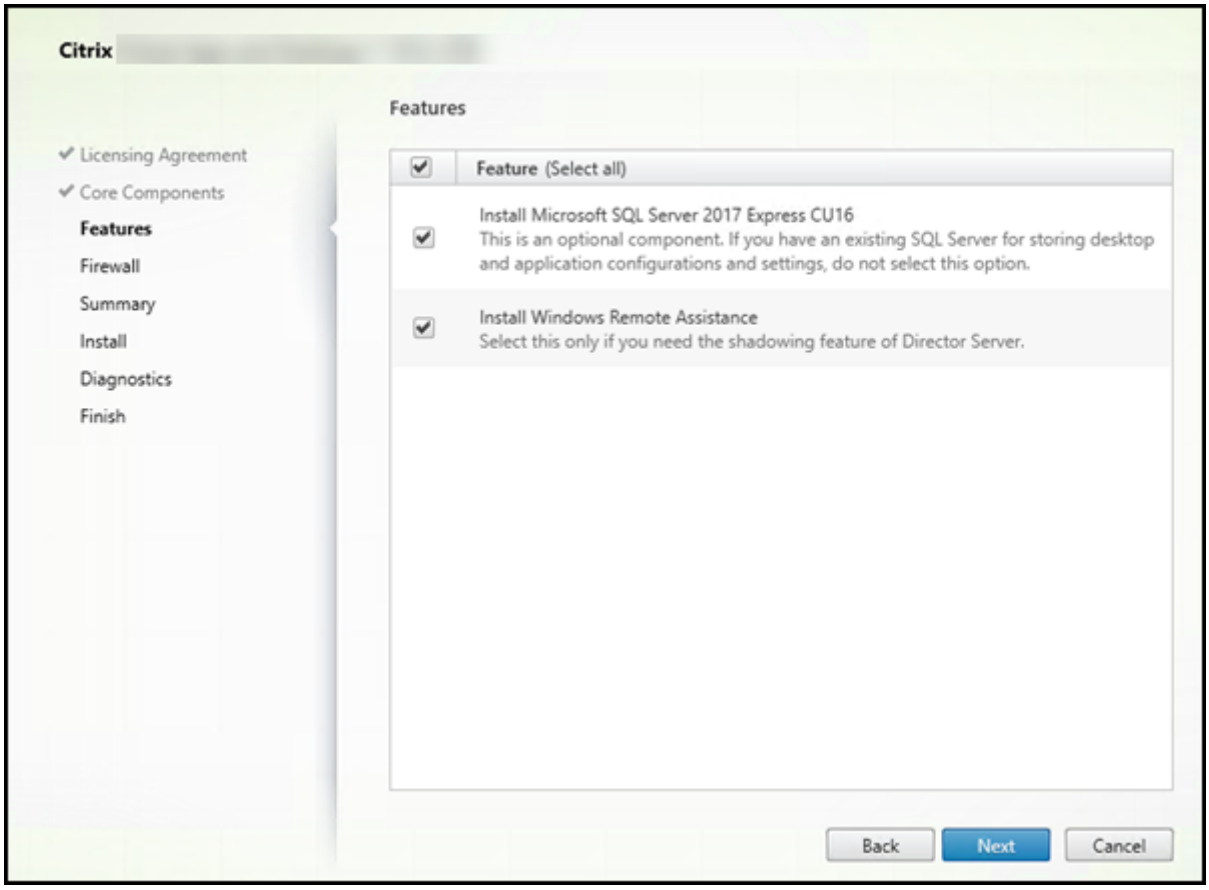
- Empfohlen: Klicken Sie auf **Abbrechen**, um die Installation abzubrechen. Installieren Sie mehr RAM auf der Maschine und starten Sie die Installation erneut.
- Sie können auch auf **Weiter** klicken, um mit der Installation fortzufahren. Die Site kann dann Stabilitätsprobleme haben.

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.

Beim Upgrade werden Sie außerdem benachrichtigt, wenn die Betriebssystem- oder SQL Server-Version nicht mehr unterstützt wird. Siehe Upgrade einer Bereitstellung.

Schritt 6: Aktivieren oder Deaktivieren von Features



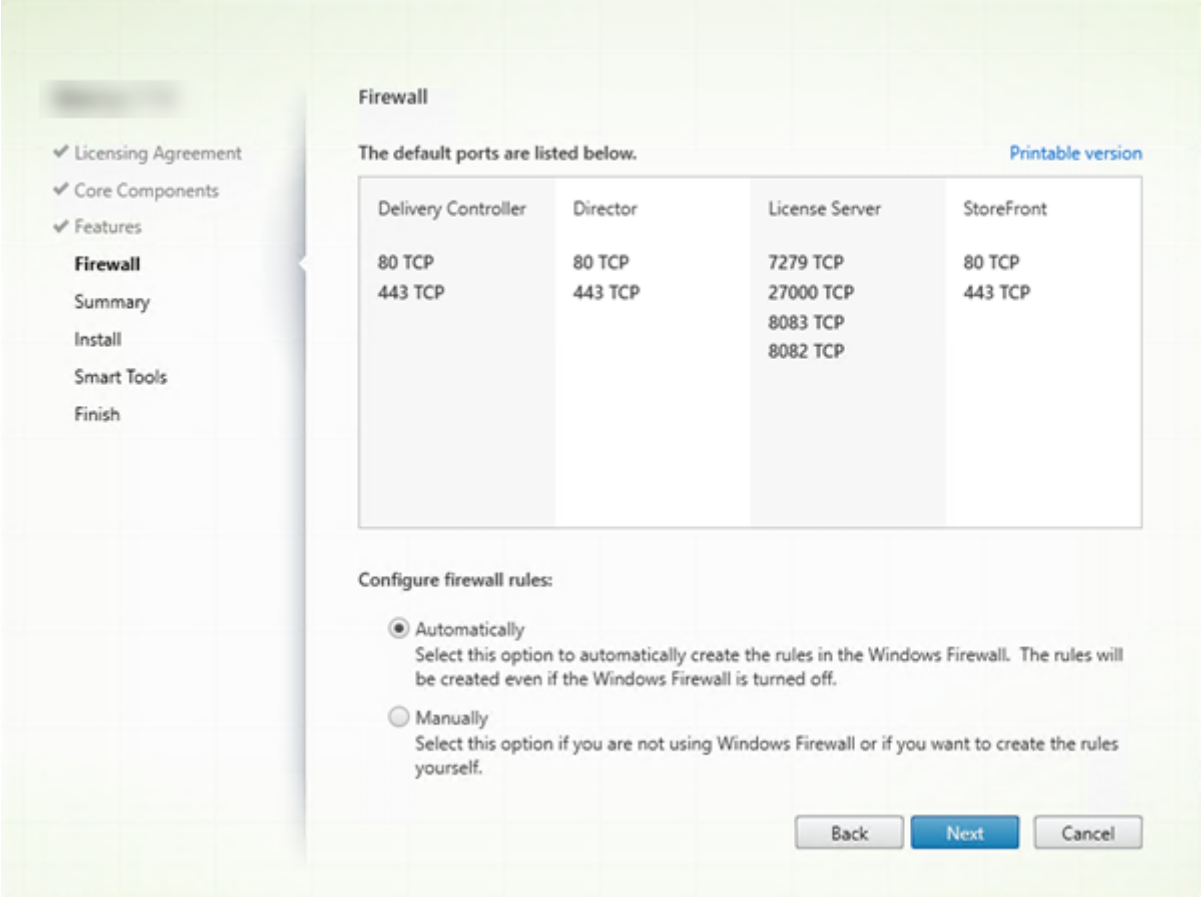
Auf der Seite **Features**:

- 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



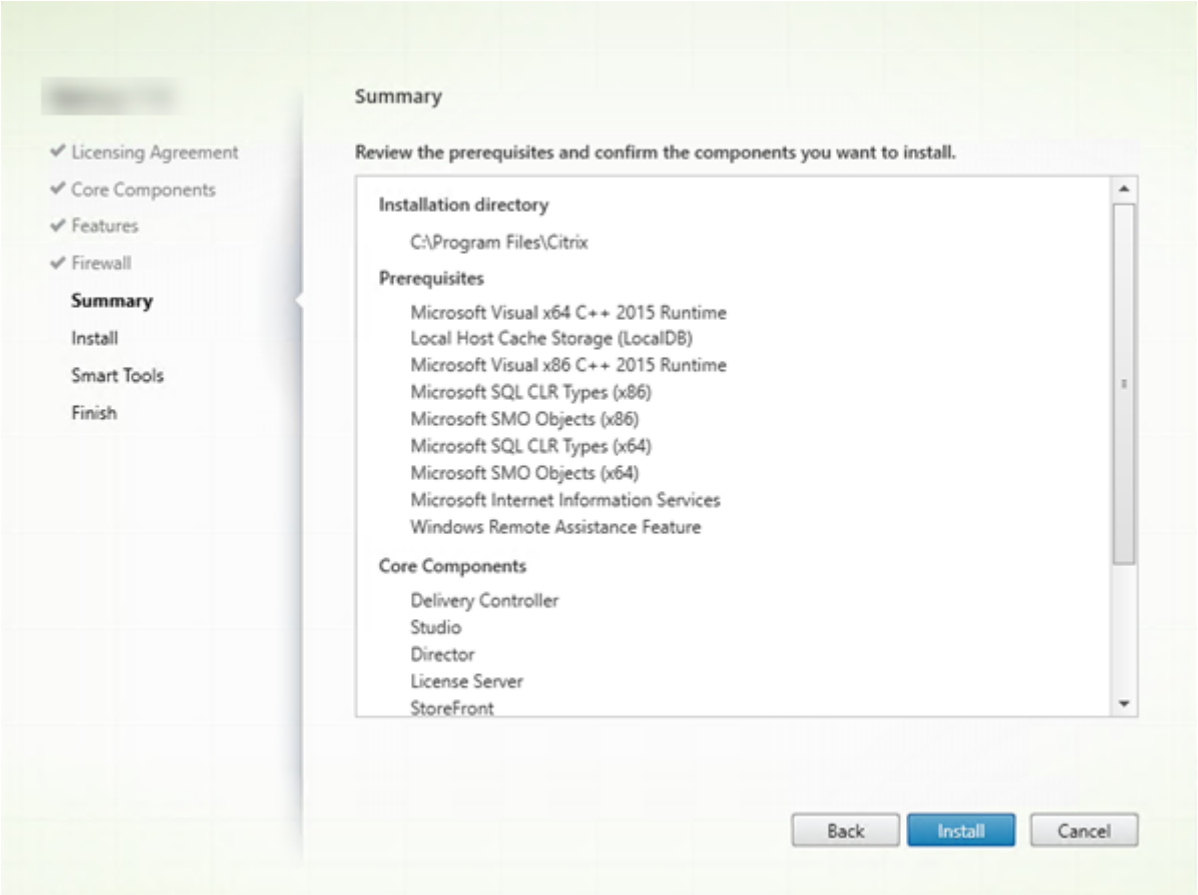
Standardmäßig werden die Ports auf der Seite **Firewall** automatisch geöffnet, wenn der Windows-Firewalldienst ausgeführt wird, selbst wenn die Firewall nicht aktiviert ist. Die Standardeinstellung ist für die meisten Bereitstellungen geeignet. Weitere Informationen zu Ports finden Sie unter Netzwerkports.

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 für Testzwecke durchgeführt.)

Befehlszeilenoption: `/configure_firewall`

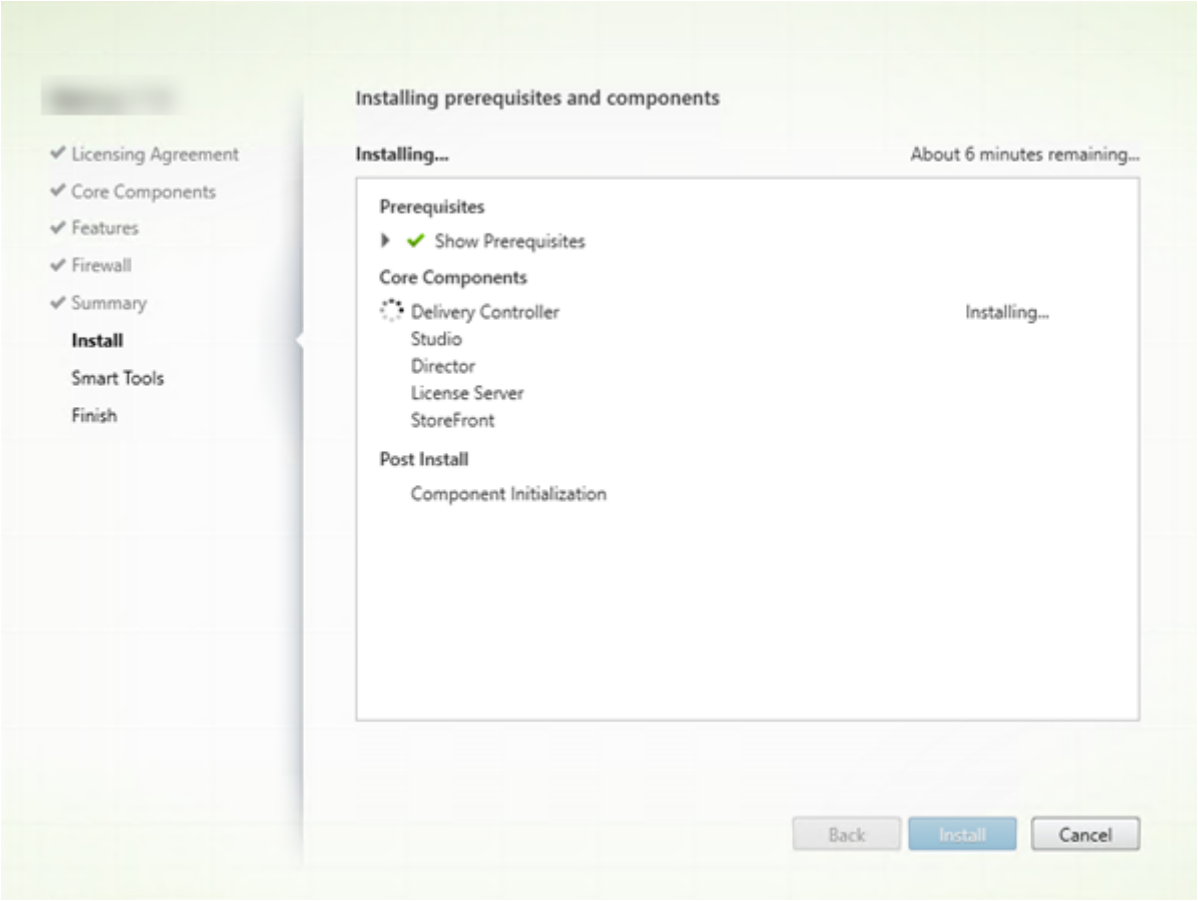
Schritt 8: Überprüfen der Voraussetzungen und Bestätigen der Installation



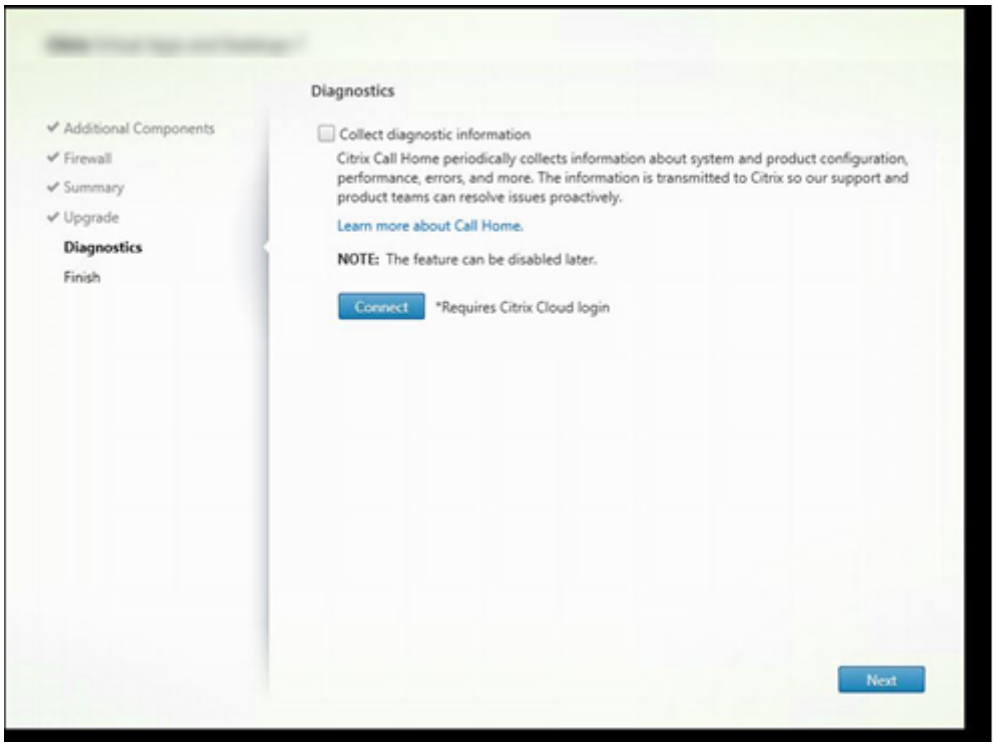
Auf der Seite **Zusammenfassung** wird aufgelistet, was installiert wird. Sie können mit der Schaltfläche **Zurück** zu vorherigen Seiten zurückkehren und Ihre Auswahl ändern.

Wenn Sie fertig sind, klicken Sie auf **Installieren**.

Der Fortschritt der Installation wird angezeigt.



Schritt 9: Teilen von Diagnoseinformationen mit Cloud Software Group



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.

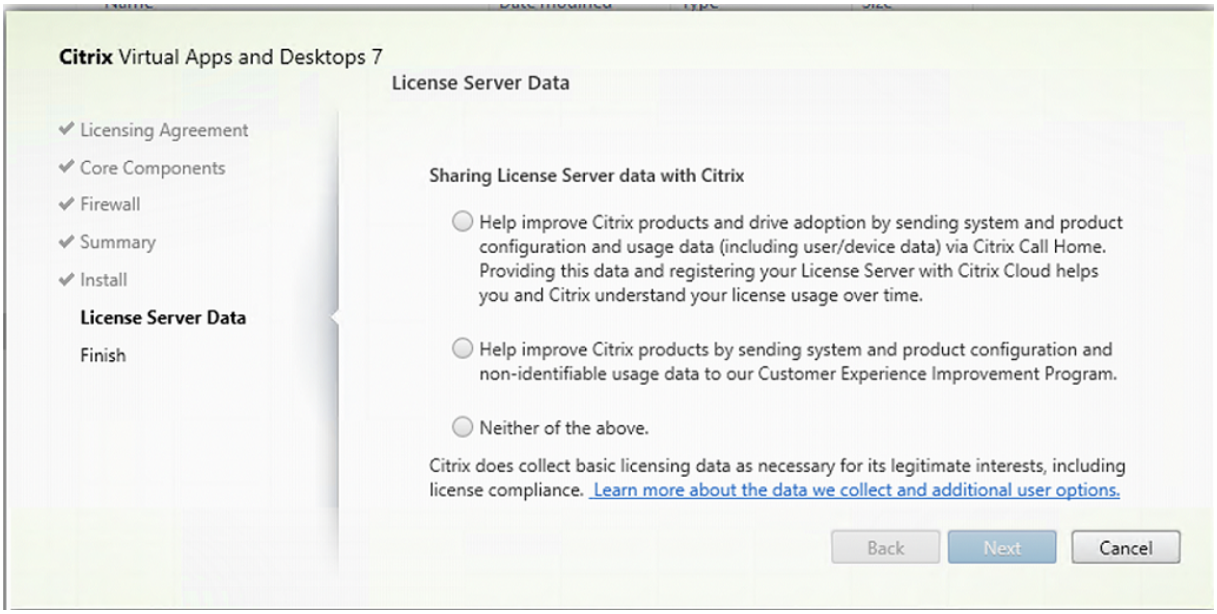
Wenn Sie teilnehmen möchten (Standardeinstellung), klicken Sie auf **Verbinden**. Geben Sie nach Aufforderung die Anmeldeinformationen Ihres Citrix-Kontos ein. Sie können die Registrierungsauswahl nach der Installation ändern.

Wenn Ihre Anmeldeinformationen überprüft sind (bzw. wenn Sie nicht teilnehmen), klicken Sie auf **Weiter**.

Wenn Sie 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. Die nächste Seite kann nicht aufgerufen werden. Um die Schaltfläche **Weiter** wieder zu aktivieren, aktivieren Sie die Option **Diagnoseinformationen sammeln** und deaktivieren Sie sie sofort wieder.

Weitere Informationen finden Sie unter Call Home.

Schritt 10: Teilen von Lizenzserverdaten mit Cloud Software Group



Auf der Seite **Lizenzserverdaten** bitten wir Sie, Daten von Call Home oder von CEIP (Programm zur Verbesserung der Benutzerfreundlichkeit) freizugeben, um uns zu unterstützen. Darüber werden allgemeine Lizenzdaten (einschließlich Daten zur Lizenzcompliance) durch Cloud Software Group erfasst, soweit dies für ihre berechtigten Interessen erforderlich ist.

Die Seite **Lizenzserverdaten** wird angezeigt, wenn Sie den Lizenzserver wie folgt installiert haben:

- Als eigenständiges Gerät.
- Als Kernkomponente bei der Installation eines Delivery Controller.

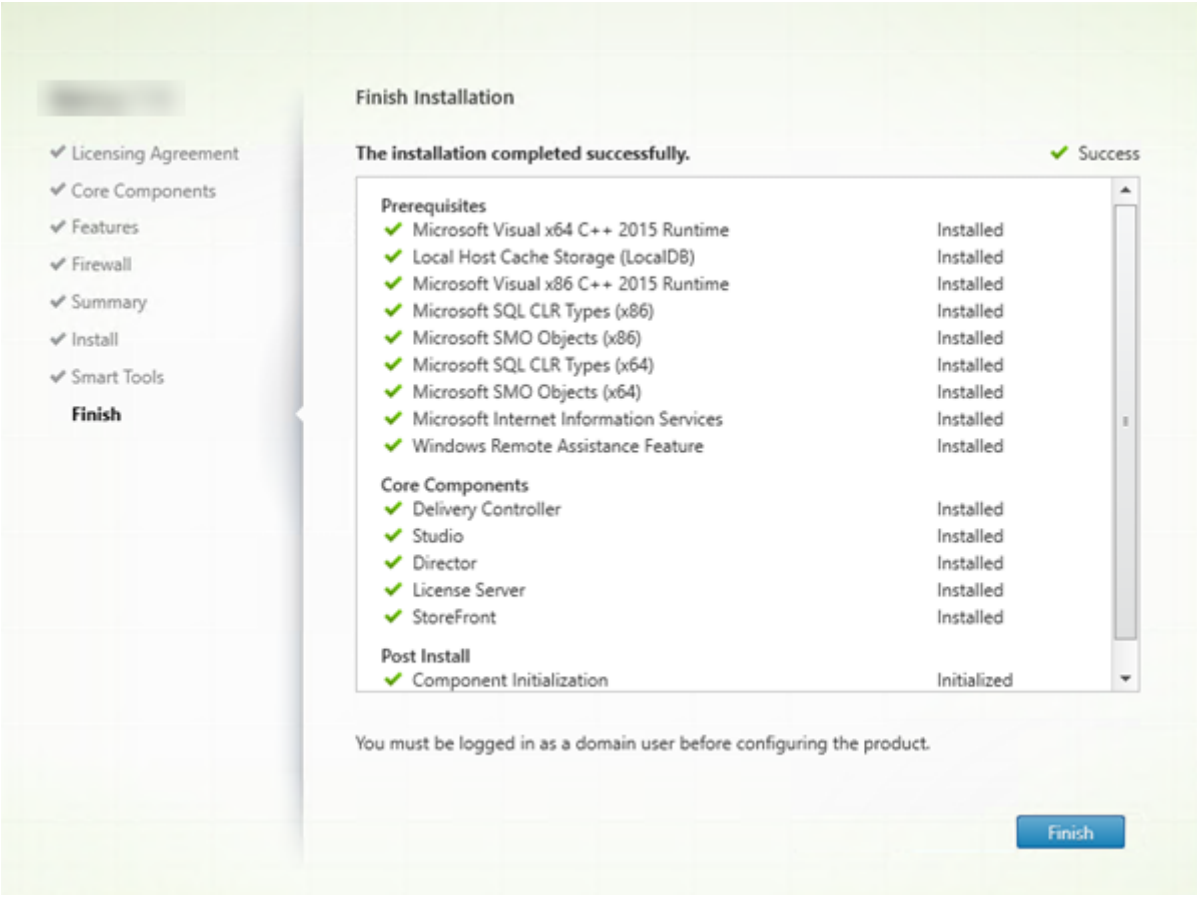
Während eines Upgrades wird diese Seite nicht angezeigt, wenn die Konfiguration bereits in der Datei `/CITRIX.opt`: festgelegt ist.

Der Lizenzserver überwacht verschiedene Arten von Benutzerdaten, z. B. Lizenzdaten, Call Home-Daten und CEIP-Daten. Die Datenerfassung für Call Home und CEIP müssen Sie selbst aktivieren.

Weitere Informationen zum Aktivieren der Datenerfassung für Call Home und CEIP bei der Installation über die Befehlszeile finden Sie unter Befehlszeilenoptionen zur Installation der Kernkomponenten.

Weitere Informationen zur Erfassung von Lizenzdaten durch Cloud Software Group finden Sie unter Datenerfassungsprogramme für die Citrix Lizenzierung.

Schritt 11: Abschließen der Installation



Die Seite **Fertigstellen** zeigt grüne Häkchen für alle Voraussetzungen und Komponenten, die erfolgreich installiert und initialisiert werden konnten.

Klicken Sie auf **Fertigstellen**.

Schritt 12: 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 Komponenten 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.

  1. Wählen Sie **Universeller Druckserver** im Bereich **Erweitern der Bereitstellung**.
  2. Akzeptieren Sie die Lizenzvereinbarung.
  3. 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 Befehlszeilenoptionen zum Installieren eines universellen Druckservers.

- Verbundauthentifizierungsdienst.
- Sitzungsaufzeichnung.
- Workspace Environment Management.

Installieren über die Befehlszeile

June 27, 2024

> **Wichtig:**
>
> - Wenn Sie ein Upgrade durchführen und die aktuelle Version verwendet die Software für persönliche vDisks oder AppDisks, bzw. diese Software ist installiert, lesen Sie den Abschnitt Entfernen von PvD, AppDisks und nicht unterstützten Hosts.
> - Citrix erfasst allgemeine Lizenzdaten, die für eigene berechtigte Interessen erforderlich sind, einschließlich Daten zur Lizenzcompliance. Weitere Informationen finden Sie unter Daten zur Citrix Lizenzierung.

Einführung

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 VDAs auf Maschinen in Active Directory. Weitere Informationen finden Sie unter Installieren von VDAs mit Skripts.

Wenn Sie die Installation bzw. ein Upgrade unter einem für diese Citrix Virtual Apps and Desktops-Version nicht unterstützten Betriebssystem versuchen, werden Sie durch eine Meldung zu Informationen über Ihre Optionen geleitet. Siehe Ältere Betriebssysteme.

Informationen dazu, wie Citrix die Ergebnisse 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 Verzeichnis `\x64\XenDesktop Setup` 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.

   VDA-Installation: Führen Sie `XenDesktopVDASetup.exe` mit den unter Befehlszeilenoptionen zur VDA-Installation beschriebenen Optionen aus.

   Gehen Sie zum Installieren von StoreFront folgendermaßen vor: Führen Sie `CitrixStoreFront-x64.exe` im Ordner `x64 > StoreFront` auf dem Installationsmedium 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 Sitzungsaufzeichnung: Folgen Sie den Anweisungen unter Sitzungsaufzeichnung.

Installieren von Workspace Environment Management: Folgen Sie den Anweisungen in Workspace Environment Management.

Installieren von Secure Private Access: Führen Sie `XenDesktopSPASetup.exe` im Ordner `x64 > XenDesktop` auf dem Installationsmedium aus. Folgen Sie den Anweisungen in den Befehlszeilenoptionen zur Installation eines Secure Private Access.

Befehlszeilenoptionen zur Installation der Kernkomponenten

Die folgenden Parameteroptionen sind bei Installation der Kernkomponenten mit dem Befehl `XenDesktopServerSetup.exe` zulässig. Weitere Informationen zu den Optionen finden Sie unter Installieren der Kernkomponenten.

- **/ceipoptin** *ceipoptin* [,*ceipoptin*] …

  Aktiviert die Datenerfassung für Call Home und das Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP). Gültige Werte:

  - `DIAGNOSTIC`: Bei Auswahl dieses Werts sammelt die Citrix Lizenzierung Call Home-Daten.
  - `ANONYMOUS`: Bei Auswahl dieses Werts sammelt die Citrix Lizenzierung nicht identifizierende CEIP-Daten (Daten, die den Benutzer nicht identifizieren).
  - `NONE`: Bei Auswahl dieses Werts ist die Erfassung von CEIP-Daten durch die Citrix Lizenzierung deaktiviert.

  Weitere Informationen zur Erfassung von Call Home-Daten finden Sie unter Call Home für die Citrix Lizenzierung.

  Weitere Informationen zur Erfassung von CEIP-Daten finden Sie unter Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) für die Citrix Lizenzierung.

  Weitere Informationen zu CEIP-Daten finden Sie unter CEIP-Datenelemente für die Citrix Lizenzierung.

  Weitere Informationen zu Lizenzserver-Lizenzdaten finden Sie unter Daten zur Citrix Lizenzierung.

- **/components** *component* [,*component*] …

  Durch Trennzeichen getrennte Liste der zu installierenden oder zu entfernenden Komponenten. Gültige Werte:

  - `CONTROLLER`: Controller
  - `DESKTOPSTUDIO`: Studio
  - `WEBSTUDIO`: Web Studio
  - `DESKTOPDIRECTOR`: Director
  - `LICENSESERVER`: Citrix Lizenzserver
  - `SECUREPRIVATEACCESS`: Secure Private Access

  Wenn diese Option ausgelassen wird, werden alle Komponenten installiert (bzw. entfernt, wenn die Option `/remove` ebenfalls angegeben ist).

  (In Versionen vor 2003 war `STOREFRONT` als Wert gültig. Verwenden Sie ab Version 2003 den dedizierten, im Artikel Verwenden des Produktinstallationsprogramms aufgeführten StoreFront-Installationsbefehl).

- **/configure_firewall**

  Öffnet alle Ports in der Windows-Firewall, die von den installierten Komponenten verwendet werden, wenn der Windows-Firewalldienst ausgeführt wird, selbst wenn die Firewall nicht aktiviert ist. Wenn Sie die Firewall eines Drittanbieters verwenden oder keine Firewall verwenden, müssen die Ports manuell geöffnet werden.

- **/disableexperiencemetrics**

  Verhindert das automatische Senden der bei Installation, Upgrade oder Deinstallation erfassten Analysedaten an Citrix.

- **/exclude** "*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 für gewöhnlich 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

Bei Upgrades wird diese Option ignoriert, wenn eine nicht unterstützte SQL Server-Version erkannt wird. Einzelheiten finden Sie unter SQL Server-Versionsprüfung.

- **/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_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).

- **/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.

- **/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 Delivery 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
```

Mit dem folgenden Befehl werden ein Delivery Controller, Secure Private Access und SQL Server Express auf einem Server installiert. Für die Komponentenkommunikation erforderliche Firewallports werden automatisch geöffnet.

```
\x64\XenDesktop Setup XenDesktopServerSetup.exe /xenapp /components
controller,secureprivateaccess /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_xxxx.exe`
   - Virtual Delivery Agent für Einzelsitzungs-OS: `VDAWorkstationSetup_xxxx.exe`
   - Core Services Virtual Delivery Agent für Einzelsitzungs-OS: `VDAWorkstationCoreSetup_xxxx.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.: `C:\YourExtractFolder\VDAWorkstationCoreSetup.exe /extract %temp%\CitrixVDAInstallMedia` Das Verzeichnis muss vorhanden sein. Andernfalls schlägt das Extrahieren fehl. Führen Sie dann separat den entsprechenden Befehl 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): `VDAServerSetup_xxxx.exe`, `VDAWorkstationSetup_xxxx.exe` und `VDAWorkstationCoreSetup_xxxx.exe`.

Weitere Informationen zu den Optionen finden Sie unter VDAs installieren.

- **/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_xxxx.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_hdx_tls_dtls**

  Öffnet den TCP- und UDP-Port 443 für HDX Direct V1.

- **/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.

- **/enablerestore** oder **/enablerestorecleanup**

  (Gilt nur für Einzelsitzungs-VDAs) Ermöglicht die automatische Rückkehr zum Wiederherstellungspunkt, wenn die VDA-Installation oder das Upgrade fehlschlägt.

  Beim erfolgreichen Abschluss von Installation oder Upgrade:

  - `/enablerestorecleanup` weist an, dass der Wiederherstellungspunkt entfernt wird.
  - `/enablerestore` weist an, dass der nicht genutzte Wiederherstellungspunkt beibehalten wird.

  Weitere Informationen finden Sie unter Wiederherstellung bei Installations- oder Upgradefehlern.

- **/enable_ss_ports**

  Öffnet, wenn der Windows-Firewalldienst erkannt wird, die für die Bildschirmfreigabe erforderlichen Ports in der Windows-Firewall, selbst wenn die Firewall nicht aktiviert ist. Wenn Sie eine andere oder keine Firewall verwenden, müssen die Ports manuell geöffnet werden.

- **/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 sind:

Multisitzungs-OS	Einzelsitzungs-OS	Core Services für Einzelsitzungs-OS
Citrix Authentication Identity Assertion VDA Plug-in	Citrix Authentication Identity Assertion VDA Plug-in	Citrix Authentication Identity Assertion VDA Plug-in
Citrix Backup and Restore	Citrix Backup and Restore	Citrix Browser Content Redirection
Citrix Browser Content Redirection	Citrix Browser Content Redirection	Citrix Personalization **for** App-V - VDA
Citrix MCS IODriver	Citrix MCS IODriver	Citrix Telemetry Service
Citrix Personalization **for** App-V - VDA	Citrix Personalization **for** App-V - VDA	Citrix Universal Print Client
Citrix Profile Management	Citrix Profile Management	Citrix Vda Log Capture Service
Citrix Profile Management WMI Plug-in	Citrix Profile Management WMI Plug-in	CSE Component
Citrix Rendezvous V2	Citrix Rendezvous V2	Director VDA Plug-in
Citrix Telemetry Service	Citrix Telemetry Service	Machine Management Provider
Citrix Universal Print Client	Citrix Universal Print Client	VDA Monitor Plug-in
Citrix Vda Log Capture Service	Citrix Vda Log Capture Service	VDA WMI Proxy Plug-in
Citrix VDA Upgrade Agent	Citrix VDA Upgrade Agent	
CSE Component	CSE Component	
Director VDA Plug-in	Director VDA Plug-in	

Multisitzungs-OS	Einzelsitzungs-OS	Core Services für Einzelsitzungs-OS
`Machine Identity Service`	`Machine Identity Service`	
`Machine Management Provider`	`Machine Management Provider`	
`VDA Monitor Plug-in`	`User Personalization Layer`	
`VDA WMI Proxy Plug-in`	`VDA Monitor Plug-in`	
	`VDA WMI Proxy Plug-in`	
`Citrix App Protection Component`	`Citrix App Protection Component`	`Citrix App Protection Component`
`Citrix HyperV Filter Driver`	`Citrix HyperV Filter Driver`	
`Citrix Personalization for App-V - VDA`	`Citrix Personalization for App-V - VDA`	`Citrix Personalization for App-V - VDA`

Ausschließen der Citrix User Profilverwaltung aus der Installation (`/exclude "Citrix Profile Management"`) 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 sowohl `/exclude` als auch `/includeadditional` mit demselben 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. Die Option kann hilfreich sein, wenn Sie eine Remote-PC-Zugriff-Bereitstellung erstellen und andere Komponenten installieren möchten, die standardmäßig nicht enthalten sind. Gültige Werte sind:

Multisitzungs-OS	Einzelsitzungs-OS
`Citrix Backup and Restore`	`Citrix Backup and Restore`
`Citrix MCS IODriver`	`Citrix MCS IODriver`
`Citrix Personalization for App-V - VDA`	`Citrix Personalization for App-V - VDA`
`Citrix Profile Management`	`Citrix Profile Management`
`Citrix Profile Management WMI Plug-in`	`Citrix Profile Management WMI Plug-in`
`Citrix Rendezvous V2`	`Citrix Rendezvous V2`
`Citrix VDA Upgrade Agent`	`Citrix VDA Upgrade Agent`
`Citrix Web Socket Vda Registration Tool`	`Citrix Web Socket Vda Registration Tool`
`Machine Identity Service`	`Machine Identity Service`
	`User Personalization Layer`

  Wenn Sie sowohl /`exclude` als auch /`includeadditional` mit demselben Komponentennamen angeben, wird diese Komponente nicht installiert.

- **/installdir** *directory*

  Vorhandenes leeres Verzeichnis, in dem die Komponenten installiert werden. Standard: C:\Programme\Citrix

- **/install_mcsio_driver**

  Nicht verwenden. Verwenden Sie stattdessen /`includeadditional "Citrix MCS IODriver"` oder /`exclude "Citrix MCS IODriver"`.

- **/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 den VDA als Image ein, das zum Erstellen anderer Maschinen verwendet wird. Diese Option entspricht `/mastermcsimage`.

  Diese Option ist ungültig, wenn Sie das Installationsprogramms `VDAWorkstationCoreSetup_xxxx.exe` verwenden.

- **/mastermcsimage**

  Gibt an, dass die Maschine als Image zum Provisioning mit MCS verwendet wird. Diese Option entspricht `/masterimage`.

- **/masterpvsimage**

  Gibt an, dass die Maschine als Image zum Provisioning von VMs mit Citrix Provisioning oder einem Drittanbietertool (z. B. Microsoft System Center Configuration Manager) verwendet wird.

- **/websockettoken** *WebSocketToken*

  Erstellt einen Web Socket VDA. Das WebSocketToken ist für das Token, das benötigt wird.

- **/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, wird die VDA-Installation beendet, da die Voraussetzungen nicht erfüllt sind. Bei den meisten unterstützten Windows-Editionen ist Media Foundation bereits installiert. Eine Ausnahme bilden die N-Editionen. Wenn Sie "Windows-Features > Medienfeatures"*manuell* aktivieren, hat der vom Citrix Meta Installer gesuchte Registrierungsschlüssel möglicherweise keinen festgelegten Wert. Überprüfen Sie den Registrierungsschlüssel `SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\Windows-Features\WindowsMediaVersion`, bevor Sie die Installation starten, um sicherzustellen, dass der Wert vorhanden und nicht leer ist.

- **/nodesktopexperience**

  Das Feature Enhanced Desktop Experience gibt es nicht mehr. Wird diese Option (bzw. die Richtlinieneinstellung) angegeben, so wird sie ignoriert.

  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.

- **/physicalmachine**

  Verwenden Sie dieses Argument zusammen mit /`remotepc` für die RemotePC-Installation. Andernfalls verhält sich der VDA in bestimmten Benutzerszenarios möglicherweise nicht wie erwartet.

- **/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.

- **/proxyconfig** "*Adresse oder PAC-Dateipfad*"

  Wenn Sie in Ihrer Umgebung das Rendezvous-Protokoll mit Gateway Service, VDA Upgrade Service usw. verwenden möchten und in Ihrem Netzwerk einen nicht transparenten Proxy für ausgehende Verbindungen haben, geben Sie den Proxy hier an. Es werden nur HTTP-Proxys unterstützt. Die Adresse oder der PAC-Dateipfad des Proxys zur Verwendung mit Rendezvous. Einzelheiten zu dem Feature finden Sie unter Rendezvousprotokoll.

  - Proxy-Adressformat: `http://<url-or-ip>:<port>`
  - PAC-Dateiformat: `http://<url-or-ip>:<port>/<path>/<filename>.pac`

- **/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). Schließt die Installation zusätzlicher Komponenten aus (siehe Komponentenlisten mit den Optionen /`exclude` und /`includeadditional`).

Diese Option ist ungültig, wenn Sie das Installationsprogramms `VDAWorkstationCoreSetup.exe` verwenden. Das Installationsprogramm schließt diese Komponenten automatisch aus.

`/remotepc` ist mit der Option `/servervdi` nicht kompatibel.

- **/remove**

  Entfernt die mit `/components` angegebenen Komponenten.

- **/remove_appdisk_ack**

  Autorisiert den VDA-Installer, das AppDisks VDA-Plug-In, sofern installiert, zu deinstallieren.

- **/remove_pvd_ack**

  Autorisiert den VDA-Installer, Personal vDisk, sofern installiert, zu deinstallieren.

- **/removeall**

  Entfernt den VDA. Ist die Citrix Workspace App installiert, wird sie nicht entfernt.

- **/REMOVEALLWITHCWA**

  Entfernt CWA zusammen mit dem VDA.

- **/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.

  Verwenden Sie diese Option nur mit dem VDA-Installationsprogramm für das vollständige Produkt.

- **/site_guid** *guid*

  GUID (Globally Unique Identifier) der Site 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.

- **/xendesktopcloud**

  Zeigt an, dass der VDA in Citrix DaaS (Citrix Cloud) installiert ist.

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 Image und MCS zum Provisioning von VMs verwendet. Zunächst wird der VDA bei dem Controller auf dem Server `Contr-Main` in der Domäne `mydomain` registriert. Der VDA verwendet den Benutzerpersonalisierungslayer 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"/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

Problembehandlung bei VDAs

- 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.
- Nach der Installation kann ein VDA erst dann Apps oder Desktops an Benutzer bereitstellen, wenn er sich bei einem Delivery Controller registriert hat.

  Informationen zu VDA-Registrierungsmethoden und zur Behandlung von Registrierungsproblemen finden Sie unter VDA-Registrierung.

Befehlszeilenoptionen zum Installieren eines universellen Druckservers

Die folgende Option ist bei Befehl XenDesktopPrintServerSetup.exe gültig.

- **/enable_upsserver_port**

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.

Befehlszeilenoptionen zur Installation eines Secure Private Access

Die folgenden Optionen sind mit dem folgenden Befehl (Installer) gültig: XenDesktopSPASetup.exe

- **/enable_spa_ports**

  Öffnet Ports in der Windows-Firewall, die für Secure Private Access benötigt werden, wenn der Windows-Firewalldienst erkannt wird, auch 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.

- **/nosql**

  Verhindert die Installation von Microsoft SQL Server Express auf dem Server, auf dem Sie Secure Private Access installieren. Wenn diese Option ausgelassen wird, wird SQL Server Express zur Verwendung als Sitedatenbank installiert.

- **/help oder /h oder /?**

  Zeigt die Hilfe für Befehle an

- **/noreboot**

  Verhindert einen Neustart nach der Installation. Secure Private Access kann erst nach einem Neustart verwendet werden.

- **/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.

- **/remove**

  Entfernt den Secure Private Access.

Weitere Informationen zu den Optionen finden Sie unter Secure Private Access-Installationsprogramm.

Weitere Informationen

Informationen dazu, wie Citrix das Ergebnis von Komponenteninstallationen meldet, finden Sie unter Citrix Installationsrückgabecodes.

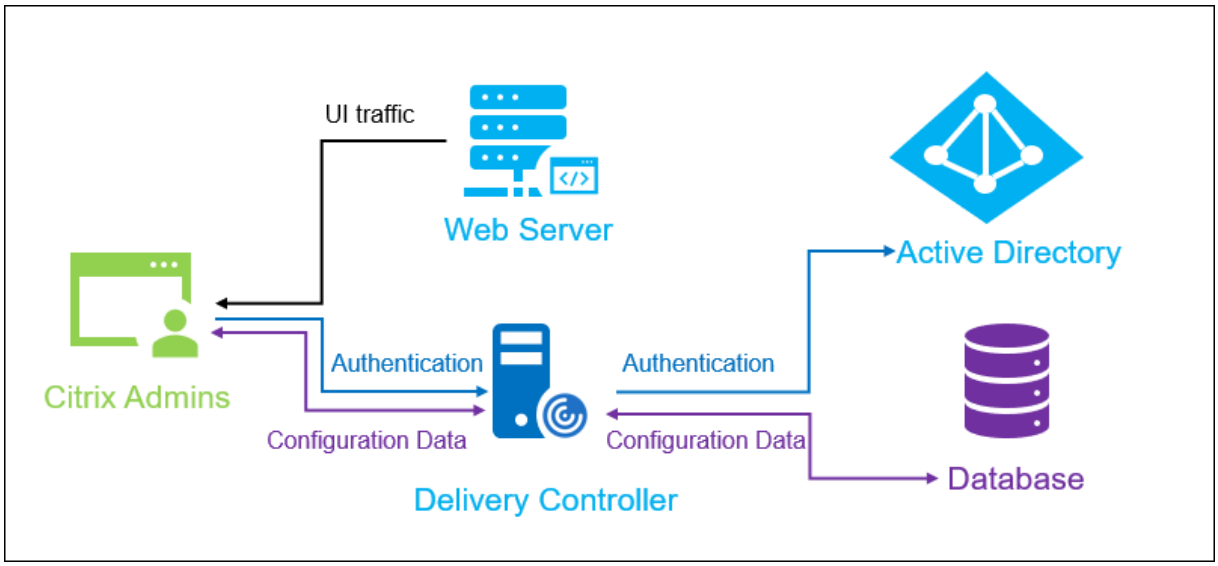
Web Studio installieren

June 28, 2024

Einführung

Citrix Studio ist eine Windows-basierte Verwaltungskonsole, mit der Sie Bereitstellungen von Citrix Virtual Apps and Desktops konfigurieren und verwalten. Web Studio hebt Citrix Studio auf die nächste Stufe –als webbasierte Verwaltungskonsole, die sämtliche Funktionen von Citrix Studio bietet. Web Studio modernisiert Verwaltungsprozesse und entspricht im Erscheinungsbild der Oberfläche "Vollständige Konfiguration"von Citrix DaaS.

Sie können Web Studio auf jedem Windows-Server mit installiertem Internetinformationsdienst (IIS) bereitstellen. Zur beschleunigten Bereitstellung empfehlen wir, Web Studio zusammen mit einem Delivery Controller zu installieren. Web Studio wird dann als Site auf dem Delivery Controller installiert. Dieses Verfahren vereinfacht die Architektur und senkt den Verwaltungsaufwand. Das folgende Diagramm zeigt die Architektur von Web Studio:



Ein allgemeiner Workflow zur Inbetriebnahme von Web Studio sieht wie folgt aus:

1. Web Studio installieren.
2. Site einrichten.
3. Delivery Controller zur Verwaltung in Web Studio hinzufügen.
4. Bei Web Studio anmelden.

Informationen zum Einrichten einer Web Studio-Bereitstellung mit Lastenausgleich finden Sie in diesem Artikel.

Neue Features in Web Studio

Siehe Neue Features.

Systemanforderungen

Unterstützte Betriebssysteme:

- Windows Server 2022
- 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 11
- Windows 10

Unterstützte Browser:

- Internet Explorer 11
  - Der Kompatibilitätsmodus wird für Internet Explorer nicht unterstützt. Verwenden Sie die Standardeinstellungen, um auf Web Studio zuzugreifen.
  - 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 Web Studio ist 1440 x 1024.

Voraussetzungen

Dieses Release von Web Studio ist mit Citrix Virtual Apps and Desktops-Bereitstellungen ab Version 2212 kompatibel.

Führen Sie für Bereitstellungen vor 2212 zunächst ein Upgrade auf Version 2212 durch und installieren Sie dann Web Studio.

Bekannte Einschränkungen

Wenn Sie Web Studio und Citrix Studio im Wechsel verwenden, berücksichtigen Sie folgende Einschränkung: In Web Studio erstellte Vorlagen werden nicht in Citrix Studio angezeigt und umgekehrt.

Dies liegt daran, dass Web Studio und Citrix Studio unterschiedliche Datenbanken zur Speicherung von Vorlagen verwenden. Sie umgehen dieses Problem, indem Sie aus einer Web Studio-Vorlage zunächst eine Richtlinie und aus dieser Richtlinie dann eine Vorlage in Citrix Studio erstellen (und umgekehrt).

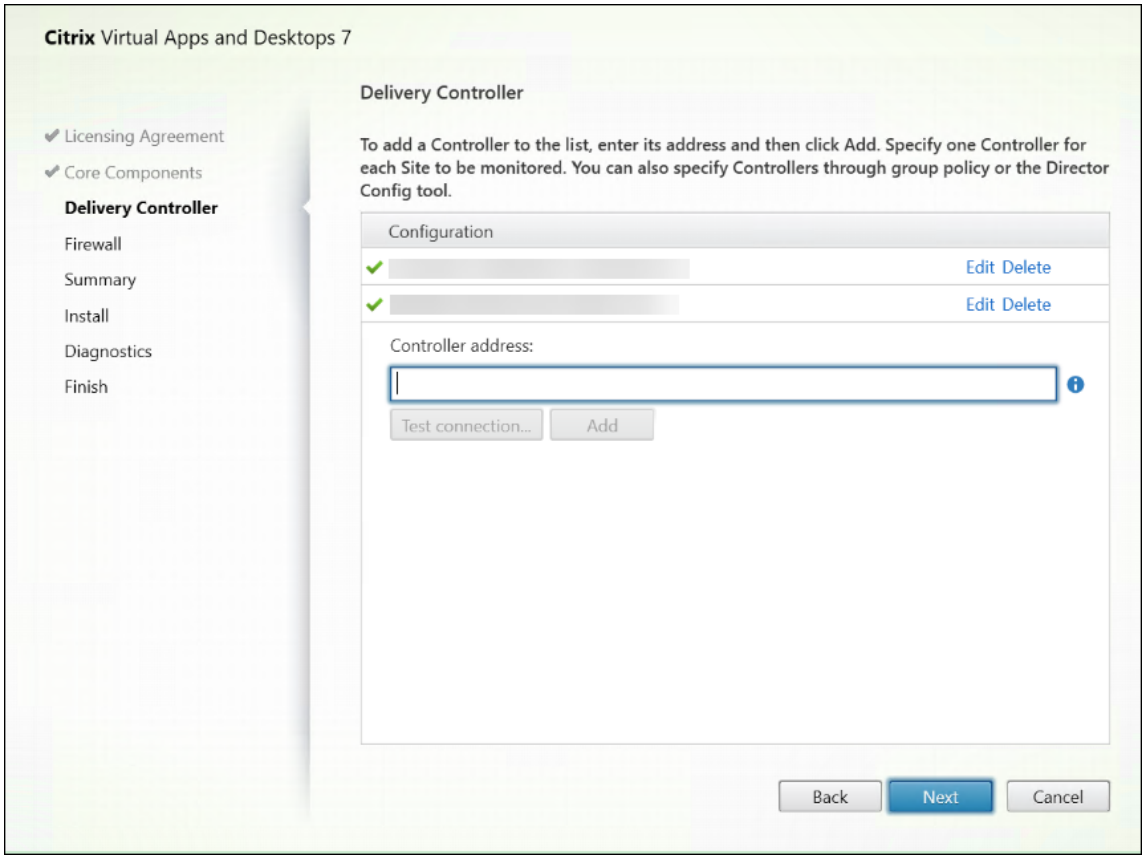
- Zur einwandfreien Installation von Web Studio ändern Sie den Namen der Standardwebsite (**Standardwebsite**) in IIS-Manager (IIS) nicht. Jegliche Änderung des Standardsitenamens führt zu Installationsfehlern.

Web Studio installieren

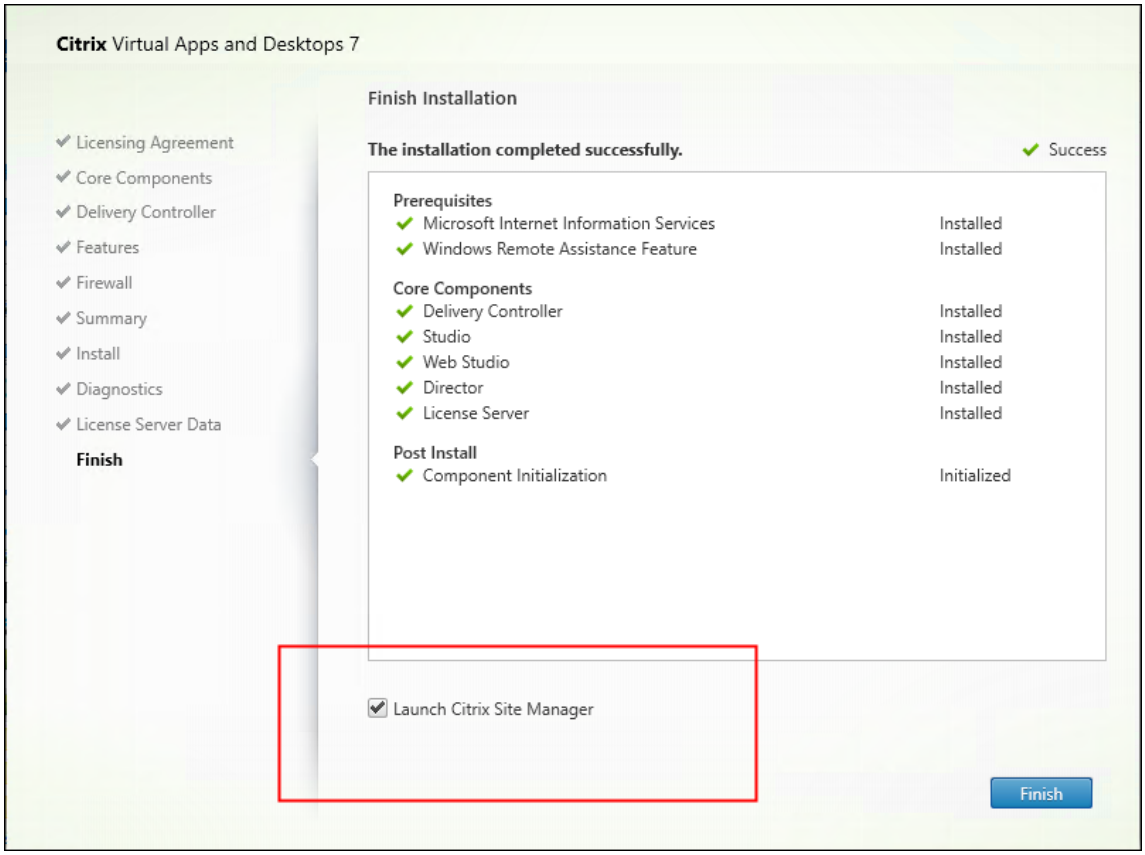
Die folgenden Informationen sind eine Ergänzung zu den Anleitungen unter Kernkomponenten installieren. Installieren von Web Studio:

- Installieren Sie Web Studio mit dem vollständigen ISO-Installationsprogramm für Citrix Virtual Apps and Desktops. Das ISO-Installationsprogramm prüft die Voraussetzungen, installiert fehlende Komponenten, richtet eine Website für Web Studio ein (auf dem Delivery Controller, falls in der Delivery Controller-Installation enthalten) und führt die Grundkonfiguration durch.
- Wenn Web Studio bei der Installation nicht enthalten ist, fügen Sie Web Studio mit dem Installationsprogramm hinzu.
- Bei der Installation von Web Studio werden Sie aufgefordert, die Adresse eines Delivery Controllers einzugeben.

  > **Hinweis:**
  >
  > - Sie können mehrere Delivery Controller hinzufügen. Web Studio wählt dann einen Delivery Controller nach dem Zufallsprinzip aus und versucht, eine Verbindung herzustellen. Wenn dieser Delivery Controller nicht erreichbar ist, greift Web Studio automatisch auf andere Delivery Controller zu.
  > - Wenn Director in **Kernkomponenten** ausgewählt ist und installiert wurde, werden die hier hinzugefügten Delivery Controller für Web Studio und Director verwendet.
  > - Wenn Sie kein externes, öffentlich vertrauenswürdiges Zertifikat konfiguriert haben und kein Zertifikat von einer Zertifizierungsstelle des Unternehmens anfordern möchten, müssen Sie nur den FQDN Ihres Delivery Controllers konfigurieren.
  > - Wenn Sie über das externe, öffentlich vertrauenswürdige Zertifikat verfügen und das öffentliche DNS für Ihren Delivery Controller konfigurieren können, können Sie den DNS-Namen als Delivery Controller-Adresse eingeben.
  > - Wenn Sie das Zertifikat von der Zertifizierungsstelle Ihres Unternehmens anfordern können und Ihr persönliches DNS angeben können, können Sie Ihr persönliches DNS als Delivery Controller-Adresse hinzufügen.



- Zur sicheren Kommunikation zwischen Browser und Webserver sowie Browser und Delivery Controller muss die TLS-Verschlüsselung auf der IIS-Website, auf der Web Studio gehostet wird, und auf dem Delivery Controller aktiviert sein. Wenn kein TLS-Zertifikat für den Delivery Controller konfiguriert ist, wird vom Installationsprogramm ein selbstsigniertes Zertifikat mit dem FQDN des Delivery Controllers und localhost als DNS-Namenszertifikat erstellt. Wenn ein TLS-Zertifikat konfiguriert ist, nimmt das Installationsprogramm keine Änderung vor. Weitere Informationen zur TLS-Verschlüsselung finden Sie unter Web Studio-Bereitstellung sichern (optional).
- Auf der Seite **Fertigstellen** ist das Kontrollkästchen **Site Manager starten** standardmäßig aktiviert, sodass der Citrix Site Manager automatisch geöffnet wird. Um ihn später zu starten, öffnen Sie das Desktop-Startmenü und wählen Sie **Citrix > Citrix Site Manager**. Bevor Sie Web Studio starten, müssen Sie mit dem Citrix Site Manager eine Site erstellen oder einer vorhandenen Site beitreten. Weitere Informationen finden Sie unter Site einrichten.



> **Hinweis:**
>
> Sie können Web Studio auch über die Befehlszeile installieren. Beispiel: `.\XenDesktopServerSetup.exe /components webstudio /controllers "ddc1.studio.local"/configure_firewall /quiet`. Weitere Informationen finden Sie unter Installieren an der Befehlszeile.

Site einrichten

Verwenden Sie den Citrix Site Manager, um Ihre Citrix Virtual Apps and Desktops-Bereitstellung (auch als Site bezeichnet) einzurichten. Das Tool wird automatisch mit einem Delivery Controller installiert.

Führen Sie folgende Schritte aus, um eine Site einzurichten:

1. Öffnen Sie auf einem Delivery Controller das Desktop-Startmenü und wählen Sie **Citrix > Citrix Site Manager**.
2. Wählen Sie im Citrix Site Manager die Option **Site erstellen**. Der Site-Setupassistent wird angezeigt.
3. Erstellen Sie eine Site und konfigurieren Sie ihre Einstellungen wie folgt:

- Geben Sie auf der Seite **Einführung** einen Namen für die Site ein.
- Die Seite **Datenbanken** enthält Optionen zum Einrichten der Datenbanken für die Site, die Überwachung und die Konfigurationsprotokollierung. Weitere Informationen finden Sie unter Schritt 3. Datenbanken.
- Geben Sie auf der Seite **Lizenzierung** die Adresse des Lizenzservers an und legen Sie fest, welche Lizenz verwendet (installiert) werden soll. Weitere Informationen finden Sie unter Schritt 4. Lizenzierung.

4. Überprüfen Sie auf der **Übersichtsseite** alle Einstellungen und klicken Sie auf **Senden**.

   Die IP-Adresse dieses Controllers wird der Site automatisch hinzugefügt.

   > **Hinweis:**
   >
   > Der Benutzer, der eine Site erstellt, ist Volladministrator dieser Site. Weitere Informationen finden Sie unter Delegierte Administration.

Wenn Sie nach dem Erstellen einer Site einen neuen Controller installieren, müssen Sie den Controller der Site hinzufügen. Verfahren:

1. Führen Sie Citrix Site Manager auf diesem neuen Controller aus.
2. Wählen Sie **Vorhandener Site beitreten**.
3. Geben Sie die Adresse eines Controllers ein, der der Site bereits hinzugefügt wurde.
4. Klicken Sie auf **Submit**.

Delivery Controller zur Verwaltung in Web Studio hinzufügen

Verwenden Sie das Studio-Konfigurationstool, um die Delivery Controller zur Verwaltung in Web Studio hinzuzufügen. Sie finden dieses Tool im Installationsordner von Web Studio.

In der Regel ist das Tool im folgenden Standardordner installiert.

- `C:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe`

Angenommen, Sie möchten für die Site, die Sie mit Web Studio verwalten wollen, die folgenden zwei Delivery Controller konfigurieren: `ddc1.studio.local` und `ddc2.studio.local`. Führen Sie den folgenden PowerShell-Befehl aus:

- `.\StudioConfig.exe --server "ddc1.studio.local,ddc2.studio.local"`

> **Hinweis:**
>
> - Für das Tool sind Computeradministratorrechte erforderlich.
> - Änderungen an der Delivery Controller-Konfiguration werden aufgrund der Cache-Einstellungen auf dem IIS-Server möglicherweise nicht sofort wirksam. Zum sofortigen

> Inkraftsetzen öffnen Sie im Web Studio-Server Internetinformationsdienste (IIS)-Manager, gehen Sie zu "Startseite > Websites > Standardwebsite"und wählen Sie im Bereich "Website verwalten"die Option **Neu starten**.
> - Um alle unterstützten Parameter anzuzeigen, führen Sie `StudioConfig.exe --help` aus.

Web Studio als Proxy für Delivery Controller konfigurieren (optional)

Bei Verwaltung Ihrer Bereitstellung über die Web Studio-Konsole nutzen Sie standardmäßig den Webbrowser, um eine Verbindung zum Web Studio-Server und zu den Delivery Controllern herzustellen. Als weitere Option können Sie auch den Web Studio-Server als Proxy für die Delivery Controller konfigurieren. Sie stellen dann nur eine Verbindung zum Web Studio-Server her, wenn Sie Ihre Bereitstellung verwalten.

In diesem Abschnitt wird erläutert, wie Sie einen Web Studio-Server als Proxy für Delivery Controller konfigurieren. Wir gehen davon aus, dass Web Studio und Delivery Controller auf unterschiedlichen Servern installiert sind.

Überprüfen Sie vor dem Start, ob alle notwendigen Kernkomponenten in Ihrer Bereitstellung installiert sind. Weitere Informationen finden Sie unter Installieren von Kernkomponenten.

Führen Sie folgende Schritte aus, um den Proxymodus für Web Studio zu aktivieren:

1. Führen Sie auf dem Web Studio-Server die Windows PowerShell als Administrator aus.
2. Führen Sie den folgenden Befehl aus, wobei Sie `fqdn_of_webstudio_machine` durch den FQDN Ihres Web Studio-Servers ersetzen.

   ```
   & "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe"--enableproxy --proxyserver "fqdn_of_webstudio_machine"
   ```

   > **Hinweis:**
   >
   > Wenn Sie über eine Web Studio-Bereitstellung mit Lastenausgleich verfügen, ersetzen Sie `fqdn_of_webstudio_machine` durch den FQDN des Load Balancer-Servers (auch als virtueller Server bezeichnet). Weitere Informationen finden Sie unter Web Studio-Bereitstellung mit Lastenausgleich einrichten.

Führen Sie den folgenden PowerShell-Befehl aus, um den Proxymodus für Web Studio zu deaktivieren:

```
1 `& "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe" --disableproxy`
```


> **Hinweis:**
>
> Als bewährte Methode empfehlen wir, die Web Studio-Bereitstellung mit einem externen, öffentlich vertrauenswürdigen Zertifikat oder einem Zertifikat einer Zertifizierungsstelle des Unternehmens zu sichern. Weitere Informationen finden Sie unter Web Studio-Bereitstellung sichern (optional).

Bei Web Studio anmelden

Die Web Studio-Website befindet sich unter `https://<address of the server hosting Web Studio>/Citrix/Studio`.

Um sich bei Web Studio anzumelden, öffnen Sie das Desktop-Startmenü und wählen **Citrix > Citrix Web Studio**. Administratoren mit Berechtigungen für Web Studio müssen Active Directory-Domänenbenutzer sein. Folgende Szenarien sind bei der Anmeldung bei Web Studio möglich:

- Sie haben noch keine Delivery Controller für die Site angegeben. In diesem Fall werden Sie aufgefordert, einen Delivery Controller anzugeben, damit Sie vorübergehend Zugriff auf Web Studio erhalten.
- Die angegebenen Delivery Controller sind derzeit nicht erreichbar und Sie können sich nicht bei Web Studio anmelden. Testen Sie Ihre Verbindungen, um sicherzustellen, dass die Delivery Controller erreichbar sind. Sie können auch einen alternativen Delivery Controller angeben, damit Sie vorübergehend Zugriff auf Web Studio erhalten.

Nächste Schritte

1. VDAs installieren
2. Führen Sie folgende Schritte aus, um virtuelle Apps und Desktops mit Web Studio bereitzustellen:
    a) Maschinenkatalog erstellen
    b) Bereitstellungsgruppe erstellen
    c) Anwendungsgruppe erstellen (optional)

VDAs installieren

June 27, 2024

> **Wichtig:**
>
> - Wenn Sie ein Upgrade durchführen und in der aktuellen Version die Software für persönliche vDisks oder AppDisks installiert ist, lesen Sie den Abschnitt PvD, AppDisks und nicht unterstützte Hosts entfernen.
> - Von Citrix vertriebene Binärdateien sind jetzt signiert. Signierte Binärdateien geben an, dass sie entweder durch von Citrix generierte Zertifikate oder durch authentische Zertifikate von Drittanbietern validiert wurden.

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.

Installieren Sie vor der Installation von VDAs die Kernkomponenten. 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 herunterladen 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** auf dem bereitgestellten Laufwerk.

   Der Installationsassistent wird gestartet.

Eigenständiges Installationspaket verwenden:

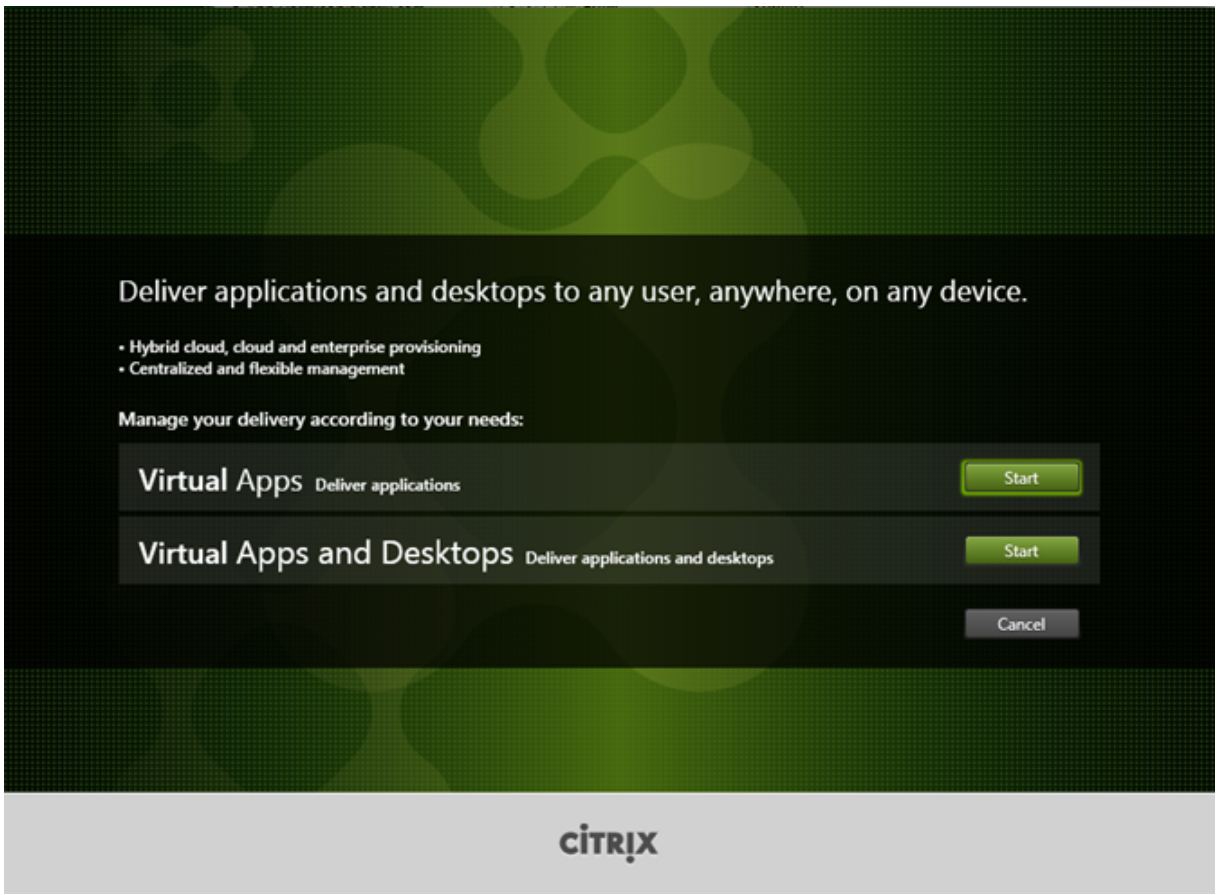
1. Rufen Sie unter Angabe Ihrer Citrix Anmeldeinformationen die Citrix Virtual Apps and Desktops-Downloadseite auf. Laden Sie das benötigte Paket:

- `VDAServerSetup_2308.exe`: VDA für Multisitzungs-OS *Version*
- `VDAWorkstationSetup_2308.exe`: VDA für Einzelsitzungs-OS *Version*
- `VDAWorkstationCoreSetup_2308.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.

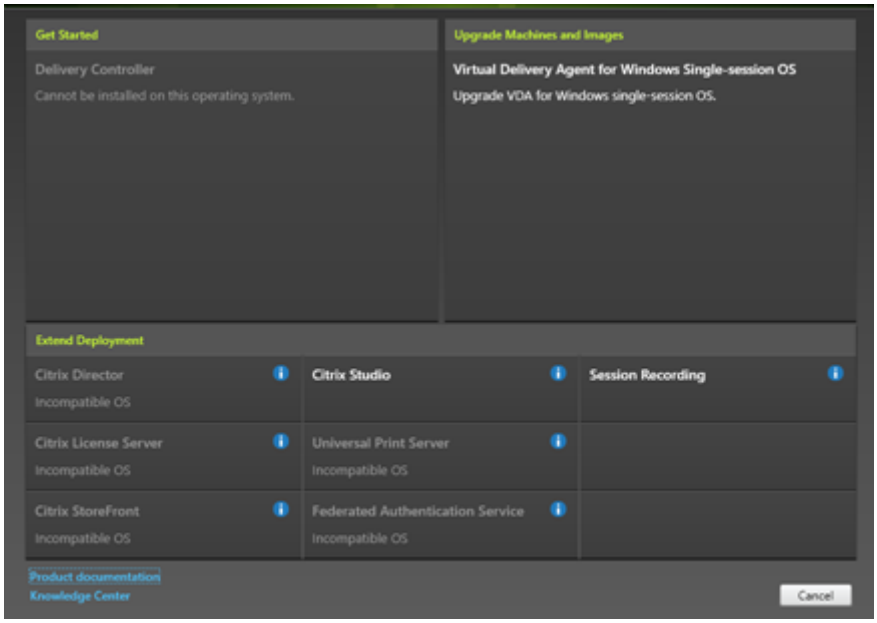
Schritt 2: Zu installierendes Produkt auswählen



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

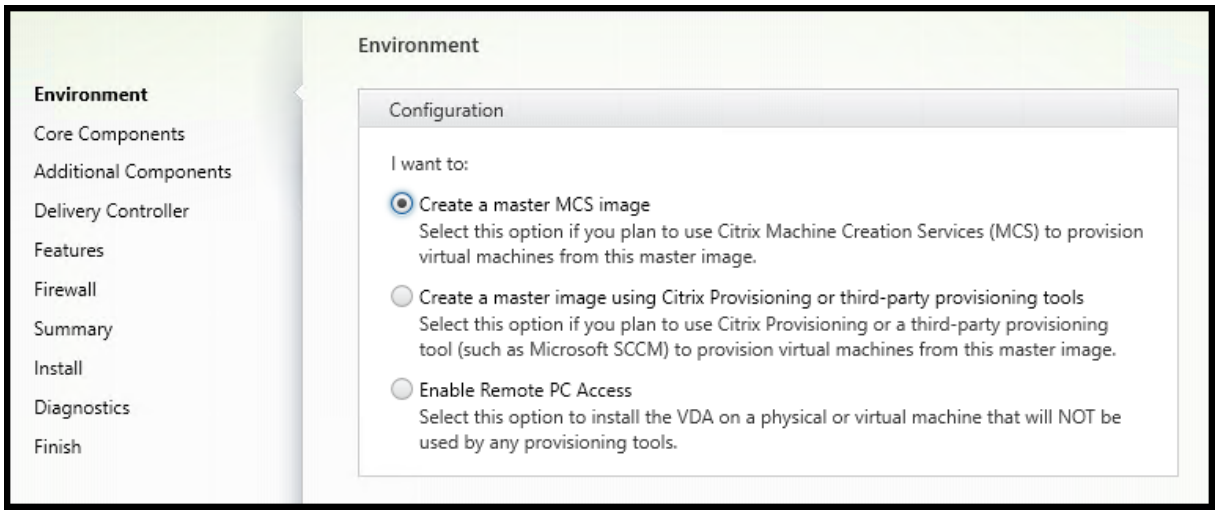


Wählen Sie den Eintrag **Virtual Delivery Agent**. Das Installationsprogramm weiß, ob ein VDA unter einem Einzel- oder Multisitzungs-OS ausgeführt wird, und bietet daher nur einen VDA des richtigen Typs an.

Wenn das Installationsprogramm beispielsweise auf einer Windows Server 2019-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 Image für das Provisioning weiterer Maschinen verwenden möchten.

Je nach gewählter Option werden dann Citrix Provisioning-Tools 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`.

Wählen Sie eine der folgenden Optionen:

- **MCS-Masterimage erstellen:** Wählen Sie diese Option, um einen VDA auf einem VM-Image zu installieren, wenn Sie Maschinenerstellungsdienste (MCS) für das Provisioning von VMs verwenden. Mit dieser Option wird der Maschinenidentitätsdienst installiert. Dies ist die Standardoption.

  Befehlszeilenoption: `/mastermcsimage` oder `/masterimage`

> **Wichtig:**
>
> Das Installationsmedium bzw. ISO-Image muss lokal bereitgestellt werden. Die Bereitstellung eines ISO-Images zur Installation von Software über ein Netzlaufwerk wird nicht unterstützt.

- **Masterimage mit Citrix Provisioning oder Bereitstellungstools von Drittanbietern erstellen:** Wählen Sie diese Option, um einen VDA auf einem VM-Image zu installieren, wenn Sie entweder Citrix Provisioning oder eine Drittanbieteranwendung (z. B. Microsoft System Center Configuration Manager) für das Provisioning von VMs verwenden.

  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 Image 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.

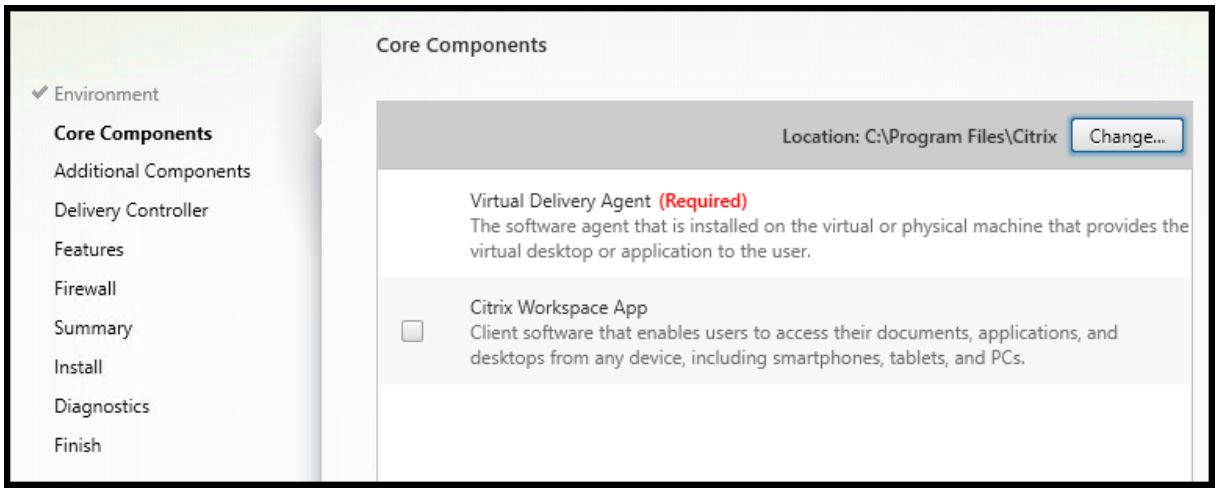
  Befehlszeilenoption: `/remotepc`

Klicken Sie auf **Weiter**.

Die Seite wird in folgenden Fällen nicht angezeigt:

- Bei VDA-Upgrades
- Bei Verwendung des Installationsprogramms `VDAWorkstationCoreSetup_2308.exe`, `VDAServerSetup_2308.exe` oder `VDAWorkstationSetup_2308.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:\Program Files\Citrix` installiert. Die Standardeinstellung ist für die meisten Bereitstellungen geeignet. Wenn Sie einen anderen Speicherort während der Installation angeben, muss dieser Speicherort `execute`-Berechtigung für den Netzwerkdienst haben.
- **Komponenten:** Standardmäßig wird die Citrix Workspace-App für Windows nicht mit dem VDA installiert. Wenn Sie das Installationsprogramm `VDAWorkstationCoreSetup.exe`

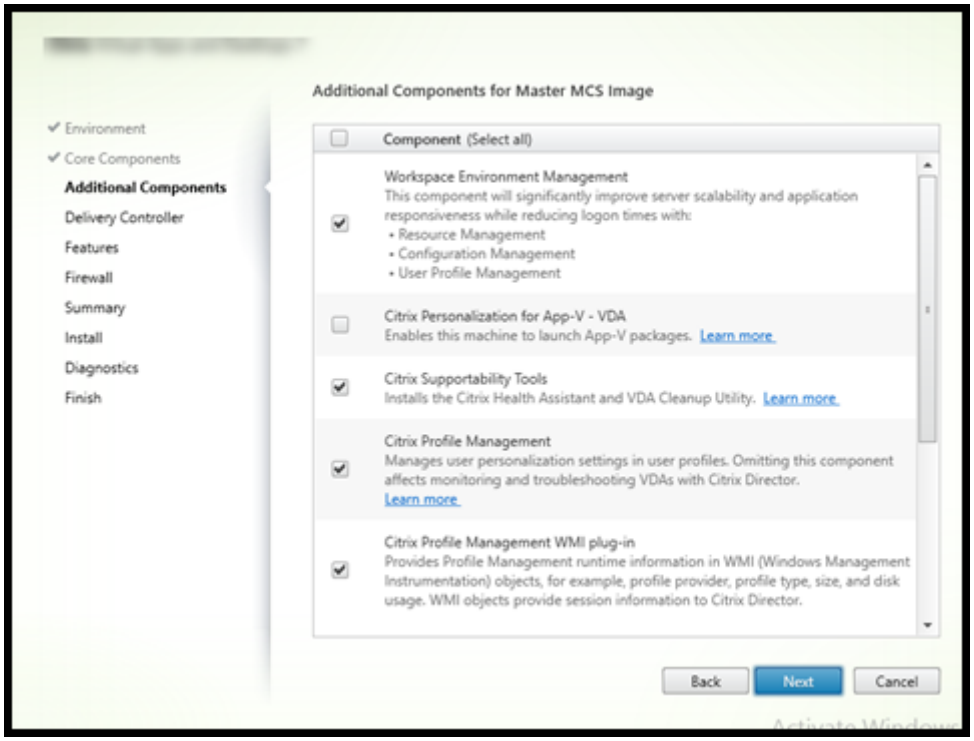
verwenden, wird die Citrix Workspace-App für Windows nie installiert, daher wird dieses Kontrollkästchen nicht angezeigt.

Klicken Sie auf **Weiter**.

Befehlszeilenoptionen: `/installdir`, `/components vda,plugin` zum Installieren des VDAs und der Citrix Workspace-App für Windows

> **Hinweis:**
>
> In den folgenden Szenarien können Sie wählen, ob Sie die Citrix Workspace-App während einer VDA-Installation, eines Upgrades oder einer Deinstallation installieren, aktualisieren oder deinstallieren möchten:
>
> - Während einer VDA-Installation können Sie wählen, ob Sie die Citrix Workspace-App installieren möchten. Standardmäßig wird die Citrix Workspace-App während der VDA-Installation nicht installiert.
> - Wenn die Citrix Workspace-App noch nicht auf dem VDA installiert ist, können Sie während eines VDA-Upgrades wählen, ob die Citrix Workspace-App installiert werden soll.
> - Wenn während eines VDA-Upgrades die Version der Citrix Workspace-App aktualisiert werden kann, wird die Option zum Upgrade der Citrix Workspace-App angezeigt.
> - Während einer VDA-Deinstallation können Sie sich dafür entscheiden, die Citrix Workspace-App nicht zu deinstallieren. Standardmäßig wird die Citrix Workspace-App während der VDA-Deinstallation deinstalliert.

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 `/includeadditional` 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 - VDA	Nicht ausgewählt	Nicht ausgewählt
Benutzerpersonalisierungslayer	Nicht ausgewählt	Nicht angezeigt, da für diesen Anwendungsfall nicht gültig
Citrix Profilverwaltung	Ausgewählt	Nicht ausgewählt

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 Profile Management WMI Plug-In	Ausgewählt	Nicht ausgewählt
Citrix VDA Upgrade Agent	Nicht ausgewählt	Nicht ausgewählt
Citrix Backup and Restore	Nicht ausgewählt	Nicht ausgewählt
Citrix MCS-E/A-Treiber	Nicht ausgewählt	Nicht ausgewählt
Citrix Rendezvous V2	Nicht ausgewählt	Nicht ausgewählt

Die Seite wird in folgenden Fällen nicht angezeigt:

- Wenn Sie das Installationsprogramm `VDAWorkstationCoreSetup.exe` verwenden. 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. (Die Komponenten werden im Installationsprogramm möglicherweise in einer anderen Reihenfolge angezeigt.)

- **Citrix Personalisierung für App-V:** Installieren Sie diese Komponente zur Verwendung von Anwendungen aus Microsoft App-V-Paketen. Weitere Informationen finden Sie unter App-V-Anwendungen bereitstellen.

  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.

- **Citrix 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.

Befehlszeilenoption: `/includeadditional "User Personalization Layer"`, um die Komponenteninstallation zu aktivieren, `/exclude "User Personalization Layer"`, um die Komponenteninstallation zu verhindern.

- **Citrix Profilverwaltung:** Diese Komponente verwaltet die Einstellungen für Benutzeranpassungen in Benutzerprofilen. Einzelheiten finden Sie unter Profilverwaltung.

  Das Ausschließen der Citrix Profilverwaltung bei der Installation hat Auswirkungen auf die Überwachung und Problembehandlung von VDAs mit Citrix Director. Auf den Seiten **Benutzerdetails** und **Endpunkt** treten Fehler in den Bereichen **Personalisierung** und **Anmeldedauer** auf. Auf den Seiten **Dashboard** und **Trends** werden im Bereich **Durchschnittliche Anmeldedauer** nur Daten für Maschinen angezeigt, auf denen 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 Profile Management"`, um die Komponenteninstallation zu aktivieren, `/exclude "Citrix Profile Management "`, um die Komponenteninstallation zu verhindern.

- **Citrix User Profile Management WMI Plug-In:** Dieses Plug-In stellt Laufzeitinformationen zur Profilverwaltung in WMI-Objekten (Windows Management Instrumentation) bereit, z. B. Profilanbieter, Profiltyp, Größe und Datenträgernutzung. WMI-Objekte stellen Sitzungsinformationen für Citrix Director bereit.

  Befehlszeilenoption: `/includeadditional "Citrix Profile Management WMI Plug-in"`, um die Komponenteninstallation zu aktivieren, `/exclude "Citrix Profile Management WMI Plug-in"`, um die Komponenteninstallation zu verhindern.

- **VDA Upgrade Agent:** Nur für Bereitstellungen mit Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service). Ermöglicht dem VDA die Verwendung des Features VDA-Upgrade. Sie können dieses Feature für das Upgrade der VDAs eines Katalogs über die Verwaltungskonsole verwenden, entweder sofort oder zu einem geplanten Zeitpunkt. Wenn dieser Agent nicht installiert ist, können Sie einen VDA aktualisieren, indem Sie das VDA-Installationsprogramm auf der Maschine ausführen.

  Befehlszeilenoptionen: `/includeadditional "Citrix VDA Upgrade Agent"` um die Komponenteninstallation zu aktivieren, `/exclude "Citrix VDA Upgrade Agent"` um die Komponenteninstallation zu verhindern.

- **MCSIO-Schreibcache zur Speicheroptimierung:** Installiert den Citrix MCS-E/A-Treiber. Weitere Informationen finden Sie unter Für Hypervisors freigegebener Speicher und Konfigurieren eines Cache für temporäre Daten.

Befehlszeilenoptionen: `/includeadditional "Citrix MCS IODriver"` um die Komponenteninstallation zu aktivieren, `/exclude "Citrix MCS IODriver"` um die Komponenteninstallation zu verhindern.

- **Proxykonfiguration:** Installieren Sie diese Komponente, wenn Sie das Rendezvous-Protokoll mit dem Gateway Service, dem VDA Upgrade Service usw. in Ihrer Umgebung verwenden möchten. Wenn Sie in Ihrem Netzwerk einen intransparenten Proxy für ausgehende Verbindungen haben, geben Sie den Proxy hier an. Es werden nur HTTP-Proxys unterstützt.

  Wenn Sie diese Komponente installieren, geben Sie auf der Seite **Rendezvousproxykonfiguration** die Proxyadresse oder den Pfad der PAC-Datei an. Einzelheiten zu dem Feature finden Sie unter Rendezvousprotokoll.

  Befehlszeilenoption: `/includeadditional "Citrix Rendezvous V2"`, um die Komponenteninstallation zu aktivieren, `/exclude "Citrix Rendezvous V2"`, um die Komponenteninstallation zu verhindern.

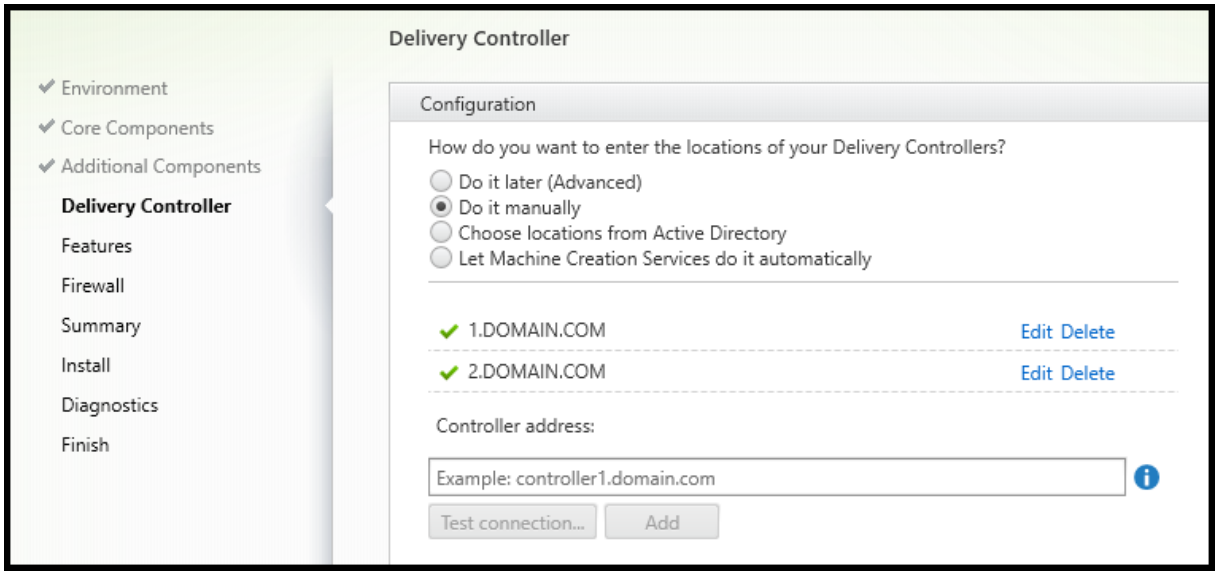
- **Citrix Backup and Restore:** Wenn eine VDA-Installation oder ein VDA-Upgrade fehlschlägt, kann diese Komponente die Maschine auf ein vor der Installation bzw. dem Upgrade erstelltes Backup zurücksetzen.

  Vergewissern Sie sich, dass die Microsoft-Voraussetzungen erfüllt sind, wie unter Vorbereiten der Installationbeschrieben.

  Befehlszeilenoption: `/includeadditional "Citrix Backup and Restore"`, um die Komponenteninstallation zu aktivieren, `/exclude "Citrix Backup and Restore "`, um die Komponenteninstallation zu verhindern.

  > **Hinweis:**
  >
  > Wenn die MCS-Speicheroptimierung aktiviert ist, schlägt Backup oder Wiederherstellung für das Windows Server- oder Desktop-Betriebssystem möglicherweise fehl. Um dieses Problem zu beheben, deaktivieren Sie die MCS-Speicheroptimierungsoption im Meta-Installer.

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.
- **WebSocket-Token verwenden (Tech Preview):** Erstellt einen WebSocket-VDA. Das WebSocketToken ist für das Token, das benötigt wird.
- **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: Proxykonfiguration

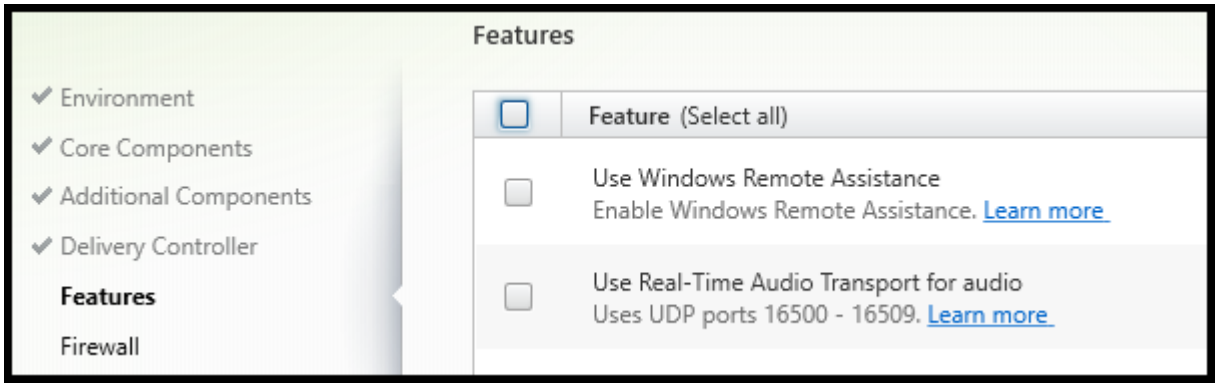
Die Seite **Proxykonfiguration** wird nur angezeigt, wenn Sie auf der Seite **Zusätzliche Komponenten** das Kontrollkästchen **Proxykonfiguration** aktiviert haben.

1. Wählen Sie aus, ob Sie die Proxyquelle anhand der Proxyadresse oder des PAC-Dateipfads angeben möchten.
2. Geben Sie die Proxyadresse bzw. den PAC-Dateipfad an.
    - Proxy-Adressformat: `http://<url-or-ip>:<port>`
    - PAC-Dateiformat: `http://<url-or-ip>:<port>/<path>/<filename>.pac`

Die Firewall muss für den Proxyport geöffnet sein, damit der Verbindungstest ausgeführt werden kann. Kann keine Verbindung zum Proxy hergestellt werden, können Sie wählen, ob Sie mit der VDA-Installation fortfahren möchten.

Befehlszeilenoption: `/proxyconfig`

Schritt 9: Aktivieren oder Deaktivieren von Features



Verwenden Sie auf der Seite **Features** die Kontrollkästchen, um die Features zu aktivieren oder zu deaktivieren, die Sie verwenden möchten.

- **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`

- **Bildschirmfreigabe verwenden:** Wenn diese Option aktiviert ist, werden die von der Bildschirmfreigabe verwendeten Ports in der Windows-Firewall geöffnet. (Standard = deaktiviert)

  Befehlszeilenoption: `/enable_ss_ports`

- **Ist dieser VDA auf einer VM in der Cloud installiert:** Mit dieser Einstellung kann Citrix für Telemetriezwecke die korrekten Ressourcenstandorte für VDA-Bereitstellungen entweder on-premises oder als Service (Citrix Cloud) erkennen. Dieses Feature hat keine Auswirkungen auf die kundenseitige Nutzung. Aktivieren Sie diese Einstellung, wenn Ihre Bereitstellung Citrix DaaS verwendet (Standard = deaktiviert).

  Befehlszeilenoption: `/xendesktopcloud`

Klicken Sie auf **Weiter**.

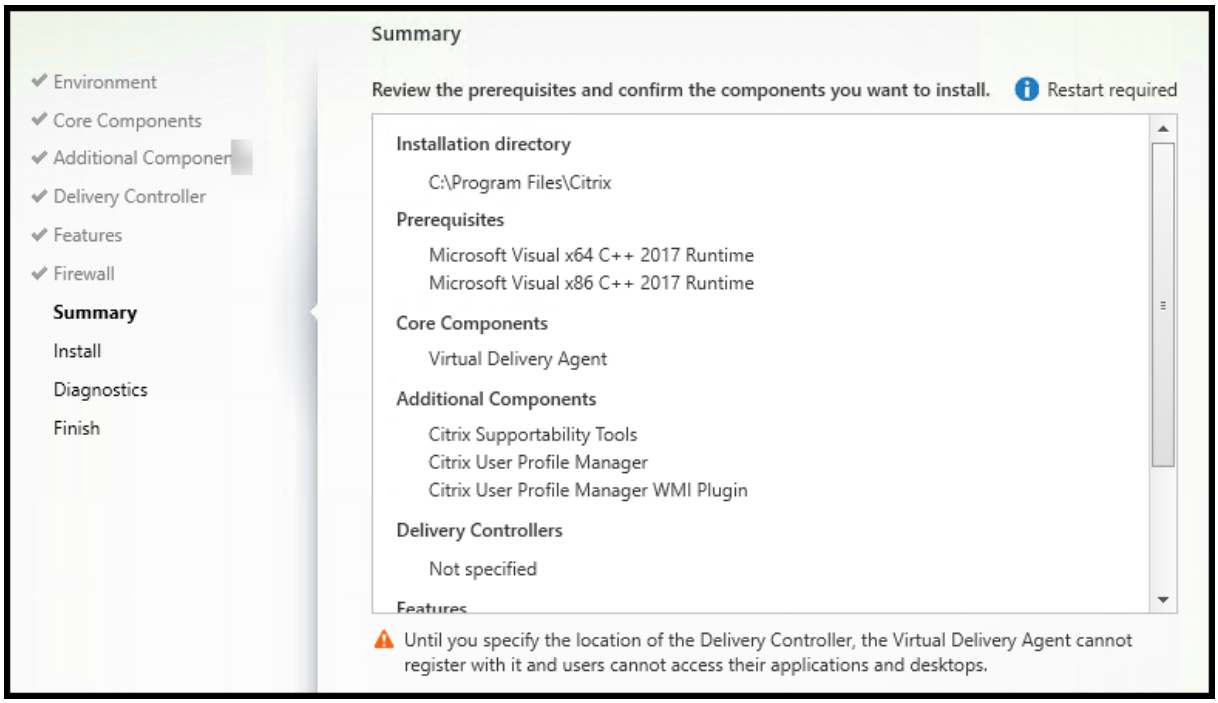
Schritt 10: Firewallports

Standardmäßig sind auf der Seite **Firewall** die folgenden Ports geöffnet, wenn der Windows-Firewalldienst ausgeführt wird, selbst wenn die Firewall nicht aktiviert ist. Die Standardeinstellung ist für die meisten Bereitstellungen geeignet. Weitere Informationen zu Ports finden Sie unter Netzwerkports.

Klicken Sie auf **Weiter**.

Befehlszeilenoption: `/enable_hdx_ports`

Schritt 11: Überprüfen der Voraussetzungen und Bestätigen der Installation

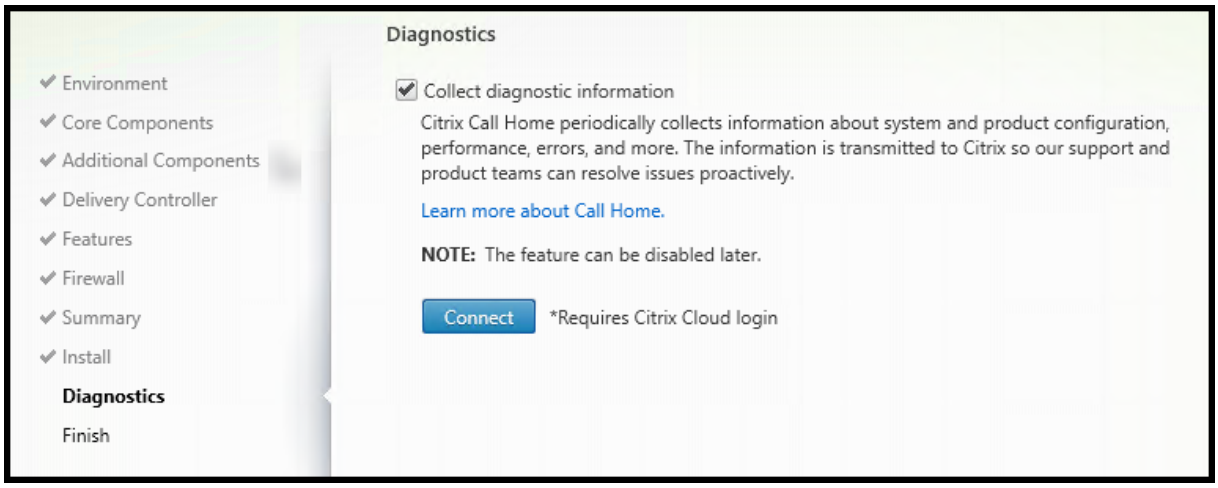


Auf der Seite **Zusammenfassung** wird aufgelistet, was installiert wird. Sie können mit der Schaltfläche **Zurück** zu vorherigen Seiten zurückkehren und Ihre Auswahl ändern.

Wenn Sie fertig sind, klicken Sie auf **Installieren**.

Wenn erforderliche Software (Voraussetzungen) nicht bereits installiert oder aktiviert ist, wird die Maschine evtl. ein- oder mehrmals neu gestartet. Siehe Vorbereiten der Installation.

Schritt 12: Diagnose



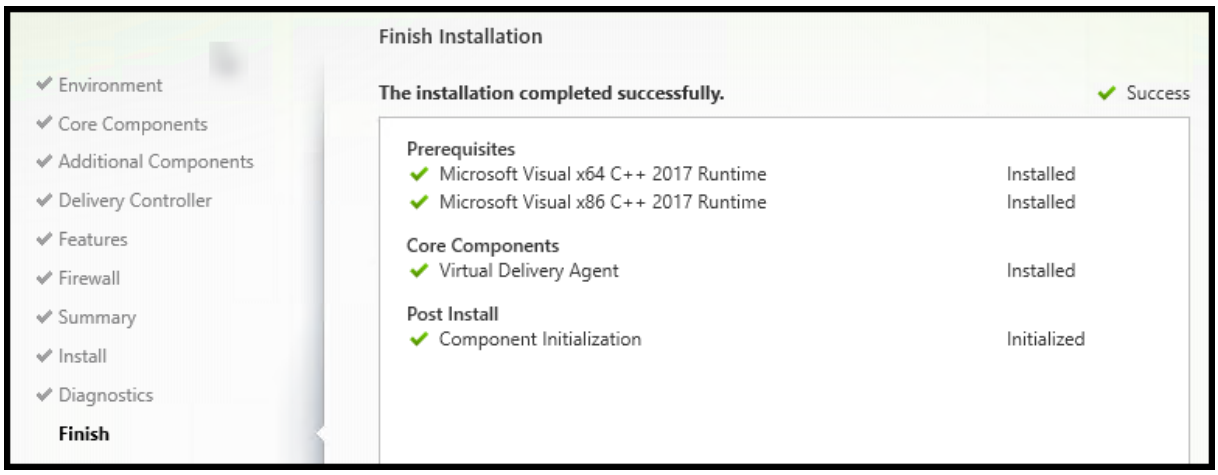
Geben Sie auf der Seite **Diagnose** an, ob Sie bei Citrix Call Home teilnehmen möchten. Wenn Sie teilnehmen möchten (Standardeinstellung), klicken Sie auf **Verbinden**. Geben Sie nach Aufforderung die Anmeldeinformationen Ihres Citrix-Kontos ein.

Wenn Ihre Anmeldeinformationen überprüft sind (bzw. wenn Sie nicht teilnehmen), klicken Sie auf **Weiter**.

Wenn Sie das Komplettinstallationsprogramm verwenden 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. Die nächste Seite kann nicht aufgerufen werden. Um die Schaltfläche **Weiter** wieder zu aktivieren, aktivieren Sie die Option **Diagnoseinformationen sammeln** und deaktivieren Sie sie sofort wieder.

Weitere Informationen finden Sie unter Call Home.

Schritt 13: Abschließen der Installation



Die Seite **Fertigstellen** zeigt grüne Häkchen für alle Voraussetzungen und Komponenten, die erfolgreich installiert und initialisiert werden konnten.

Klicken Sie auf **Fertigstellen**. 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:

- Site erstellen
- Maschinenkataloge erstellen
- Bereitstellungsgruppen erstellen

Citrix Optimizer

Citrix Optimizer ist ein Tool für Windows-Betriebssysteme, das verschiedene Komponenten entfernt bzw. optimiert und Citrix-Administratoren dadurch das Optimieren von VDAs erleichtert.

Nach der Installation des VDAs und dem letzten Neustart können Sie Citrix Optimizer herunterladen und installieren. Siehe CTX224676. Der CTX-Artikel enthält das Download-Paket sowie Anweisungen zur Installation und Verwendung von Citrix Optimizer.

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 die Ergebnisse 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.
- Nach der Installation kann ein VDA erst dann Apps oder Desktops an Benutzer bereitstellen, wenn er sich bei einem Delivery Controller registriert hat.

Informationen zu VDA-Registrierungsmethoden und zur Behandlung von Registrierungsproblemen finden Sie unter VDA-Registrierung.

Bekannte Einschränkung

Wenn Sie die Citrix Workspace-App für Windows Version 1912 oder früher verwenden, wird die Sitzung nach einer Weile unterbrochen. Dieses Problem wurde in den neueren LTSR- und CR-Versionen der Citrix Workspace-App behoben.
Weitere Informationen zu den unterstützten Releaseversionen finden Sie unter Citrix Workspace-App für Windows/Citrix Receiver für Windows Long Term Service Releases.

Windows Defender Access Control im Zusammenhang mit der VDA-Installation konfigurieren

June 27, 2024

Kunden konfigurieren die Windows Defender Access Control (WDAC)-Einstellungen so, dass das Laden unsignierter Binärdateien verhindert wird. Die unsignierten Binärdateien, die über VDA-Installationsprogramme verteilt werden, sind daher verboten, was die VDA-Installation einschränkt.

Citrix signiert jetzt alle von Citrix generierten Binärdateien mit einem Citrix Codesignaturzertifikat. Darüber hinaus signiert Citrix auch die Binärdateien von Drittanbietern, die zusammen mit unserem Produkt vertrieben werden, mit einem Zertifikat, das diese Drittanbieter-Binärdateien als vertrauenswürdige Binärdateien authentifiziert.

> **Wichtig:**
>
> Beim Upgrade von einem älteren VDA mit unsignierten Binärdateien von Drittanbietern auf eine neuere VDA-Version mit signierten Binärdateien werden die signierten Binärdateien möglicherweise nicht immer auf der aktualisierten Maschine platziert.
> Dies ist auf einen Mechanismus innerhalb des Betriebssystems zurückzuführen, bei dem das Upgrade des Systems keine Binärdateien mit derselben Version ersetzt.
> Obwohl die Binärdateien von Drittanbietern signiert wurden, können ihre Versionen, die von Drittanbietern kontrolliert werden, nicht von Citrix aktualisiert werden, was dazu führt, dass diese Binärdateien nicht aktualisiert werden. So können Sie diese Einschränkung umgehen:
>
> 1. Nehmen Sie die Binärdateien in eine Positivliste auf. Dadurch entfällt die Notwendigkeit, die Binärdateien zu signieren.
> 2. Deinstallieren Sie den älteren VDA und installieren Sie den neuen VDA. Dies ähnelt einer

> neuen VDA-Installation und die signierten Versionen werden installiert.

Neue Basisrichtlinie mit dem Assistenten erstellen

Mit dem WDAC können Sie vertrauenswürdige Binärdateien hinzufügen, die auf Ihrem System ausgeführt werden sollen. Nach der Installation von WDAC wird der **Windows Defender Application Control Policy-Assistent** automatisch geöffnet.

Um die Binärdateien hinzuzufügen, muss eine neue WDAC-Basisrichtlinie erstellt werden. In diesem Abschnitt finden Sie die von Citrix empfohlenen Richtlinien für die Erstellung einer Basisrichtlinie.

- Wählen Sie den **signierten und seriösen Modus** als Basisvorlage aus, da damit Windows-Betriebskomponenten, aus dem Microsoft Store installierte Apps, gesamte von Microsoft signierte Software und Windows-hardwarekompatible Treiber von Drittanbietern autorisiert werden.
- **Aktivieren Sie den Überwachungsmodus**, da Sie damit neue Windows Defender Application Control-Richtlinien testen können, bevor Sie sie durchsetzen.
- Fügen Sie eine **benutzerdefinierte Regel** für **Dateiregeln** hinzu, um die Ebene anzugeben, auf der Anwendungen identifiziert und als vertrauenswürdig eingestuft werden, und um eine Referenzdatei bereitzustellen. Wenn Sie "Publisher"als Regeltyp auswählen, kann eine Referenzdatei ausgewählt werden, die von einem der Citrix-Zertifikate signiert ist.
- Nachdem die Regeln hinzugefügt wurden, navigieren Sie zu dem Ordner, in dem die Dateien `.XML` und `.CIP` gespeichert sind. Die Datei `.XML` enthält alle in der Richtlinie definierten Regeln. Sie kann so konfiguriert werden, dass Regeln geändert, hinzugefügt oder entfernt werden.
- Vor der Bereitstellung der WDAC-Richtlinien muss die Datei `.XML` in ihre Binärform konvertiert werden. Die WDAC-Datei konvertiert die `.XML`-Datei in eine `.CIP`-Datei.
- Kopieren Sie die `.CIP`-Datei, fügen Sie sie in: C:\WINDOWS\System32\CodeIntegrity\CiPolicies\Active ein und starten Sie die Maschine neu. Die generierte Richtlinie wird im Auditmodus angewendet.
- Eine schrittweise Anleitung zum Erstellen einer Basisrichtlinie finden Sie unter Neue Basisrichtlinie mit dem Assistenten erstellen.

Wenn diese Richtlinie angewendet wird, warnt WDAC nicht vor Citrix-Dateien, die von der angegebenen Herausgeber/Zertifizierungsstelle signiert wurden.

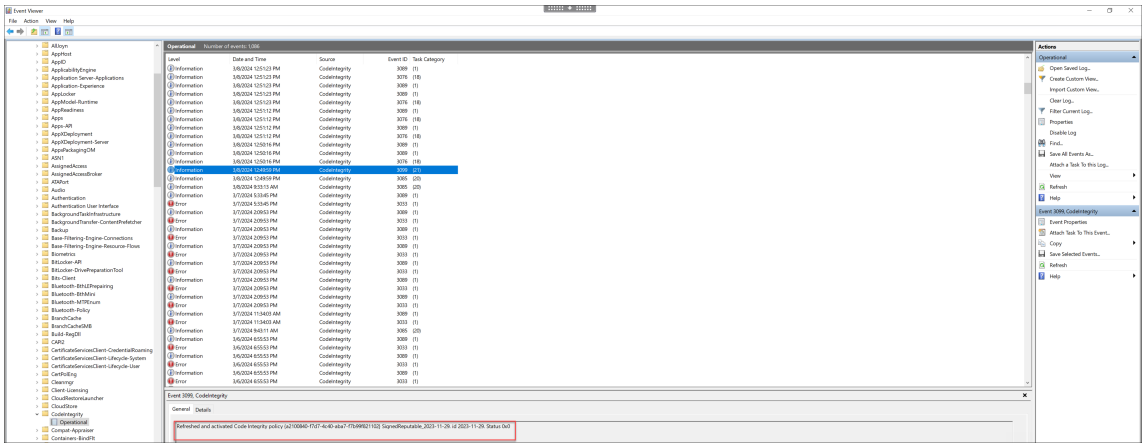
Ebenso kann eine Regel auf Herausgeberebene für die Dateien erstellt werden, die vom Drittanbieter signiert wurden.

Angewendete Richtlinie überprüfen

1. Öffnen Sie nach dem Neustart der Maschine die **Ereignisanzeige** und gehen Sie zu **Anwendungs- und Dienstprotokolle > Microsoft > Windows > CodeIntegrity > Opera-**

tional.

2. Vergewissern Sie sich, dass die angewendete Richtlinie aktiviert ist.



3. Suchen Sie nach Protokollen, die gegen die Richtlinie verstoßen haben, und überprüfen Sie die Eigenschaften dieser Datei. Bestätigen Sie zunächst, dass sie signiert wurde. Wenn nicht und diese Maschine ein VDA-Upgrade durchlaufen hat, ist dies höchstwahrscheinlich der in der obigen Einschränkung beschriebene Fall. Wenn diese Datei signiert ist, wird sie möglicherweise mit dem alternativen Zertifikat signiert, wie zuvor beschrieben.

Ein Beispiel für eine von Citrix generierte Datei, die mit einem Citrix-Zertifikat signiert ist`C:\Windows\System32\drivers\picadm.sys`:
Ein Beispiel für eine Binärdatei eines Drittanbieters, die mit dem Citrix-Zertifikat eines Drittanbieters signiert ist: `C:\Program Files\Citrix\IcaConfigTool\Microsoft.Practices.Unity.dll`.

VDAs mit Skripts installieren

June 27, 2024

> **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`. 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`. 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 Protokoll `Kickoff_VDA_Startup_Script` wird innerhalb von Sekunden nach dem Start der Bereitstellung in die zentrale Protokollfreigabe kopiert. 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.

- 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. Auf der Maschine wird unter "Programme und Features"die tatsächliche VDA-Version angezeigt.
- Nach der Installation kann ein VDA erst dann Apps oder Desktops an Benutzer bereitstellen, wenn er sich bei einem Delivery Controller registriert hat.

  Informationen zu VDA-Registrierungsmethoden und zur Behandlung von Registrierungsproblemen finden Sie unter VDA-Registrierung.

VDAs mit SCCM installieren

June 27, 2024

> **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_XXX.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.

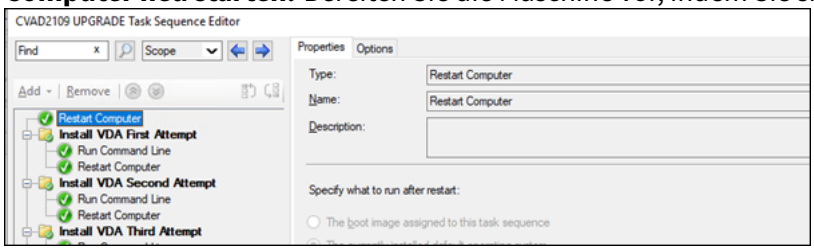
    ‘

- 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.

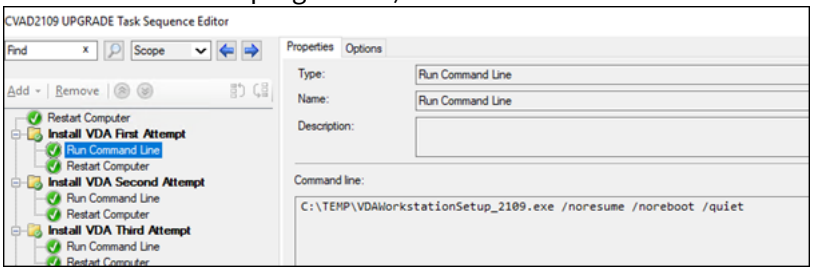
Beispiel einer Installationssequenz mit SCCM

Das folgende Beispiel zeigt die Installationssequenz.

1. **Computer neu starten:** Bereiten Sie die Maschine vor, indem Sie sie neu starten.

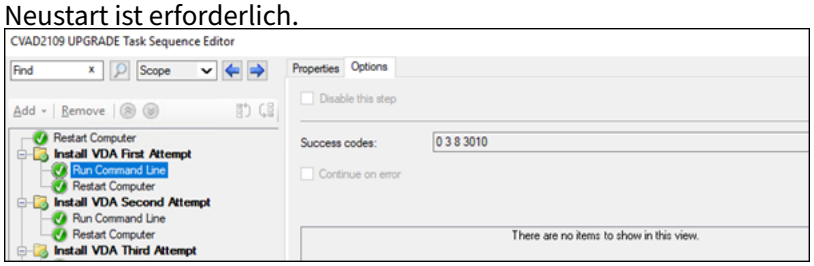


2. **Erster Versuch, den VDA zu installieren:** Starten Sie die VDA-Installation.
   a) Fügen Sie Ihren Befehlszeilenoptionen die Optionen /quiet, /noreboot und /noresume hinzu.
   b) Führen Sie das VDA-Installationsprogramm Ihrer Wahl aus (lokales Image oder eines der Minimalinstallationsprogramme).

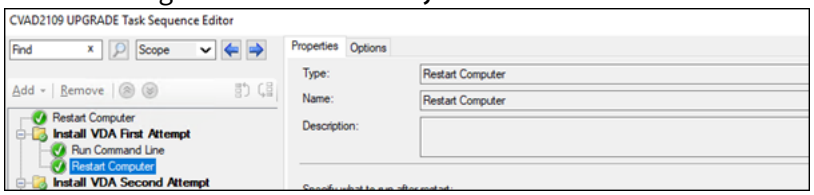


   c) SCCM muss den Rückgabecode erfassen.

- Wenn der Rückgabecode 0 oder 8 lautet, ist die Installation abgeschlossen und ein Neustart ist erforderlich.

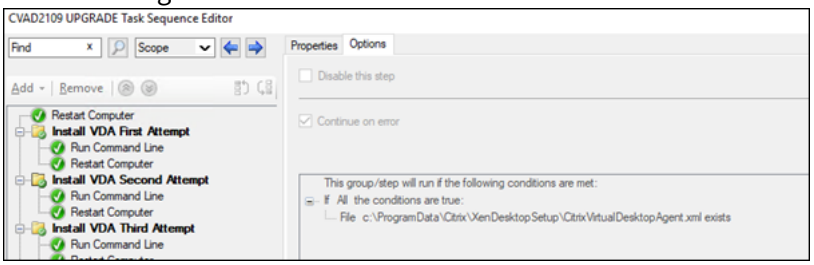


- Wenn der Rückgabecode 3 ist, starten Sie die Maschine neu und übergeben Sie dann die Steuerung an **Zweiter Versuch, den VDA zu installieren**.



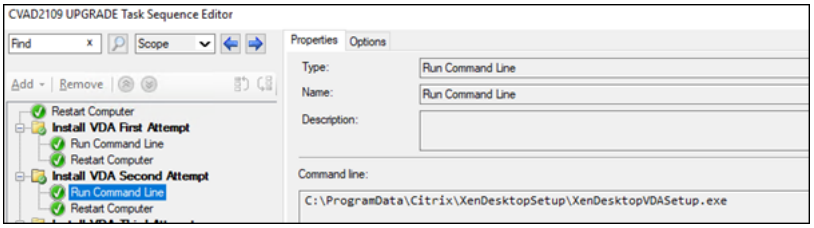
3. **Zweiter Versuch, den VDA zu installieren:** Setzen Sie die VDA-Installation fort.

   a) Wenn die Datei `%programdata%\Citrix\XenDesktopSetup\CitrixVirtualDesktopAge.xml` nach dem **ersten Versuch, den VDA zu installieren**, vorhanden ist, ist die Installation nicht abgeschlossen und muss nach Abschluss des Neustarts fortgesetzt werden.



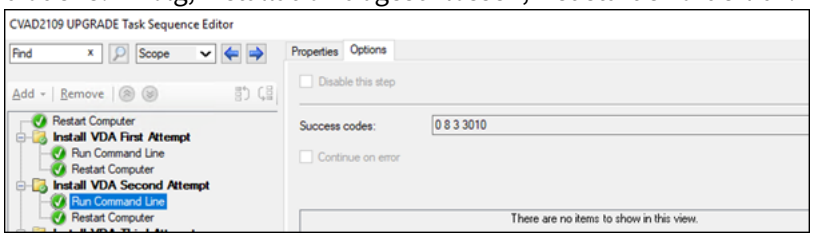
   b) **Der zweite Versuch, den VDA zu installieren**, wird wiederholt, bis die Datei `%programdata%\Citrix\XenDesktopSetup\CitrixVirtualDesktopAgent.xml` nicht existiert oder ein anderer Rückgabecode als 0 oder 8 zurückgegeben wird. Behandeln Sie jeden anderen Rückgabecode als Fehler, und ZWEITER VERSUCH, DEN VDA ZU INSTALLIEREN, sollte einen Fehler melden und den Vorgang beenden.

   c) Setzen Sie die VDA-Installation fort, indem Sie das entsprechende VDA-Installationsprogramm (`XenDesktopVdaSetup.exe` in den meisten Fällen oder `XenDesktopRemotePCSetup.exe`, falls `VDAWorkstationCoreSetup_XXXX.exe` verwendet wurde) aus dem Dateiverzeichnis `%programdata%\ Citrix\XenDesktopSetup\` ohne Befehlszeilenparameter ausführen. (Das VDA-Installationsprogramm verwendet die Parameter, die es bei der ersten Ausführung des Installationsprogramms gespeichert hat.)



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 ZWEITER VERSUCH, DEN VDA ZU INSTALLIEREN, bis die Datei `%programdata%\Citrix\XenDesktopSetup\CitrixVirtualDesktopAgent.xml` nicht existiert oder bis eine 0 oder 8 zurückgegeben wird. Behandeln Sie jeden anderen Rückgabecode als Fehler, und ZWEITER VERSUCH, DEN VDA ZU INSTALLIEREN, 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
- Installieren über die Befehlszeile

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 /physicalmachine /
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
  ```

Site erstellen

June 27, 2024

> **Hinweis:**
>
> Wenn Sie beim Erstellen einer Site eine Lizenz zum Aktivieren einer Hybrid Rights-Lizenz hinzufügen, werden Hosts öffentlicher Clouds (z. B. Microsoft Azure, Google Cloud Platform und Amazon Web Services) erst nach Abschluss der Siteerstellung in der Liste der Verbindungstypen angezeigt.

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 **Einstellungen** im linken Bereich von Web Studio und suchen Sie dann die Einstellung für das **Citrix Programm zur Verbesserung der Benutzerfreundlichkeit**. Einzelheiten finden Sie unter http://more.citrix.com/XD-CEIP.

Der Benutzer, der eine Site erstellt, wird ihr Volladministrator. Weitere Informationen finden Sie unter Delegierte Administration.

Lesen Sie den vorliegenden Artikel bevor Sie die Site erstellen.

Schritt 1: Öffnen des Assistenten für die Siteerstellung - Citrix Site Manager

Verwenden Sie den Citrix Site Manager zum Einrichten Ihrer Citrix Virtual Apps and Desktops-Bereitstellung (auch als Site bezeichnet). Das Tool wird automatisch beim Installieren eines Delivery Controllers installiert.

Um das Tool auszuführen, öffnen Sie Ihr Desktop-Startmenü auf einem Delivery Controller und wählen Sie **Citrix > Citrix Site Manager**. Siehe Web Studio installieren.

Schritt 2: Sitename

Geben Sie auf der Seite **Einführung** einen Namen für die Site ein.

Schritt 3: Datenbanken

Die Seite **Datenbanken** enthält Optionen zum Einrichten der Datenbanken für die Site, die Überwachung und die Konfigurationsprotokollierung. Informationen zu Anforderungen für die Datenbanken und zu deren Einrichtung finden Sie unter Datenbanken.

> **Hinweis:**
>
> Wenn ein immer aktivierter SQL Server-Listener für die TLS-Verschlüsselung konfiguriert ist, werden Sie möglicherweise aufgefordert, Anmeldeinformationen mit Berechtigungen zur Datenbankerstellung einzugeben. Die Datenbankerstellung schlägt selbst dann fehl, wenn Sie gültige Administratoranmeldeinformationen eingeben. Vergewissern Sie sich, dass das SQL Server-Zertifikat den DNS-Namen des Listeners in den SAN (alternative Antragstellernamen) enthält. Weitere Informationen finden Sie unter https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/listeners-client-connectivity-application-failover#SSLcertificates.

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: 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 **Fertig stellen**.

Weitere Informationen

Hostverbindung, Netzwerk und Speicher

Wenn Sie für die Bereitstellung von Anwendungen und Desktops VMs einen Hypervisor oder anderen Service 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 einem anderen Service verwenden (oder wenn Sie Web 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** oder **Remote-PC Wake-On-LAN**. Weitere Informationen finden Sie unter Wake-On-LAN.

  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.
- Wenn Sie über eine Hybrid Rights-Lizenz verfügen und Verbindungen mit Hosts öffentlicher Clouds (z. B. AWS) hinzugefügt haben, werden diese Verbindungen hier aufgelistet. Um diese Public-Cloud-Hostverbindungen anzuzeigen, aktualisieren Sie Web Studio einige Minuten nach dem Hinzufügen.

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.

Verbindungen und Ressourcen erstellen und verwalten

June 27, 2024

> **Wichtig:**
>
> Ab Citrix Virtual Apps and Desktops 7 2006 können Bereitstellung mit einer der folgenden Technologien erst dann auf die aktuelle Version aktualisiert werden, nachdem Elemente am Ende des Lebenszyklus (EOL), die diese Technologien verwenden, entfernt wurden.
>
> - Persönliche vDisks (PvDs)
> - AppDisks
> - Hosts öffentlicher Clouds: Citrix CloudPlatform, Microsoft Azure Classic
>
> Weitere Informationen finden Sie unter Entfernen von persönlichen vDisks, AppDisks und nicht unterstützten Hosts.
>
> **Hinweis:**
>
> Sie können Ihre Citrix Virtual Apps and Desktops-Bereitstellung mithilfe von zwei Verwaltungskonsolen verwalten: Web Studio (webbasiert) und Citrix Studio (Windows-basiert). Dieser Artikel behandelt nur Web Studio. Informationen zu Citrix Studio finden Sie im entsprechenden Artikel in Citrix Virtual Apps and Desktops 7 2212 oder früher.

Um in Ihrer Bereitstellung Verbindungen mit Hosts öffentlicher Clouds zu verwenden, benötigen Sie eine Hybrid Rights-Lizenz, um Ihre Neuinstallation oder das Upgrade auf die aktuelle Version abzuschließen.

Wenn das Installationsprogramm eine nicht unterstützte Technologie oder Hostverbindung ohne Hybrid Rights-Lizenz erkennt, wird das Upgrade angehalten oder beendet und eine Meldung mit einer Erläuterung angezeigt. Die Installationsprotokolle enthalten die Details. Weitere Informationen finden Sie unter Upgrade einer Bereitstellung.

Auswirkung der Hybrid Rights-Lizenz auf Hostverbindungen

In folgenden drei Szenarios werden Verbindungen mit Hosts öffentlicher Clouds vom Hybrid Rights-Lizenzanspruch beeinflusst:

- Um eine neue Verbindung zu Hosts öffentlicher Clouds herzustellen, müssen Sie über eine Hybrid Rights-Lizenz verfügen.
- Wenn Ihre vorhandene Hybrid Rights-Lizenz abgelaufen ist, werden bestehende Verbindungen mit Hosts öffentlicher Clouds als nicht berechtigt markiert und wechseln in den Wartungsmodus. Wenn vorhandene Hostverbindungen im Wartungsmodus sind, sind folgende Prozesse nicht möglich:
  - Hinzufügen oder Ändern von Hostverbindungen
  - Erstellen von Katalogen und Aktualisieren von Images
  - Ausführen von Energieaktionen
- Sobald nicht berechtigte Hostverbindungen in den Zustand “Berechtigt”wechseln, werden vorhandene Hostverbindungen wieder aktiviert.

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 den Speicherort und das Netzwerk unter den Verbindungsressourcen aus.

Administratoren mit Nur-Lese-Zugriff können Verbindungs- und Ressourcendetails anzeigen. Zum Erstellen und Verwalten von Verbindungen müssen Sie Volladministrator sein. 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.

Weitere Informationen finden Sie in den folgenden Informationsquellen:

- **XenServer (früher Citrix Hypervisor):**
  - XenServer-Virtualisierungsumgebungen.
  - XenServer-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
- **Verbindungen mit Hosts öffentlicher Clouds (AWS, Google Cloud, Microsoft Azure, Nutanix-Cloud und Partnerlösungen sowie VMware-Cloud und Partnerlösungen):** Informationen zu Hosts öffentlicher Clouds finden Sie unter Einrichten des Ressourcentyps.

  > **Hinweis:**
  >
  > Die Informationsquellen leiten Sie zur Citrix DaaS-Dokumentation. Wenn Sie bereits mit Hosts öffentlicher Clouds in Citrix DaaS vertraut sind, werden Ihnen Unterschiede zur On-Premises-Version auffallen. In der On-Premises-Version von Virtual Apps and Desktops heißt die Verwaltungsoberfläche Web Studio. Updates für den Service werden ungefähr alle vier Wochen bereitgestellt. Daher könnten Sie feststellen, dass bestimmte Features im Service nicht in der On-Premises-Version verfügbar sind.

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. Zu diesen Daten gehören alle nicht persistenten Daten, die auf durch die Maschinenerstellungsdiensten (MCS) bereitgestellten Maschinen geschrieben werden, Windows-Seitendateien, Benutzerprofildaten und alle Daten, die mit ShareFile synchronisiert werden. Diese Daten werden beim Neustart einer Maschine verworfen.

Durch die Bereitstellung von separatem Speicher für die einzelnen Datentypen können Sie auf Speichergeräten die Last reduzieren und die Leistung verbessern und so den größten Nutzen aus den verfügbaren Ressourcen des Hosts ziehen. Außerdem kann so der entsprechende Speicher für

die verschiedenen Datentypen verwendet werden, denn Persistenz und Resilienz ist für einige Daten wichtiger als für andere.

Speicher kann freigegeben sein (zentraler Speicher, der separat von den Hosts ist, aber von allen Hosts verwendet wird) oder lokal auf einem Hypervisor bereitgestellt werden. Ein zentraler freigegebener Speicher kann beispielsweise aus einem oder mehreren geclusterten Windows Server 2012-Speichervolumes (mit oder ohne angeschlossenem Speicher) oder dem Gerät eines Speicheranbieters bestehen. Der zentrale Speicher bietet möglicherweise auch eigene Optimierungen, wie Steuerungspfade für Hypervisorspeicher und direkter Zugriff über Partner-Plug-Ins.

Durch das lokale Speichern temporärer Daten muss für den Zugriff auf freigegebenen Speicher nicht das Netzwerk passiert werden. Dadurch wird auch die Last 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 XenServer-Hosts lokalen Speicher für die temporäre Datenspeicherung verwenden, vergewissern Sie sich, 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 enthält die Betriebssystemdatenträger.

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 als Daten im freigegebenen Speicher (= *temporärer Datencache*). Der lokale Datenträger 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: Bei Verwendung geclusterter Speichervolumes (CSV) gestattet Microsoft System Center Virtual Machine Manager keine temporären Datenträgercaches auf dem lokalen Speicher.

Erstellen Sie eine Verbindung, um temporäre Daten lokal zu speichern, und aktivieren Sie benutzerdefinierte Werte für die Größe von Cachedatenträger und Speicher jeder VM. Die Standard-

werte sind auf den Verbindungstyp zugeschnitten und in den meisten Fällen ausreichend. Weitere Informationen finden Sie unter Erstellen von Maschinenkatalogen.

Der Hypervisor kann auch Optimierungstechnologien über lokales Lese-Caching der Datenträgerimages bieten. XenServer bietet beispielsweise IntelliCache, wodurch der Netzwerkdatenverkehr zum zentralen Speicher reduziert wird.

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 die Hypervisors der Site übertragen. Dieser Vorgang wird beim Erstellen von Maschinen und zukünftigen Imageupdates durchgeführt. Dieser Prozess führt zu intensivem Datenverkehr auf dem Verwaltungsnetzwerk. Imageübertragungen sind zeitaufwändig und die Images werden jedem Host zu einem anderen Zeitpunkt zur Verfügung gestellt.

Erstellen einer Verbindung und von Ressourcen

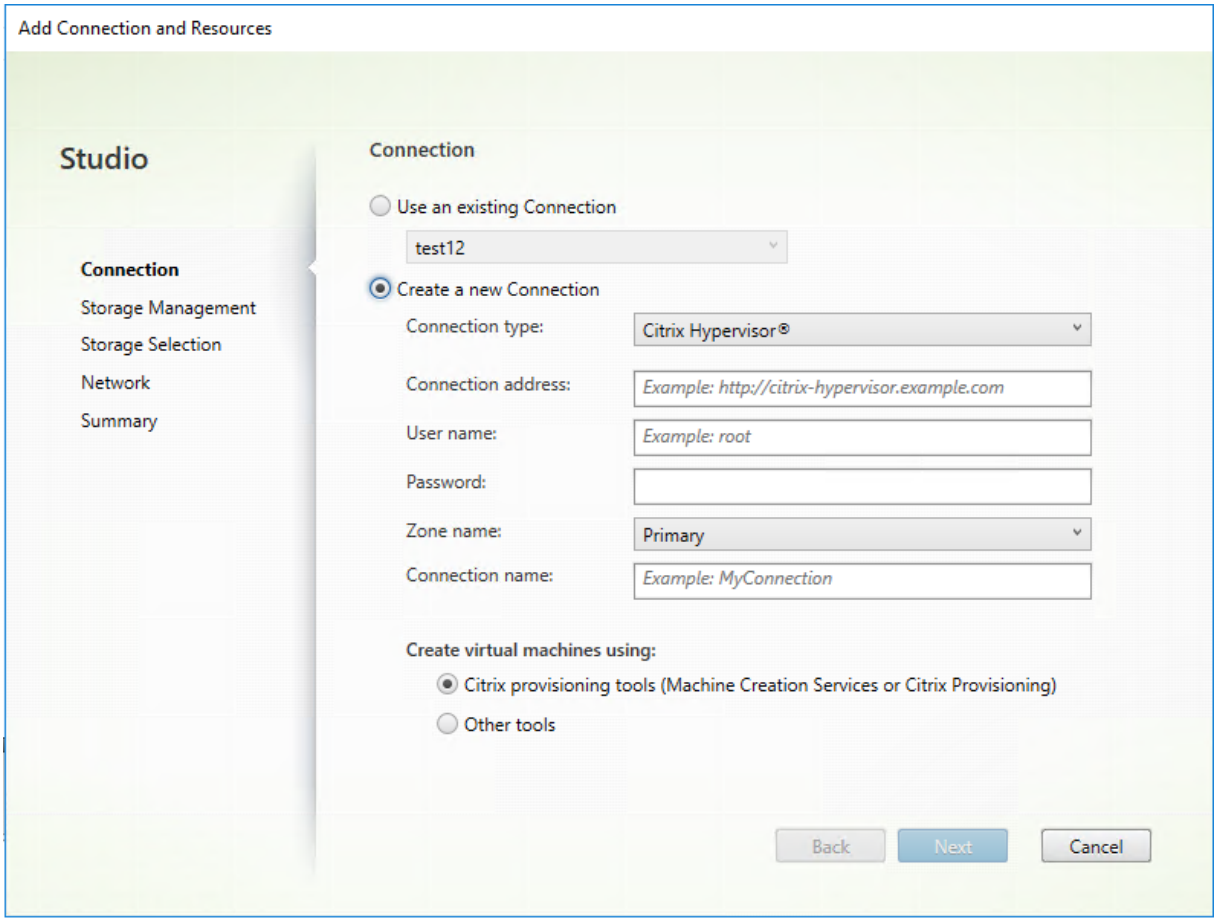
Sie können die erste Verbindung beim Erstellen der Site erstellen. Der Assistent zum Erstellen von Sites enthält die in den nachfolgenden Abschnitten beschriebenen verbindungsbezogenen Seiten.

Wenn Sie eine Verbindung erstellen, nachdem Sie die Site erstellt haben, beginnen Sie mit Schritt 1.

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

1. Melden Sie sich bei Web Studio an.
2. Wählen Sie im linken Bereich **Hosting**.
3. Wählen Sie in der Aktionsleiste die Option **Verbindung und Ressourcen hinzufügen**.
4. 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

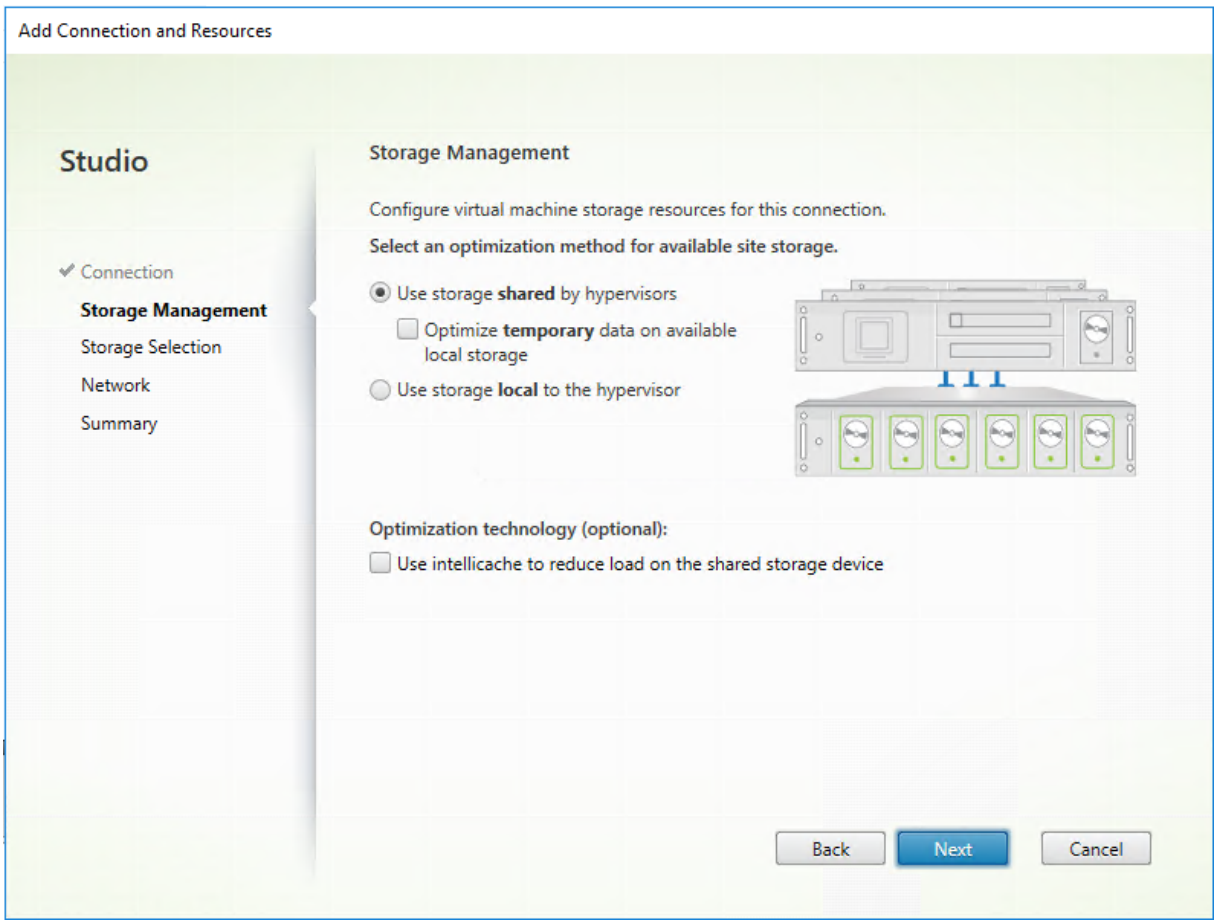


Auf der Seite **Verbindung**:

- 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 aus, den Sie verwenden. Verbindungen mit Hosts öffentlicher Clouds erscheinen nur dann in der Dropdownliste, wenn Sie eine Hybrid Rights-Lizenz verwenden. Alternativ können Sie den PowerShell-Befehl `Get -HypHypervisorPlugin [-ZoneUid] $rluid [-IncludeUnavailable]` mit "false"oder "true"verwenden, um Folgendes zu erhalten:
  - Liste aller von Citrix unterstützten Hypervisor-Plug-Ins, einschließlich derer von Drittanbietern
  - Verfügbarkeit von Hypervisor-Plug-Ins. Wenn der Verfügbarkeitsstatus **false**ist, kann dies daran liegen, dass das Hypervisor-Plug-In nicht korrekt installiert ist oder Sie keinen Anspruch auf eine Hybrid Rights-Lizenz haben.

- 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 Web angezeigt.
- Wählen Sie das Tool, mit dem Sie virtuelle Maschinen erstellen: Web 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.

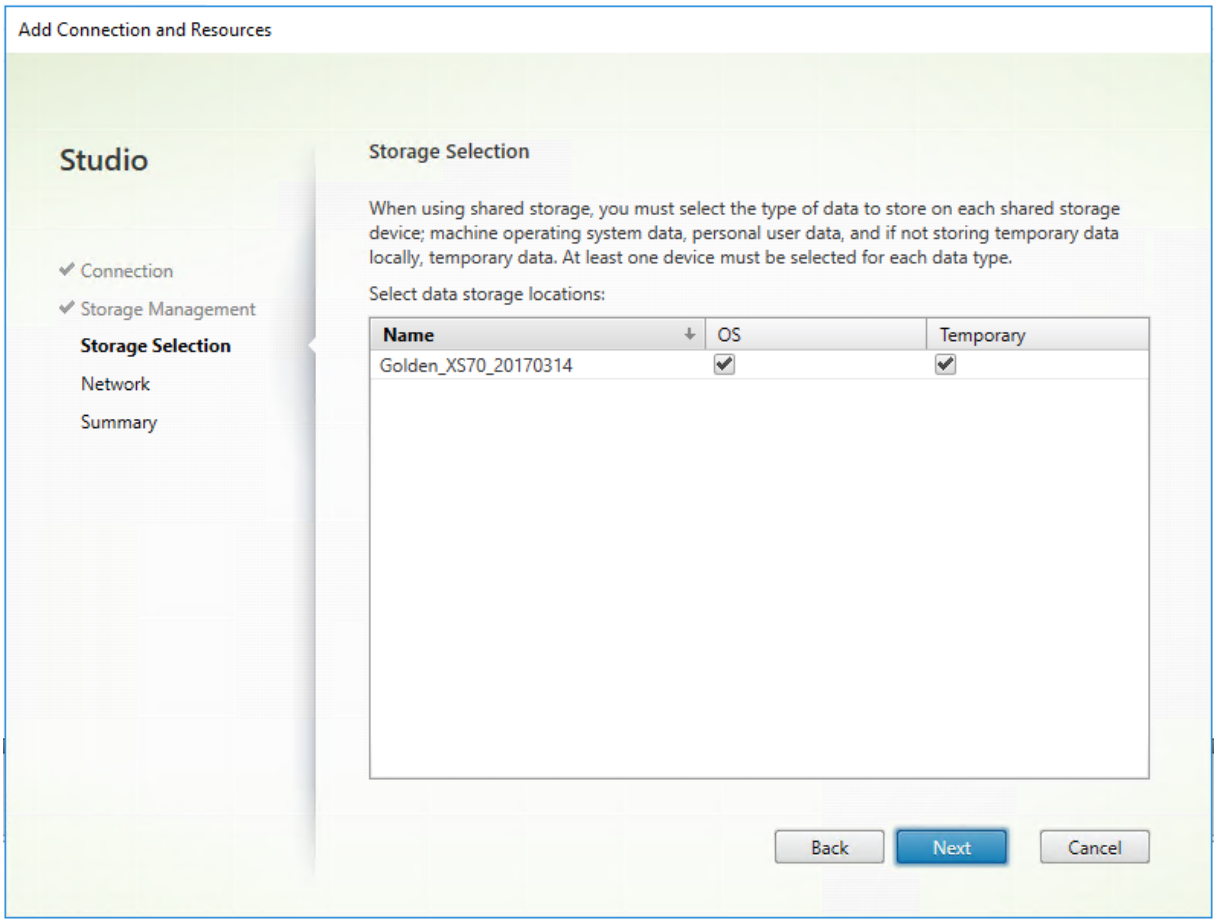
Wählen Sie eine Speicherverwaltungsmethode: für Hypervisors freigegebener Speicher oder lokaler Speicher auf dem Hypervisor.

- 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, gestattet Microsoft System Center Virtual Machine Manager keine temporären Datenträgercaches im lokalen Speicher. Diese Speicherverwaltungskonfiguration in Web Studio schlägt fehl.

Wenn Sie freigegebenen Speicher in einem XenServer-Pool verwenden, geben Sie an, ob Sie IntelliCache zum Reduzieren der Last auf dem freigegebenen Speichergerät verwenden. Weitere Informationen finden Sie unter Verwenden von IntelliCache für XenServer-Verbindungen.

Speicherauswahl



Weitere Informationen zur Speicherauswahl finden Sie unter Hostspeicher.

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

Der untere Teil der Seite **Speicherauswahl** enthält weitere Konfigurationsoptionen, wenn Sie von Hypervisors freigegebenen Speicher gewählt und auf der vorherigen Seite **Temporäre Daten in ver-**

fügbarem lokalem Speicher optimieren aktivieren. Sie können die lokalen Speichergeräte für temporäre Daten auswählen.

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.

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 Web 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. Diese Verbindungen sind unterschiedliche Operationen. 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 fehlerhaft.

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. Melden Sie sich bei Web Studio an.
2. Wählen Sie im linken Bereich **Hosting**.
3. Wählen Sie die Verbindung und dann in der Aktionsleiste **Verbindung bearbeiten** aus.

4. Folgen Sie den Anweisungen bei der Auswahl der Einstellungen zum Bearbeiten einer Verbindung.
5. Wenn Sie fertig sind, klicken Sie auf **Anwenden**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt, oder klicken Sie auf **Speichern**, 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.
- Für die Eingabe eines Servers mit hoher Verfügbarkeit für eine XenServer-Verbindung klicken Sie auf **Server bearbeiten…** und wählen dann die Server aus. Citrix empfiehlt, dass Sie alle Server im Pool auswählen, um die Kommunikation mit XenServer zu ermöglichen, wenn der Poolmaster ausfällt.

  > **Hinweis:**
  >
  > Wenn Sie HTTPS verwenden und Server mit hoher Verfügbarkeit konfigurieren möchten, installieren Sie nicht ein Platzhalterzertifikat für alle Server in einem Pool. Für jeden Server ist ein individuelles Zertifikat erforderlich.

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 dürfen.
- Über **Gleichzeitige Aktionen (alle Typen)** wird die maximale absolute Zahl Aktionen/Updates, die gleichzeitig an dieser Verbindung auftreten dürfen, und der maximale Prozentsatz aller Maschinen, die diese Verbindung verwenden, festgelegt. 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.

Seite **Freigegebene Mandanten**:

Fügen Sie Mandanten und Abonnements hinzu, die sich die Azure Compute Gallery mit dem Abonnement dieser Verbindung teilen. Sie können dann beim Erstellen oder Aktualisieren von Katalogen freigegebene Images aus diesen Mandanten und Abonnements auswählen.

- Geben Sie die **Anwendungs-ID** und das **Anwendungsgeheimnis** für die Anwendung ein, die dieser Verbindung zugeordnet ist. Mit diesen Informationen können Sie sich bei Azure authentifizieren. Es wird empfohlen, Schlüssel regelmäßig zu ändern, um die Sicherheit zu gewährleisten.
- Geben Sie freigegebene Mandanten und Abonnements an. Sie können bis zu acht freigegebene Mandanten hinzufügen. Für jeden Mandanten können Sie maximal acht Abonnements hinzufügen.
- Klicken Sie abschließend auf **Speichern** und **Übernehmen**.

Geben Sie die Informationen im Feld **Verbindungsoptionen** nur unter der Anleitung eines Supportmitarbeiters von Citrix ein.

Netzwerke bearbeiten

Sie können die Netzwerke für eine Verbindung ändern. Führen Sie folgende Schritte aus:

1. Navigieren Sie zu **Hosting**.
2. Wählen Sie die Zielressourcen unter der Verbindung und dann in der Aktionsleiste die Option **Netzwerk bearbeiten**.
3. Wählen Sie mindestens ein Netzwerk aus, das die VMs verwenden sollen.
4. Klicken Sie auf **Speichern**, um Ihre Änderungen zu speichern und den Vorgang zu beenden.

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. Melden Sie sich bei Web Studio an.
2. Wählen Sie im linken Bereich **Hosting**.
3. Wählen Sie die Verbindung aus. Zum Aktivieren des Wartungsmodus wählen Sie in der Aktionsleiste **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. Melden Sie sich bei Web Studio an.
2. Wählen Sie im linken Bereich **Hosting**.
3. Wählen Sie die Verbindung und dann in der Aktionsleiste **Verbindung löschen**.
4. 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. Melden Sie sich bei Web Studio an.
2. Wählen Sie im linken Bereich **Hosting**.
3. Wählen Sie die Verbindung und dann in der Aktionsleiste **Verbindung umbenennen** oder **Verbindung testen**.

Anzeigen von Maschinendetails für eine Verbindung

1. Melden Sie sich bei Web Studio an.
2. Wählen Sie im linken Bereich **Hosting**.

3. Wählen Sie die Verbindung und dann in der Aktionsleiste **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. Melden Sie sich bei Web Studio an.
2. Wählen Sie im linken Bereich **Hosting**.
3. Wählen Sie eine Verbindung und dann im Bereich **Aktionen** die Option **Maschinen anzeigen**.
4. Wählen Sie in der Aktionsleiste eine der folgenden Optionen aus. 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.
Anhalten	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.
Neu starten	Das Betriebssystem wird heruntergefahren und die Maschine dann neu gestartet. Wenn das Betriebssystem diese Aufgaben nicht ausführen kann, bleibt der Desktop im aktuellen Zustand.

Aktion	Beschreibung
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 Daten für VMs gespeichert werden, die eine Verbindung verwenden. Sie können auch festlegen, welche Server für die Speicherung der jeweiligen Datentypen verwendet werden.

1. Melden Sie sich bei Web Studio an.
2. Wählen Sie im linken Bereich **Hosting**.
3. Wählen Sie die Verbindung und dann in der Aktionsleiste **Speicher bearbeiten**.
4. Wählen Sie im linken Bereich den Datentyp: Betriebssystem oder temporär.
5. Aktivieren oder deaktivieren Sie für den ausgewählten Datentyp das Kontrollkästchen für mindestens ein Speichergerät.
6. 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. Melden Sie sich bei Web Studio an.
2. Wählen Sie im linken Bereich **Hosting**.
3. Wählen Sie die gewünschte Ressource und dann den entsprechenden Eintrag in der Aktionsleiste: **Ressourcen löschen**, **Ressourcen umbenennen** oder **Ressourcen testen**.

Verwaiste Azure-Ressourcen erkennen

Verwaiste Ressourcen sind ungenutzte Ressourcen im System, die zu unnötigen Kosten führen können.

Mit diesem Feature können Sie verwaiste Azure-Ressourcen in den Hosts auf Ihrer Citrix Virtual Apps and Desktops-Site erkennen.

Folgen Sie den Schritten in Web Studio:

1. Wählen Sie unter **Verwalten** im linken Bereich **Hosting**.
2. Wählen Sie eine Verbindung aus und wählen Sie in der Aktionsleiste die Option **Verwaiste Ressourcen erkennen**. Im Dialogfeld **Verwaiste Ressourcen erkennen** wird der Bericht zu verwaisten Ressourcen angezeigt.
3. Um den Bericht zu verwaiste Ressourcen anzuzeigen, wählen Sie **Bericht anzeigen**.

Alternativ können Sie verwaiste Azure-Ressourcen auch mithilfe von PowerShell erfassen. Weitere Informationen finden Sie unter Liste verwaister Ressourcen abrufen.

Weitere Informationen zu den Ursachen für verwaiste Ressourcen und zur weiteren Vorgehensweise finden Sie unter Efficiently manage Orphaned Azure resources with Citrix.

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 inaktive 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 Sitzung:** Legt fest, wie lange ein 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.

Liste verwaister Ressourcen abrufen

Sie können eine Liste der verwaisten Ressourcen abrufen, die von MCS erstellt wurden, aber nicht mehr von MCS verfolgt werden. Dies gilt derzeit für Azure-Umgebungen. Um die Liste abzurufen, können Sie PowerShell-Befehle verwenden. Sie können anhand von Verbindungen filtern.

> **Hinweis:**
>
> - Der PowerShell-Befehl wird zurückgewiesen, wenn ein Provisioning oder ein Imageupdate im Gang ist.

> - Eine vom Kunden verwaltete Ressource, die mit allen Citrix Tags gekennzeichnet ist, wird als verwaiste Ressource erkannt. Wenn Sie dieser Ressource jedoch das Tag "CitrixDetectIgnore"mit dem Wert "true"hinzufügen, wird die Ressource bei der Erkennung verwaister Ressourcen ignoriert.

Einschränkungen

- Nur ein Administrator mit der integrierten Rolle eines Administrators mit vollen Rechten oder eines Cloudadministrator kann den PowerShell-Befehl zum Abrufen der Liste verwaister Ressourcen ausführen.
- Um eine fälschliche Erkennung verwaister Ressourcen zu vermeiden, schalten Sie virtuelle Maschinen nicht ein, während Sie verwaiste Ressourcen filtern.
- Rund 2000 Datensätze werden im Falle einer möglichen hohen Workload als verwaist angezeigt.

Um die Liste der verwaisten Ressourcen anzuzeigen, gehen Sie wie folgt vor:

1. Öffnen Sie ein **PowerShell**-Fenster.
2. Führen Sie die folgenden Befehle aus:

   a) Ruft die Verbindungs-UID ab. Die Verbindungs-UID ist der Wert des HypervisorConnectionUid-Attributs.

   ```
   Get-ChildItem xdhyp:\connections | where {
     $_.PluginId -like 'Azure*'  }
    "
   <!--NeedCopy-->
   ```

   b) Rufen Sie die Liste der verwaisten Ressourcen ab.

   ```
   get-provorphanedresource -HypervisorConnectionUid <connection
      uid>
   <!--NeedCopy-->
   ```

Um die Liste der verwaisten Ressourcen einer Abonnement-ID anzuzeigen, gehen Sie wie folgt vor:

1. Öffnen Sie ein **PowerShell**-Fenster.
2. Führen Sie die folgenden Befehle aus:

   a) Suchen Sie die Verbindungs-UID anhand der Abonnement-ID. Die Verbindungs-UID ist der Wert des HypervisorConnectionUid-Attributs.

   ```
   Get-ChildItem xdhyp:\connections | where {
     $_.CustomProperties -match '<subscriptionId>'  }

   <!--NeedCopy-->
   ```


b) Rufen Sie die Liste der verwaisten Ressourcen ab:

```
get-provorphanedresource -HypervisorConnectionUid <connection
    uid>
<!--NeedCopy-->
```

> **Hinweis:**
>
> Überprüfen Sie die Ressourcen sorgfältig, bevor Sie sie löschen.

So geht es weiter

Informationen zur Verbindung zu bestimmten Hosttypen finden Sie unter:

- Verbindung zu AWS
- Verbindung zu XenServer
- Verbindung zu Google-Cloudumgebungen
- Verbindung zu Microsoft Azure
- Verbindung zu Microsoft System Center Virtual Machine Manager
- Verbindung zu Nutanix
- Verbindung zu Nutanix-Cloud und Partnerlösungen
- Verbindung zu VMware
- Verbindung zu VMware-Cloud und Partnerlösungen

Wenn dies die erste Bereitstellung ist, erstellen Sie zunächst einen Maschinenkatalog.

Verbindung zu AWS

June 27, 2024

Unter Verbindungen und Ressourcen erstellen und verwalten werden die Assistenten zum Erstellen einer Verbindung beschrieben. Die folgenden Informationen beziehen sich speziell auf AWS-Cloudumgebungen.

> **Hinweis:**
>
> Bevor Sie eine Verbindung zu AWS herstellen, müssen Sie zunächst Ihr AWS-Konto als Ressourcenstandort eingerichtet haben. Siehe AWS-Cloudumgebungen.

Verbindung erstellen

Beim Erstellen einer Verbindung von Web Studio aus gilt Folgendes:

- Sie müssen den API-Schlüssel und die geheimen Schlüsselwerte angeben. Sie können die Schlüsseldatei mit diesen Werten aus AWS exportieren und anschließend importieren. Sie müssen auch die Werte für Region, Verfügbarkeitszone, VPC-Namen, Subnetzadressen, Domänenname, Namen der Sicherheitsgruppen und Anmeldeinformationen angeben.
- Die für das AWS-Rootkonto von der AWS-Konsole abgerufene Anmeldeinformationsdatei hat nicht das gleiche Format wie die Anmeldeinformationsdateien, die für Standard-AWS-Benutzer heruntergeladen werden. Deshalb kann diese Datei nicht von Citrix Virtual Apps and Desktops zum Ausfüllen der Felder "API-Schlüssel"und "Geheimer Schlüssel"verwendet werden. Verwenden Sie AWS Identity Access Management (IAM)-Anmeldeinformationsdateien.

> **Hinweis:**
>
> Nachdem Sie eine Verbindung hergestellt haben, kann die Aktualisierung des API-Schlüssels und des geheimen Schlüssels fehlschlagen. Um das Problem zu beheben, überprüfen Sie Ihren Proxyserver oder die Firewall-Beschränkungen und stellen Sie sicher, dass die folgende Adresse erreichbar ist: `https://*.amazonaws.com`.

Standardwerte für Hostverbindungen

Wenn Sie Hostverbindungen in AWS-Cloudumgebungen erstellen, werden die folgenden Standardwerte angezeigt:

Option	Absolut	Prozent
Gleichzeitige Aktionen (alle Typen)	125	100
Höchstanzahl neue Aktionen pro Minute	125	

MCS unterstützt standardmäßig maximal 100 gleichzeitige Provisioningvorgänge.

Service-Endpunkt-URL

Standard-Service-Endpunkt-URL

Wenn Sie MCS verwenden, werden neue AWS-Verbindungen mit einem API-Schlüssel und einem API-Geheimnis hinzugefügt. Anhand dieser Informationen und des authentifizierten Kontos fragt MCS bei AWS mit dem AWS-API-Aufruf DescribeRegions EC2 die unterstützten Zonen ab. Die Abfrage erfolgt mit der generischen EC2-Service-Endpunkt-URL `https://ec2.amazonaws.com/`. Wählen Sie über MCS die Zone für die Verbindung aus der Liste der unterstützten Zonen aus. Die bevorzugte AWS-Service-Endpunkt-URL wird automatisch für die Zone ausgewählt. Nach dem Erstellen der Service-Endpunkt-URL können Sie diese nicht mehr ändern.

IAM-Berechtigungen definieren

Anhand der Informationen in diesem Abschnitt können Sie IAM-Berechtigungen für Citrix Virtual Apps and Desktops in AWS definieren. Der IAM-Dienst von Amazon gestattet Konten mit mehreren Benutzern, die in Gruppen organisiert werden können. Die Benutzer können verschiedene Berechtigungen für die Durchführung von Vorgängen haben, die mit dem Konto verknüpft sind. Weitere Informationen zu IAM-Berechtigungen finden Sie unter IAM-JSON-Richtlinienreferenz.

Gehen Sie zum Anwenden der IAM-Berechtigungsrichtlinie auf eine neue Benutzergruppe folgendermaßen vor:

1. Melden Sie sich bei der AWS-Verwaltungskonsole an und wählen Sie **IAM service** aus der Dropdownliste aus.
2. Wählen Sie **Create a New Group of Users**.
3. Geben Sie einen Namen für die neue Benutzergruppe ein und wählen Sie **Continue**.
4. Wählen Sie auf der Seite **Permissions** die Option **Custom Policy**. Wählen Sie **Select**.
5. Geben Sie einen Namen für die **Berechtigungsrichtlinie**ein.
6. Geben Sie im Abschnitt **Richtliniendokument** die relevanten Berechtigungen ein.

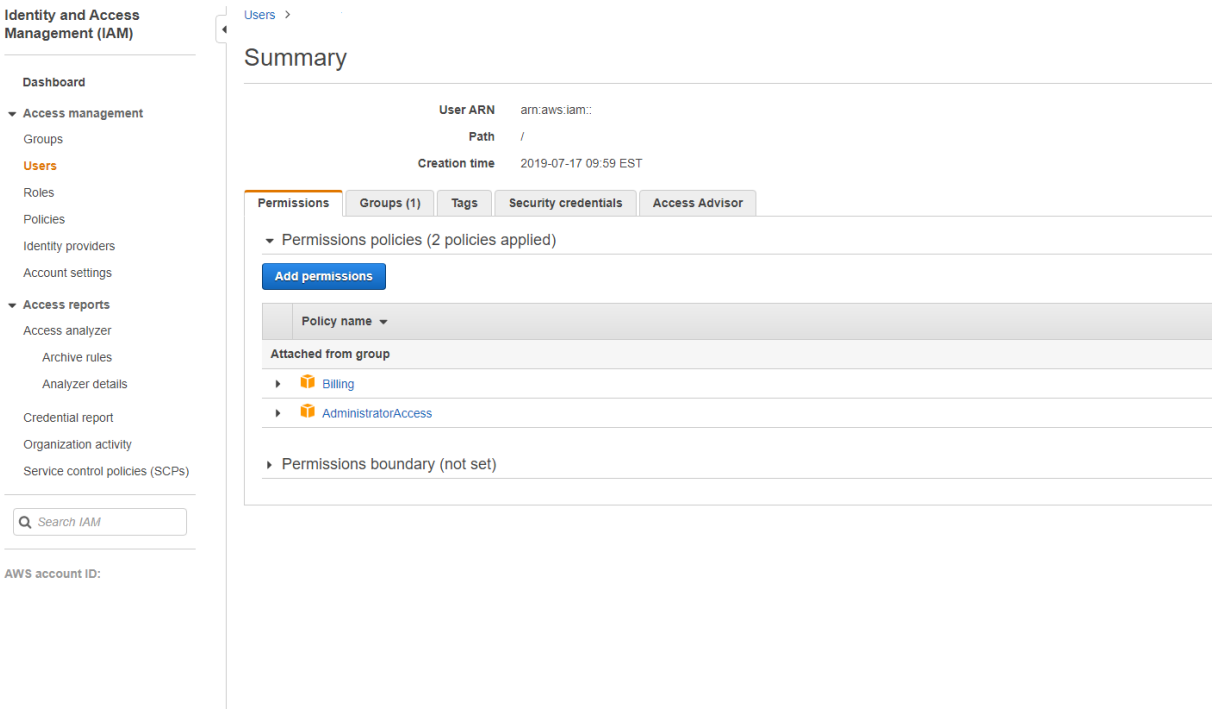
Nach Eingabe der Richtlinieninformationen wählen Sie **Continue**, um die Benutzergruppe abzuschließen. Den Benutzern in der Gruppe werden nur die Berechtigungen erteilt, die sie zur Ausführung der für Citrix Virtual Apps and Desktops erforderlichen Aktionen benötigen.

> **Wichtig:**
>
> Verwenden Sie den Richtlinientext im obigen Beispiel, um die von Citrix Virtual Apps and Desktops in einem AWS-Konto durchgeführten Aktionen aufzulisten, ohne diese auf bestimmte Ressourcen zu beschränken. Citrix empfiehlt die Verwendung des Beispiels zu Testzwecken. Für Produktionsumgebungen können Sie weitere Beschränkungen für Ressourcen hinzufügen.

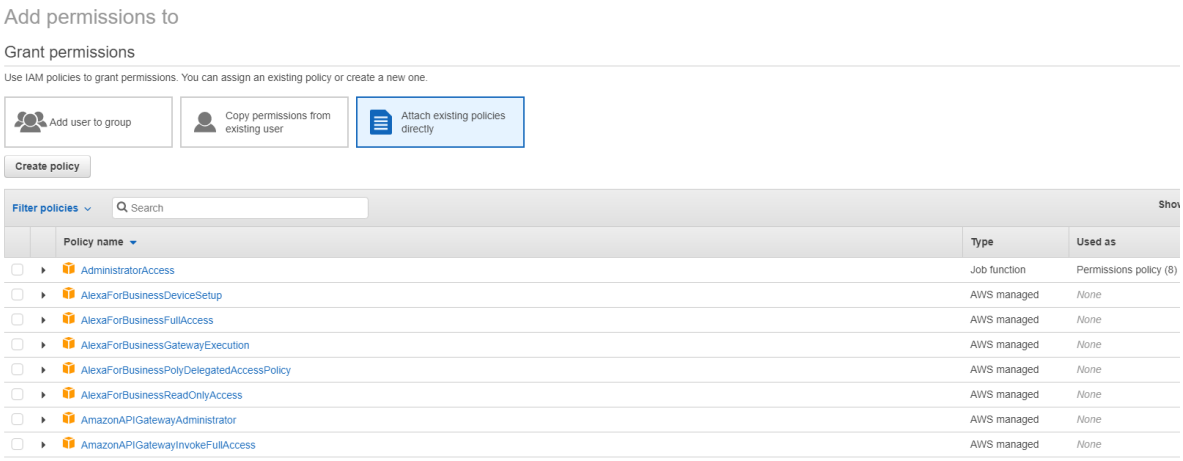
IAM-Berechtigungen festlegen

Legen Sie die Berechtigungen im Bereich **IAM** der AWS Management Console fest:

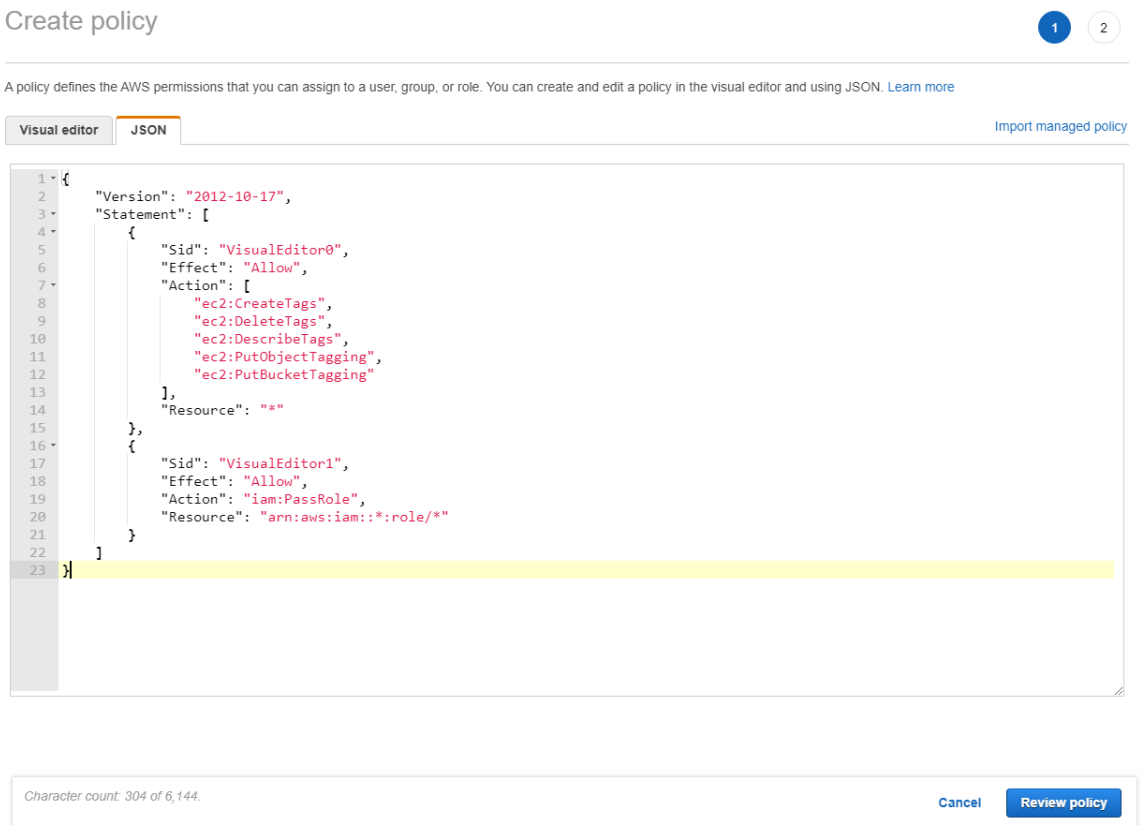
1. Wählen Sie im Bereich **Summary** die Registerkarte **Permissions**.
2. Wählen Sie **Add Permissions**.



Erteilen Sie im Fenster **Add Permissions to** folgende Berechtigungen:



Verwenden Sie Folgendes als Beispiel für die Registerkarte **JSON**:



> **Tipp:**
>
> Das JSON-Beispiel enthält möglicherweise nicht alle Berechtigungen für Ihre Umgebung. Weitere Informationen finden Sie unter How to Define Identity Access Management Permissions Running Citrix Virtual Apps and Desktops on AWS.

Erforderliche AWS-Berechtigungen

Dieser Abschnitt enthält die vollständige Liste der AWS-Berechtigungen.

> **Hinweis:**
>
> Die Berechtigung *iam:PassRole* wird nur für **role_based_auth** benötigt.

Hostverbindung erstellen

Eine neue Hostverbindung wird unter Verwendung der Informationen von AWS hinzugefügt.

```
{

    "Version": "2012-10-17",
    "Statement": [
        {
```



```
6
7               "Action": [
8                   "ec2:DescribeAvailabilityZones",
9                   "ec2:DescribeImages",
10                  "ec2:DescribeInstances",
11                  "ec2:DescribeInstanceTypes",
12                  "ec2:DescribeSecurityGroups",
13                  "ec2:DescribeSubnets",
14                  "ec2:DescribeVpcs"
15              ],
16              "Effect": "Allow",
17              "Resource": "*"
18          }
19
20      ]
21  }
22
23  <!--NeedCopy-->
```

Energieverwaltung virtueller Maschinen

Maschineninstanzen werden ein- oder ausgeschaltet.

```
1  {
2
3      "Version": "2012-10-17",
4      "Statement": [
5          {
6
7              "Action": [
8                  "ec2:AttachVolume",
9                  "ec2:CreateVolume",
10                 "ec2:DeleteVolume",
11                 "ec2:DescribeInstances",
12                 "ec2:DescribeVolumes",
13                 "ec2:DetachVolume",
14                 "ec2:StartInstances",
15                 "ec2:StopInstances"
16             ],
17             "Effect": "Allow",
18             "Resource": "*"
19         }
20
21     ]
22  }
23
24  <!--NeedCopy-->
```


Erstellen, Aktualisieren oder Löschen von VMs

Ein Maschinenkatalog wird mit VMs erstellt, aktualisiert oder gelöscht, die als AWS-Instanzen bereitgestellt werden.

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Action": [
                "ec2:AttachVolume",
                "ec2:AssociateIamInstanceProfile",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateImage",
                "ec2:CreateLaunchTemplate",
                "ec2:CreateSecurityGroup",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DeleteVolume",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeLaunchTemplates",
                "ec2:DescribeLaunchTemplateVersions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRegions",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcs",
                "ec2:DetachVolume",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Effect": "Allow",
            "Resource": "*"
         }
 ,
        {

            "Action": [
                "ec2:AuthorizeSecurityGroupEgress",
```



```
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress"
            ],
            "Effect": "Allow",
            "Resource": "*"
         }
,
        {

            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:PutBucketAcl",
                "s3:PutBucketTagging",
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject",
                "s3:PutObjectTagging"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::citrix*"
         }
,
        {

            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
         }

    ]
 }

<!--NeedCopy-->
```

Hinweis:

Der Abschnitt zu EC2, der sich auf Sicherheitsgruppen bezieht, wird nur benötigt, wenn während der Katalogerstellung eine Isolationssicherheitsgruppe für die Vorbereitungs-VM erstellt werden muss. Sobald dies abgeschlossen ist, sind diese Berechtigungen nicht erforderlich.

Direkter Disk-Upload und -Download Durch den direkten Disk-Upload entfällt die Volumeworker-Anforderung beim Provisioning von Maschinenkatalogen. Stattdessen werden von AWS bereitgestellte öffentliche APIs verwendet. Diese Funktion reduziert die mit zusätzlichen Speicherkonten verbundenen Kosten und die komplexe Verwaltung von Volumeworker-Prozessen.

> **Hinweis:**
>
> Die Volumeworker-Unterstützung ist veraltet.

Folgende Berechtigungen müssen zur Richtlinie hinzugefügt werden:

- `ebs:StartSnapshot`
- `ebs:GetSnapshotBlock`
- `ebs:PutSnapshotBlock`
- `ebs:CompleteSnapshot`
- `ebs:ListSnapshotBlocks`
- `ebs:ListChangedBlocks`
- `ec2:CreateSnapshot`
- `ec2:DeleteSnapshot`
- `ec2:DescribeLaunchTemplates`

> **Wichtig:**
>
> - Sie können eine VM zu vorhandenen Maschinenkatalogen ohne Volumeworker-Prozesse wie Volumeworker-AMI und Volumeworker-VM hinzufügen.
> - Wenn Sie einen vorhandenen Katalog löschen, in dem Volumeworker verwendet wurde, werden alle Artefakte inklusive zugehörigem Volumeworker gelöscht.

EBS-Verschlüsselung erstellter Volumes

EBS kann neu erstellte Volumes automatisch verschlüsseln, wenn das AMI verschlüsselt ist oder EBS zur Verschlüsselung aller neuen Volumes konfiguriert ist. Zum Implementieren der Funktionalität müssen jedoch die folgenden Berechtigungen in der IAM-Richtlinie enthalten sein.

```
{

     "Version": "2012-10-17",
     "Statement": [
        {

            "Effect": "Allow",
            "Action": [
                 "kms:CreateGrant",
                 "kms:Decrypt",
                 "kms:DescribeKey",
```



```
                    "kms:GenerateDataKeyWithoutPlainText",
                    "kms:ReEncryptTo",
                    "kms:ReEncryptFrom"
                ],
                "Resource": "*"
            }

        ]
    }

<!--NeedCopy-->
```

Hinweis:

Die Berechtigungen können durch Hinzufügen eines Abschnitts "Resource"und "Condition" nach Ermessen des Benutzers auf bestimmte Schlüssel beschränkt werden. Beispiel: **KMS-Berechtigungen mit Bedingung**:

```
{

     "Version": "2012-10-17",
     "Statement": [
        {

            "Effect": "Allow",
            "Action": [
                 "kms:CreateGrant",
                 "kms:Decrypt",
                 "kms:DescribeKey",
                 "kms:GenerateDataKeyWithoutPlainText",
                 "kms:ReEncryptTo",
                 "kms:ReEncryptFrom"
            ],
            "Resource": [
                "arn:aws:kms:us-east-2:123456789012:key/abcd1234-a123
                   -456d-a12b-a123b4cd56ef"
            ],
            "Condition": {

                "Bool": {

                    "kms:GrantIsForAWSResource": true
                 }

             }

         }

    ]
}

<!--NeedCopy-->
```


Die folgende Schlüsselrichtlinienanweisung ist die komplette Standardrichtlinie für KMS-Schlüssel, die erforderlich ist, damit das Konto unter Einsatz von IAM-Richtlinien Berechtigungen für alle Aktionen (kms: *) für den KMS-Schlüssel delegieren kann.

```
{

"Sid": "Enable IAM policies",
"Effect": "Allow",
"Principal": {

"AWS": "arn:aws:iam::111122223333:root"
 }
 ,
"Action": "kms:",
"Resource": ""
 }

<!--NeedCopy-->
```

Weitere Informationen finden Sie in der offiziellen AWS-Dokumentation unter AWS Key Management Service.

Rollenbasierte IAM-Authentifizierung

Die folgenden Berechtigungen werden zur Unterstützung der rollenbasierten Authentifizierung hinzugefügt.

```
{

     "Version": "2012-10-17",
     "Statement": [
        {

            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::*:role/*"
         }

    ]
 }

<!--NeedCopy-->
```

Richtlinie für Mindest-IAM-Berechtigungen

Die folgende JSON kann für alle derzeit unterstützten Features verwendet werden. Unter Verwendung der Richtlinie können Sie Hostverbindungen erstellen, VMs erstellen, aktualisieren und löschen und die Energieverwaltung durchführen.

Die Richtlinie kann auf die Benutzer angewendet werden (siehe IAM-Berechtigungen definieren) oder Sie können die rollenbasierte Authentifizierung über den Sicherheitsschlüssel **role_based_auth** und den geheimen Schlüssel verwenden.

> **Wichtig:**
>
> Um **role_based_auth** zu verwenden, konfigurieren Sie zunächst die gewünschte IAM-Rolle auf allen Delivery Controllers auf unserer Site. Fügen Sie unter Verwendung von Web Studio die Hostingverbindung hinzu und geben Sie role_based_auth für den Authentifizierungsschlüssel und das Geheimnis an. Eine Hostingverbindung mit diesen Einstellungen verwendet dann die rollenbasierte Authentifizierung.

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Action": [
                "ec2:AttachVolume",
                "ec2:AssociateIamInstanceProfile",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateImage",
                "ec2:CreateLaunchTemplate",
                "ec2:CreateNetworkInterface",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DeleteLaunchTemplate",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteSnapshot",
                "ec2:DeleteTags",
                "ec2:DeleteVolume",
                "ec2:DeregisterImage",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeLaunchTemplates",
                "ec2:DescribeLaunchTemplateVersions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRegions",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcs",
```



```
                "ec2:DetachVolume",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:RebootInstances",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
,
        {

            "Action": [
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
,
        {

            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:DeleteObject",
                "s3:GetObject",
                "s3:PutBucketAcl",
                "s3:PutObject",
                "s3:PutBucketTagging",
                "s3:PutObjectTagging"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::citrix*"
        }
,
        {

            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
            ],
```



```
            "Effect": "Allow",
            "Resource": "*"
        }
,
        {

            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:Decrypt",
                "kms:DescribeKey",
                "kms:GenerateDataKeyWithoutPlainText",
                "kms:GenerateDataKey",
                "kms:ReEncryptTo",
                "kms:ReEncryptFrom"
            ],
            "Resource": "*"
        }
,
        {

            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::*:role/*"
        }

    ]
}

<!--NeedCopy-->
```

Hinweis:

- Der Abschnitt zu EC2, der sich auf SecurityGroups bezieht, wird nur benötigt, wenn während der Katalogerstellung eine Isolationssicherheitsgruppe für die Vorbereitungs-VM erstellt werden muss. Sobald dies abgeschlossen ist, sind diese Berechtigungen nicht erforderlich.
- Der KMS-Abschnitt ist nur bei Verwendung der EBS-Volume-Verschlüsselung erforderlich.
- Der Berechtigungsbereich iam:PassRole wird nur für **role_based_auth** benötigt.
- Anstelle eines Vollzugriffs können spezifische Berechtigungen auf Ressourcenebene gemäß Ihren Anforderungen und Ihrer Umgebung hinzugefügt werden. Weitere Informationen finden Sie in den AWS-Dokumenten Demystifying EC2 Resource-Level Permissions und Access management for AWS resources.

So geht es weiter

- Wenn dies die erste Bereitstellung ist, lesen Sie Maschinenkatalog erstellen.
- AWS-spezifische Informationen finden Sie unter AWS-Katalog erstellen.

Weitere Informationen

- Verbindungen und Ressourcen
- Maschinenkataloge erstellen

Verbindung zu XenServer

June 27, 2024

Unter Verbindungen und Ressourcen erstellen und verwalten werden die Assistenten zum Erstellen einer Verbindung beschrieben. Die folgenden Informationen beziehen sich speziell auf XenServer-Virtualisierungsumgebungen.

> **Hinweis:**
>
> Bevor Sie eine Verbindung zu XenServer herstellen, müssen Sie zunächst Ihr XenServer-Konto als Ressourcenstandort eingerichtet haben. Weitere Informationen finden Sie unter XenServer-Virtualisierungsumgebungen.

Erstellen einer Verbindung zu XenServer

Beim Erstellen einer Verbindung zu XenServer (früher Citrix Hypervisor) müssen Sie die Anmeldeinformationen eines VM-Hauptadministrators oder eines höherrangigen Benutzers eingeben.

Citrix empfiehlt, HTTPS zum Sicheren der Kommunikation mit XenServer zu verwenden. Um HTTPS zu verwenden, müssen Sie das standardmäßig mit XenServer installierte SSL-Zertifikat ersetzen (siehe CTX128656).

Sie können hohe Verfügbarkeit konfigurieren, wenn dies auf dem XenServer-Server aktiviert ist. Citrix empfiehlt, dass Sie alle Server im Pool (über Server mit hoher Verfügbarkeit bearbeiten) auswählen, um die Kommunikation mit dem XenServer-Server zu ermöglichen, wenn der Poolmaster ausfällt.

Sie können einen GPU-Typ und eine GPU-Gruppe oder Passthrough auswählen, wenn der XenServer vGPU unterstützt. Es wird angezeigt, ob die Auswahl dedizierte GPU-Ressourcen umfasst.

Wenn Sie auf XenServer-Hosts lokalen Speicher für die temporäre Datenspeicherung verwenden, vergewissern Sie sich, 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 Sie Citrix Provisioning (zuvor "Provisioning Services") und Maschinenerstellungsdienste (MCS) zum Bereitstellen folgender Elemente:

- Legacy-BIOS für unterstützte Desktop- oder Serverbetriebssystem-VMs.
- UEFI für unterstützte Desktop- oder Serverbetriebssystem-VMs, mit Secure Boot.

> **Hinweis:**
>
> Bei der Konfiguration von MCS sind Poolbetreiberberechtigungen oder höher erforderlich.

Verwenden von IntelliCache für XenServer-Verbindungen

Durch den Einsatz von IntelliCache werden gehostete VDI-Bereitstellungen kostengünstiger, da eine Kombination aus freigegebenem und lokalem Speicher verwendet werden kann. Dies verbessert die Leistung und reduziert den Datenverkehr im Netzwerk. Das Masterimage aus dem freigegebenen Speicher wird im lokalen Speicher zwischengespeichert, wodurch die Anzahl der Lesevorgänge im freigegebenen Speicher reduziert wird. Bei gemeinsam genutzten Desktops werden Schreibvorgänge auf den 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 zu verwenden, müssen Sie es in diesem Produkt und XenServer aktivieren.

- Bei der Installation von XenServer wählen Sie **Enable thin provisioning (Optimized storage for 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 für XenServer.
- In Citrix Virtual Apps and Desktops ist IntelliCache standardmäßig deaktiviert. Sie können die Einstellung nur beim Erstellen einer XenServer-Verbindung ändern, IntelliCache kann später nicht deaktiviert werden. Gehen Sie folgendermaßen vor, wenn Sie eine XenServer-Verbindung hinzufügen:
  - Wählen Sie als Speichertyp **Freigegeben** aus.
  - Aktivieren Sie das Kontrollkästchen **IntelliCache verwenden**.

Erforderliche XenServer-Berechtigungen

Die XenServer-Berechtigungen sind rollenbasiert (RBAC). Mit der Funktion Role-Based Access Control (RBAC) in XenServer können Sie Ihren Benutzern Rollen und Berechtigungen zuweisen, um zu steuern, wer Zugriff auf Ihren XenServer hat und welche Aktionen sie ausführen können. Das XenServer RBAC-System ordnet einen Benutzer (oder eine Gruppe von Benutzern) definierten Rollen (einem benannten Satz von Berechtigungen) zu. Den Rollen sind XenServer-Berechtigungen zugeordnet, um bestimmte Operationen auszuführen.

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

Aufgabe	Erforderliche Mindestrolle
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.

So geht es weiter

- Wenn dies die erste Bereitstellung ist, lesen Sie Maschinenkatalog erstellen.
- Alle XenServer-spezifischen Informationen finden Sie unter XenServer-Katalog erstellen

Weitere Informationen

- Verbindungen und Ressourcen
- Maschinenkataloge erstellen

Verbindung zu Google-Cloudumgebungen

June 27, 2024

Unter Verbindungen und Ressourcen erstellen und verwalten werden die Assistenten zum Erstellen einer Verbindung beschrieben. Die folgenden Informationen beziehen sich speziell auf Google-Cloudumgebungen.

> **Hinweis:**
>
> Bevor Sie eine Verbindung zu Google-Cloudumgebungen herstellen, müssen Sie zunächst Ihr Google-Cloudkonto als Ressourcenstandort eingerichtet haben. Siehe Google Cloud-Umgebungen.

Hinzufügen einer Verbindung

Folgen Sie den Anweisungen unter Erstellen einer Verbindung und von Ressourcen. Die folgende Beschreibung erläutert, wie Sie eine Hostverbindung einrichten:

1. Wählen Sie unter **Verwalten > Konfiguration** im linken Bereich **Hosting**.
2. Wählen Sie in der Aktionsleiste **Verbindung und Ressourcen hinzufügen**.
3. Wählen Sie auf der Seite **Verbindung** die Optionen **Neue Verbindung erstellen** und **Citrix-Provisioningtools** und wählen Sie **Weiter**.
   - **Verbindungstyp**. Wählen Sie im Menü die Option **Google Cloud**.
   - **Verbindungsname**. Geben Sie einen Namen für die Verbindung ein.
4. Wählen Sie auf der Seite **Region** einen Projektnamen aus dem Menü aus, wählen Sie die Region, in der sich die gewünschten Ressourcen befinden, und wählen Sie **Weiter**.
5. Geben Sie auf der Seite **Netzwerk** einen Ressourcennamen ein, wählen Sie ein virtuelles Netzwerk aus dem Menü aus, wählen Sie einen Teilbereich (Subset) und wählen Sie **Weiter**. Mit dem Ressourcennamen kann diese Kombination von Region und Netzwerk identifiziert werden. Virtuelle Netzwerke mit dem Namenssuffix *(Shared)* sind freigegebene VPCs. Wenn Sie eine IAM-Rolle auf Subnetzebene für eine freigegebene VPC konfigurieren, werden nur bestimmte Subnetze der freigegebenen VPC in der Subnetzliste angezeigt.

   > **Hinweis:**
   >
   > - Der Ressourcenname muss aus 1–64 Zeichen bestehen, er darf nicht ausschließlich aus Leerzeichen bestehen, und folgende Zeichen sind nicht erlaubt: `\ / ; : # . * ? = < > | [ ] { } "' ( )' )`.

6. Überprüfen Sie die Informationen auf der Seite **Zusammenfassung** und wählen Sie **Fertigstellen**, um das Fenster **Verbindung und Ressourcen hinzufügen** zu schließen.

Nach dem Erstellen der Verbindung und der Ressourcen wird die erstellte Verbindung samt Ressourcen aufgelistet. Wählen Sie zum Konfigurieren der Verbindung diese aus und wählen Sie in der Aktionsleiste die entsprechende Option.

Sie können außerdem die unter der Verbindung erstellten Ressourcen löschen, umbenennen oder testen. Wählen Sie hierfür die Ressource unter der Verbindung aus und wählen Sie in der Aktionsleiste die entsprechende Option.

Service-Endpunkt-URLs

Sie müssen Zugriff auf die folgenden URLs haben:

- `https://oauth2.googleapis.com`
- `https://cloudresourcemanager.googleapis.com`
- `https://compute.googleapis.com`
- `https://storage.googleapis.com`
- `https://cloudbuild.googleapis.com`

Google Cloud-Projekte

Es gibt grundsätzlich zwei Arten von Google Cloud-Projekten:

- Bereitstellungsprojekt: Hier besitzt das aktuelle Administratorkonto die bereitgestellten Maschinen im Projekt. Das Projekt wird auch als "lokales Projekt"bezeichnet.
- Freigegebene-VPC-Projekt: Projekt, in dem im Bereitstellungsprojekt erstellte Maschinen die VPC aus dem Freigegebene-VPC-Projekt verwenden. Das für das Bereitstellungsprojekt verwendete Administratorkonto hat in diesem Projekt eingeschränkte Berechtigungen, spezifisch hat es nur Berechtigungen zur Verwendung der VPC.

Sichere Umgebung für von GCP verwalteten Netzwerkverkehr erstellen

Sie können den Google-Zugriff auf Ihre Google Cloud-Projekte auf den privaten Zugriff einschränken. Diese Implementierung erhöht die Sicherheit beim Umgang mit vertraulichen Daten. Hierfür können Sie einen der folgenden Schritte ausführen:

- Schließen Sie die folgenden Eingangsregeln von VPC Service Controls für das Cloud Build-Dienstkonto ein. Wenn Sie diesen Schritt ausführen, stellen Sie keine sichere Umgebung für GCP-verwalteten Datenverkehr gemäß der folgenden Anleitung her.

```
Ingress Rule 1
From:
Identities:
<ProjectID>@cloudbuild.gserviceaccount.com
Source > All sources allowed
To:
Projects =
All projects
Services =
Service name: All services
<!--NeedCopy-->
```

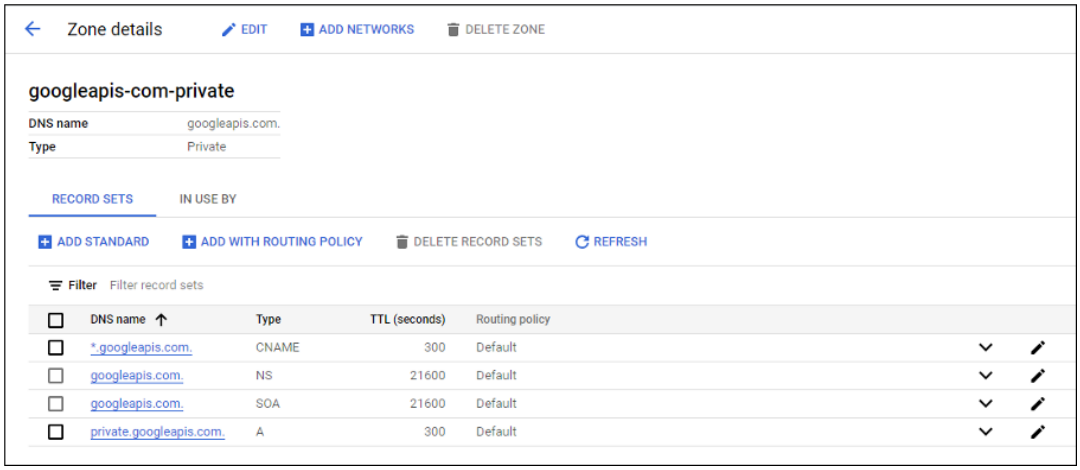
- Wenn Sie einen privaten Pool verwenden, fügen Sie `UsePrivateWorkerPool` zu `CustomProperties` hinzu. Informationen zum privaten Workerpool finden Sie unter Private Pools –Übersicht.

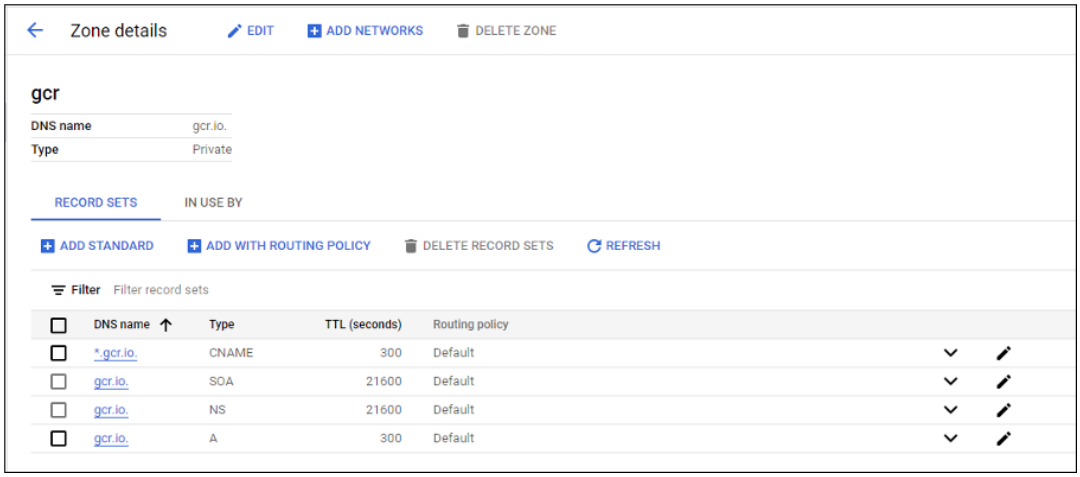
Anforderungen für die Schaffung einer sicheren Umgebung für den von GCP verwalteten Netzwerkverkehr

Für die Schaffung einer sicheren Umgebung für den von GCP verwalteten Netzwerkverkehr gelten folgende Anforderungen:

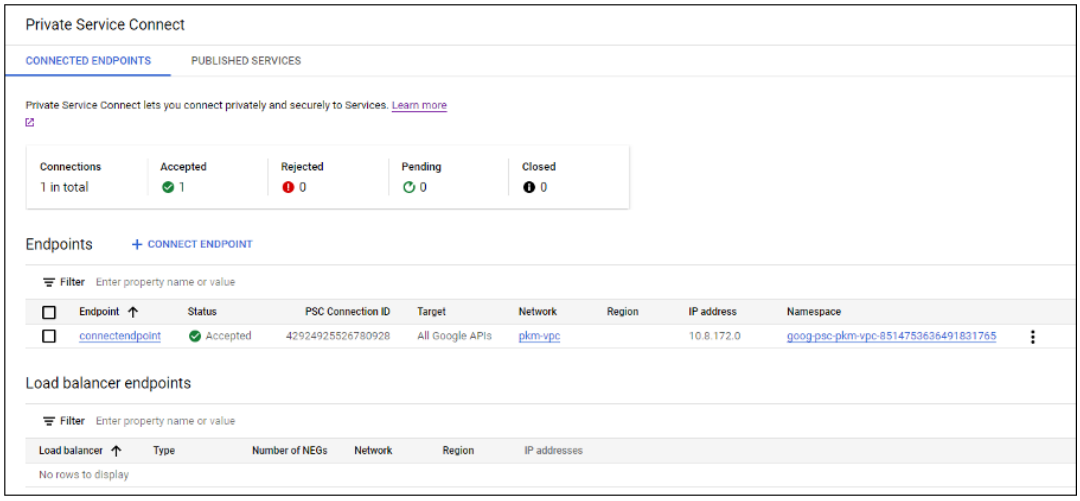
- Die Hostingverbindung muss sich im Wartungsmodus befinden, wenn Sie die benutzerdefinierten Eigenschaften aktualisieren.

- Um private Workerpools verwenden zu können, sind die folgenden Änderungen erforderlich:
  - Fügen Sie für das Citrix Cloud Service-Konto die folgenden IAM-Rollen hinzu:
    * Cloud Build-Dienstkonto
    * Compute Instance-Administrator
    * Dienstkontobenutzer
    * Dienstkonto-Token-Ersteller
    * Inhaber von Cloud Build-Workerpools
  - Erstellen Sie das Citrix Cloud Service-Konto in demselben Projekt, das Sie für die Erstellung einer Hostingverbindung verwenden.
  - Richten Sie DNS-Zonen für **`private`**`.googleapis.com` und `gcr.io` ein (siehe DNS-Konfiguration).

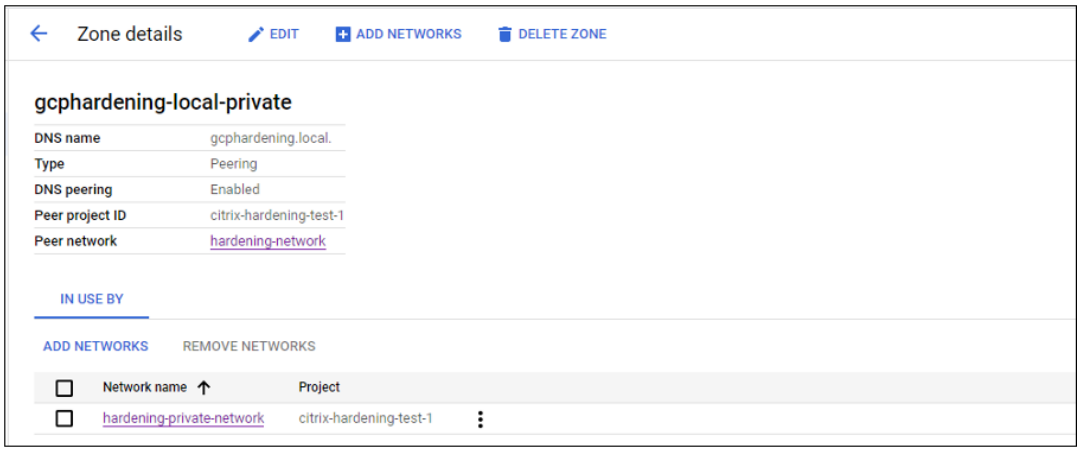




  - Richten Sie die private Netzwerkadressübersetzung (NAT) ein oder verwenden Sie Private Service Connect. Weitere Informationen finden Sie unter Zugriff auf Google-APIs über Endpunkte.



- Wenn Sie eine Peering-VPC verwenden, erstellen Sie ein Cloud-DNS-Zonen-Peering zur Peering-VPC. Weitere Informationen finden Sie unter Peering-Zone erstellen.



- Richten Sie in VPC Service Controls Ausgangsregeln ein, damit die APIs und VMs mit dem Internet kommunizieren können. Eingangsregeln sind optional. Beispiel:

```
Egress Rule 1
From:
Identities:ANY_IDENTITY
To:
Projects =
All projects
Service =
Service name: All services
<!--NeedCopy-->
```

Privaten Workerpool aktivieren

Um den privaten Workerpool zu aktivieren, legen Sie die benutzerdefinierten Eigenschaften für die Hostverbindung wie folgt fest:

1. Öffnen Sie ein PowerShell-Fenster auf dem Delivery Controller-Host, oder verwenden Sie das Remote PowerShell-SDK. Weitere Informationen zum Remote PowerShell SDK finden Sie unter SDKs und APIs.
2. Führen Sie die folgenden Befehle aus:

   a) `Add-PSSnapin citrix*`
   b) `cd XDHyp:\Connections\`
   c) `dir`

3. Kopieren Sie die `CustomProperties` von der Verbindung in einen Editor.
4. Hängen sie die Eigenschaftseinstellung `<Property xsi:type="StringProperty" Name="UsePrivateWorkerPool"Value="True"/>` an. Beispiel:

```
1 ```
2 <CustomProperties xmlns:xsi="http://www.w3.org/2001/XMLSchema-
     instance" xmlns="http://schemas.citrix.com/2014/xd/
     machinecreation">
3 <Property xsi:type="StringProperty" Name="UsePrivateWorkerPool"
     Value="True"/>
4 </CustomProperties>
5 <!--NeedCopy--> ```
```

5. Weisen Sie im PowerShell-Fenster den geänderten benutzerdefinierten Eigenschaften eine Variable zu. Beispiel:
   `$customProperty = '<CustomProperties...</CustomProperties>'`.
6. Führen Sie `$gcpServiceAccount = "<ENTER YOUR SERVICE ACCOUNT EMAIL HERE>"` aus.
7. Führen Sie `$gcpPrivateKey = "<ENTER YOUR SERVICE ACCOUNT PRIVATE KEY HERE AFTER REMOVING ALL INSTANCES OF \n >"` aus.
8. Führen Sie `$securePassword = ConvertTo-SecureString $gcpPrivateKey -AsPlainText -Force` aus.
9. Führen Sie den folgenden Befehl aus, um eine bestehende Hostverbindung zu aktualisieren:

```
1 Set-Item -PassThru -Path @('XDHyp:\Connections\&lt;ENTER YOUR
     CONNECTION NAME HERE&gt;') -SecurePassword $securePassword -
     UserName $gcpServiceAccount -CustomProperties $customProperty
2 <!--NeedCopy-->
```

Erforderliche GCP-Berechtigungen

Dieser Abschnitt enthält die vollständige Liste der GCP-Berechtigungen. Verwenden Sie sämtliche Berechtigungen, wie im Abschnitt angegeben, um eine ordnungsgemäße Funktionalität sicherzustellen.

> **Hinweis:**
>
> Ab dem 29. April 2024 führt GCP Änderungen am Standardverhalten von Cloud Build Services und der Verwendung von Dienstkonten ein. Weitere Informationen finden Sie unter Änderungen des Cloud Build-Dienstkontos. Ihre bestehenden Google-Projekte mit aktivierter Cloud Build API vor dem 29. April 2024 sind von dieser Änderung nicht betroffen. Wenn Sie jedoch das bestehende Cloud Build Service-Verhalten nach dem 29. April beibehalten möchten, können Sie die Organisationsrichtlinie erstellen oder anwenden, um die Durchsetzung der Einschränkungen zu deaktivieren, bevor Sie die API aktivieren. Wenn Sie die neue Organisationsrichtlinie festlegen, können Sie weiterhin den vorhandenen Berechtigungen in diesem Abschnitt und den Elementen folgen, die als **Vor der Änderung des Cloud Build Service-Kontos** markiert sind. Wenn nicht, folgen Sie den vorhandenen Berechtigungen und Elementen, die als **Nach der Änderung des Cloud Build Service-Kontos** markiert sind.

Hostverbindung erstellen

- Mindestberechtigungen für das Citrix Cloud-Dienstkonto im Bereitstellungsprojekt:

```
compute.instanceTemplates.list
compute.instances.list
compute.networks.list
compute.projects.get
compute.regions.list
compute.subnetworks.list
compute.zones.list
resourcemanager.projects.get
<!--NeedCopy-->
```

  Die folgenden von Google definierten Rollen haben die oben aufgeführten Berechtigungen:

  - Compute Admin
  - Cloud Datastore User

- Weitere für die freigegebene VPC für das Citrix Cloud-Dienstkonto im Freigegebene-VPC-Projekt erforderliche Berechtigungen:

```
compute.networks.list
compute.subnetworks.list
resourcemanager.projects.get
<!--NeedCopy-->
```

  Die folgenden von Google definierten Rollen haben die oben aufgeführten Berechtigungen:

  - Compute Network User

Energieverwaltung virtueller Maschinen

Mindestberechtigungen, die für das Citrix Cloud-Dienstkonto im Bereitstellungsprojekt erforderlich sind, wenn Kataloge nur mit Energieverwaltung verwendet werden:

```
compute.instanceTemplates.list
compute.instances.list
compute.instances.get
compute.instances.reset
compute.instances.resume
compute.instances.start
compute.instances.stop
compute.instances.suspend
compute.networks.list
compute.projects.get
compute.regions.list
compute.subnetworks.list
compute.zones.list
resourcemanager.projects.get
compute.zoneOperations.get
<!--NeedCopy-->
```

Die folgenden von Google definierten Rollen haben die oben aufgeführten Berechtigungen:

- Compute Admin
- Cloud Datastore User

Erstellen, Aktualisieren oder Löschen von VMs

- Mindestberechtigungen für das Citrix Cloud-Dienstkonto im Bereitstellungsprojekt:

```
cloudbuild.builds.create
cloudbuild.builds.get
cloudbuild.builds.list
compute.acceleratorTypes.list
compute.diskTypes.get
compute.diskTypes.list
compute.disks.create
compute.disks.createSnapshot
compute.disks.delete
compute.disks.get
compute.disks.list
compute.disks.setLabels
compute.disks.use
compute.disks.useReadOnly
compute.firewalls.create
compute.firewalls.delete
compute.firewalls.list
compute.globalOperations.get
compute.images.create
compute.images.delete
```



```
compute.images.get
compute.images.list
compute.images.setLabels
compute.images.useReadOnly
compute.instanceTemplates.create
compute.instanceTemplates.delete
compute.instanceTemplates.get
compute.instanceTemplates.list
compute.instanceTemplates.useReadOnly
compute.instances.attachDisk
compute.instances.create
compute.instances.delete
compute.instances.detachDisk
compute.instances.get
compute.instances.list
compute.instances.reset
compute.instances.resume
compute.instances.setDeletionProtection
compute.instances.setLabels
compute.instances.setMetadata
compute.instances.setServiceAccount
compute.instances.setTags
compute.instances.start
compute.instances.stop
compute.instances.suspend
compute.machineTypes.get
compute.machineTypes.list
compute.networks.list
compute.networks.updatePolicy
compute.nodeGroups.list
compute.nodeTemplates.get
compute.projects.get
compute.regions.list
compute.snapshots.create
compute.snapshots.delete
compute.snapshots.list
compute.snapshots.get
compute.snapshots.setLabels
compute.snapshots.useReadOnly
compute.subnetworks.get
compute.subnetworks.list
compute.subnetworks.use
compute.zoneOperations.get
compute.zoneOperations.list
compute.zones.get
compute.zones.list
iam.serviceAccounts.actAs
resourcemanager.projects.get
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.buckets.list
storage.buckets.update
```



```
74  storage.objects.create
75  storage.objects.delete
76  storage.objects.get
77  storage.objects.list
78  compute.networks.get
79  compute.resourcePolicies.use
80
81  <!--NeedCopy-->
```

Die folgenden von Google definierten Rollen haben die oben aufgeführten Berechtigungen:

- Compute Admin
- Speicher-Administrator
- Cloud Build-Editor
- Dienstkontobenutzer
- Cloud Datastore User

- Weitere für die freigegebene VPC für das Citrix Cloud-Dienstkonto im Freigegebene-VPC-Projekt erforderliche Berechtigungen zur Erstellung einer Hostingeinheit unter Verwendung der VPC und des Subnetzes aus dem Freigegebene-VPC-Projekt:

```
1  compute.firewalls.list
2  compute.networks.list
3  compute.projects.get
4  compute.regions.list
5  compute.subnetworks.get
6  compute.subnetworks.list
7  compute.subnetworks.use
8  compute.zones.list
9  resourcemanager.projects.get
10 <!--NeedCopy-->
```

Die folgenden von Google definierten Rollen haben die oben aufgeführten Berechtigungen:

- Compute Network User
- Cloud Datastore User

- (Vor der Änderung des Cloud Build Service-Kontos): Mindestberechtigungen für das Cloud Build-Dienstkonto im Bereitstellungprojekt, die vom Google Cloud Build-Dienst beim Herunterladen des Anweisungsdatenträgers auf MCS erfordert werden:
- (Nach der Änderung des Cloud Build Service-Kontos): Mindestberechtigungen für das Cloud Compute-Dienstkonto im Bereitstellungprojekt, die vom Google Cloud Compute Service beim Herunterladen des Anweisungsdatenträgers auf MCS erfordert werden:

```
1  compute.disks.create
2  compute.disks.delete
3  compute.disks.get
4  compute.disks.list
```



```
compute.disks.setLabels
compute.disks.use
compute.disks.useReadOnly
compute.images.get
compute.images.list
compute.images.useReadOnly
compute.instances.create
compute.instances.delete
compute.instances.get
compute.instances.getSerialPortOutput
compute.instances.list
compute.instances.setLabels
compute.instances.setMetadata
compute.instances.setServiceAccount
compute.machineTypes.list
compute.networks.get
compute.networks.list
compute.projects.get
compute.subnetworks.list
compute.subnetworks.use
compute.subnetworks.useExternalIp
compute.zoneOperations.get
compute.zones.list
iam.serviceAccounts.actAs
logging.logEntries.create
pubsub.topics.publish
resourcemanager.projects.get
source.repos.get
source.repos.list
storage.buckets.create
storage.buckets.get
storage.buckets.list
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
<!--NeedCopy-->
```

Die folgenden von Google definierten Rollen haben die oben aufgeführten Berechtigungen:

- Cloud Build Service-Konto (Nach der Änderung des Cloud Build Service-Kontos ist es das Cloud Compute Service-Konto)
- Compute Instance-Administrator
- Dienstkontobenutzer

- Mindestberechtigungen für das Cloud Compute-Dienstkonto im Bereitstellungprojekt, die vom Google Cloud Build-Dienst beim Herunterladen des Anweisungsdatenträgers auf MCS erfordert werden:

```
resourcemanager.projects.get
storage.objects.create
storage.objects.get
```



```
storage.objects.list
<!--NeedCopy-->
```

Die folgenden von Google definierten Rollen haben die oben aufgeführten Berechtigungen:

- Compute Network User
- Storage Account User
- Cloud Datastore User

- (Vor der Änderung des Cloud Build Service-Kontos): Zusätzliche Berechtigungen für die freigegebene VPC für das Cloud Build-Dienstkonto im Bereitstellungprojekt, die vom Google Cloud Build-Dienst beim Herunterladen des Anweisungsdatenträgers auf MCS erfordert werden:
- (Nach der Änderung des Cloud Build Service-Kontos): Zusatzberechtigungen für das Cloud Compute-Dienstkonto für Shared VPC im Bereitstellungprojekt, die vom Google Cloud Compute Service beim Herunterladen des Anweisungsdatenträgers auf MCS erfordert werden:

```
compute.firewalls.list
compute.networks.list
compute.subnetworks.list
compute.subnetworks.use
resourcemanager.projects.get
<!--NeedCopy-->
```

Die folgenden von Google definierten Rollen haben die oben aufgeführten Berechtigungen:

- Compute Network User
- Storage Account User
- Cloud Datastore User

- Zusätzliche Berechtigungen für den Cloud-Schlüsselverwaltungsdienst (KMS) für das Citrix Cloud-Dienstkonto im Bereitstellungsprojekt:

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.list
cloudkms.keyRings.get
cloudkms.keyRings.list
<!--NeedCopy-->
```

Die folgenden von Google definierten Rollen haben die oben aufgeführten Berechtigungen:

- Compute KMS Viewer

Allgemeine Berechtigungen

Im Folgenden sind die Berechtigungen für das Citrix Cloud-Dienstkonto im Provisioning-Projekt für alle in MCS unterstützten Funktionen aufgeführt. Diese Berechtigungen ab jetzt die beste Kompatibil-

ität:

```
resourcemanager.projects.get
cloudbuild.builds.create
cloudbuild.builds.get
cloudbuild.builds.list
compute.acceleratorTypes.list
compute.diskTypes.get
compute.diskTypes.list
compute.disks.create
compute.disks.createSnapshot
compute.disks.delete
compute.disks.get
compute.disks.setLabels
compute.disks.use
compute.disks.useReadOnly
compute.firewalls.create
compute.firewalls.delete
compute.firewalls.list
compute.globalOperations.get
compute.images.create
compute.images.delete
compute.images.get
compute.images.list
compute.images.setLabels
compute.images.useReadOnly
compute.instanceTemplates.create
compute.instanceTemplates.delete
compute.instanceTemplates.get
compute.instanceTemplates.list
compute.instanceTemplates.useReadOnly
compute.instances.attachDisk
compute.instances.create
compute.instances.delete
compute.instances.detachDisk
compute.instances.get
compute.instances.list
compute.instances.reset
compute.instances.resume
compute.instances.setDeletionProtection
compute.instances.setLabels
compute.instances.setMetadata
compute.instances.setTags
compute.instances.start
compute.instances.stop
compute.instances.suspend
compute.instances.update
compute.instances.updateAccessConfig
compute.instances.updateDisplayDevice
compute.instances.updateSecurity
compute.instances.updateShieldedInstanceConfig
compute.instances.updateShieldedVmConfig
compute.machineTypes.get
compute.machineTypes.list
```



```
compute.networks.list
compute.networks.updatePolicy
compute.nodeGroups.list
compute.nodeTemplates.get
compute.projects.get
compute.regions.list
compute.snapshots.create
compute.snapshots.delete
compute.snapshots.list
compute.snapshots.get
compute.snapshots.setLabels
compute.snapshots.useReadOnly
compute.subnetworks.get
compute.subnetworks.list
compute.subnetworks.use
compute.subnetworks.useExternalIp
compute.zoneOperations.get
compute.zoneOperations.list
compute.zones.get
compute.zones.list
resourcemanager.projects.get
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.buckets.list
storage.buckets.update
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.list
cloudkms.keyRings.get
cloudkms.keyRings.list
compute.disks.list
compute.instances.setServiceAccount
compute.networks.get
compute.networks.use
compute.networks.useExternalIp
iam.serviceAccounts.actAs
compute.resourcePolicies.use
<!--NeedCopy-->
```

So geht es weiter

- Wenn dies die erste Bereitstellung ist, lesen Sie Maschinenkatalog erstellen.
- Spezielle Informationen zur Google Cloud Platform (GCP) finden Sie unter Google Cloud Platform-Katalog erstellen.

Weitere Informationen

- Verbindungen und Ressourcen
- Maschinenkataloge erstellen

Verbindung zu HPE Moonshot

June 27, 2024

Unter Verbindungen und Ressourcen erstellen und verwalten werden die Assistenten zum Erstellen einer Verbindung beschrieben. Die folgenden Informationen beziehen sich speziell auf HPE Moonshot.

> **Hinweis:**
>
> Bevor Sie eine Verbindung zu HPE Moonshot herstellen, müssen Sie Ihr HPE-Konto einrichten. Siehe HPE Moonshot Virtualisierungsumgebungen.

Verbindung erstellen

Sie können zum Einrichten einer Verbindung zu HPE Moonshot Folgendes verwenden:

- Web Studio
- PowerShell-Befehle

Verbindung mit Web Studio erstellen

1. Wählen Sie auf der Seite **Verbindung und Ressourcen hinzufügen** den Verbindungstyp **HPE Moonshot**.
2. Geben Sie die Verbindungsadresse Ihres Moonshot iLO Chassis Managers ein. Sie können eine IP-Adresse, einen Hostnamen oder einen FQDN für die Adresse verwenden.
3. Geben Sie Ihre Chassis-Administratoranmeldeinformationen und einen Verbindungsanzeigenamen ein.

Die Einrichtung der Verbindung endet, wenn eine der folgenden Situationen eintritt:

- Citrix Virtual Apps and Desktops erhält ein von einer öffentlichen Zertifizierungsstelle signiertes Zertifikat mit Fehlern: Eine Fehlermeldung wird angezeigt. Folgen Sie den angezeigten Anweisungen, um das Problem zu lösen. Andernfalls können Sie mit der Verbindungserstellung nicht fortfahren.

- Citrix Virtual Apps and Desktops erhält ein privates, von einer Zertifizierungsstelle signiertes Zertifikat. Eine Warnseite wird angezeigt. Vergleichen Sie den empfangenen Fingerabdruck mit dem des Servers, um die Gültigkeit des Zertifikats zu ermitteln. Wenn es gültig ist, wählen Sie **Zertifikat vertrauen** und klicken Sie auf **OK**, um mit der Verbindungserstellung fortzufahren. Citrix Virtual Apps and Desktops vertraut dann dem Zertifikat und speichert den Fingerabdruck für eine zukünftige Validierung.

Verbindung mithilfe von PowerShell-Befehlen erstellen

Wenn Sie eine Verbindung über PowerShell erstellen, geben Sie die folgenden Informationen an:

- IP: HPE Server-IP-Adresse
- Username: HPE-Benutzername
- Password: HPE-Kennwort

Beispiel:

```
1 New-Item -ConnectionType "Custom" -HypervisorAddress $IP -Metadata @{
2  "Citrix_Orchestration_Hypervisor_Secret_Allow_Edit"="false" }
3   -Path @("XDHyp:\Connections$connectionName") -Persist -PluginId "
       HPMoonshotFactory" -Scope @() -SecurePassword $Password -UserName
       $UserName -sslthumbprint $SslThumbprint New-
       BrokerHypervisorConnection -HypHypervisorConnectionUid
       $HypervisorConnectionID
4 <!--NeedCopy-->
```

> **Hinweis:**
>
> Der Parameter `sslthumbprint` ist nur für von privaten ZS signierte Zertifikate erforderlich.

Zertifikat- und Fingerabdruckvalidierung

Um eine Verbindung zu **HPE Moonshot** herzustellen, darf das Zertifikat keine Fehler enthalten und der Fingerabdruck muss einen korrekten Wert haben. Im Folgenden sind die Anwendungsfälle für die Zertifikat- und Fingerabdruckvalidierung aufgeführt:

- Das von einer öffentlichen Zertifizierungsstelle signiertes Zertifikat weist Fehler auf. Die Verbindung wird nicht erstellt. Sehen Sie sich die Fehlerdetails an und beheben Sie das Problem.
- Von einer öffentlichen Zertifizierungsstelle signiertes Zertifikat ohne Fehler. Die Verbindung wird erstellt und der Wert von `SslThumbprints` ist **Null**.
- Von einer privaten Zertifizierungsstelle signiertes Zertifikat ohne Fehler und Wert `sslthumbprint`. Die Verbindung wird mit einem korrekten `SslThumbprints`-Wert erstellt.

- Von einer privaten ZS signiertes Zertifikat mit einem falschen Fingerabdruckwert. Die Verbindung wird nicht erstellt.
- Von einer privaten Zertifizierungsstelle signiertes Zertifikat ohne Fehler. Die Verbindung wird erstellt. `SSlThumbprints` ist **Null**, wenn die Verbindung erstellt wird. `SSlThumbprints` wird vom Sitedienst auf einen Wert aktualisiert.

Verbindungen verwalten

In diesem Abschnitt erfahren Sie, wie Sie Verbindungen verwalten können:

- Zertifikatsprobleme mit Web Studio beheben
- Fingerabdruckwert mithilfe von PowerShell aktualisieren

Probleme mit Zertifikaten beheben

Citrix Virtual Apps and Desktops blockiert eine HPE Moonshot-Verbindung, wenn Probleme mit dem Zertifikat auftreten, und verhindert, dass Sie Workloads auf zugehörigen HPE Moonshot-Knoten bereitstellen und verwalten können. In der Liste der **Hostverbindungen** wird neben der Verbindung ein Fehlersymbol angezeigt. In der folgenden Tabelle finden Sie spezifische Probleme und Lösungen.

Problem	Lösung
Fehler im von einer öffentlichen Zertifizierungsstelle signierten Zertifikat	Klicken Sie auf die Verbindung und wählen Sie die Registerkarte **Problembehandlung**. Sehen Sie sich die Fehlerdetails an und beheben Sie das Problem.
Empfangenes Zertifikat wurde von einer privaten Zertifizierungsstelle signiert oder ist abgelaufen.	Bearbeiten Sie die Hostverbindung, um den Fingerabdruck des Zertifikats zu aktualisieren. Verfahren 1. Wählen Sie die Verbindung und klicken Sie auf **Verbindung bearbeiten**. 1. Klicken Sie auf der Seite **Verbindungseigenschaften** auf **Einstellungen bearbeiten**. 1. Geben Sie das Kennwort ein, um eine Verbindung zum HPE Moonshot-Chassis herzustellen, und klicken Sie auf **Speichern**.

Problem	Lösung
	1. Vergleichen Sie auf der Seite **Warnung** den empfangenen Fingerabdruck mit dem des Servers hinsichtlich der Gültigkeit des Zertifikats. 1. Sind beide identisch, wählen Sie **Zertifakt vertrauen** und klicken Sie auf **OK**.

Fingerabdruckwert aktualisieren

Nach dem Erstellen einer Verbindung können Sie deren Fingerabdruckwert mithilfe des PowerShell-Befehls `Set-Item` aktualisieren. Führen Sie beispielsweise die folgenden Befehle aus:

1. Abrufen der Verbindungsdetails. Beispiel:

```
Get-Item -LiteralPath xdhyp:\connections\SinMoonshot-101
<!--NeedCopy-->
```

2. Aktualisieren des Fingerabdruckwerts. Beispiel:

```
Set-Item -LiteralPath xdhyp:\connections\SinMoonshot-101 -Username
    Administrator -SslThumbprint
   xxxxxxxxxxx12AD048480631BB7AB10D69xxxxx
<!--NeedCopy-->
```

3. Überprüfen des aktualisierten Fingerabdruckwerts. Beispiel:

```
Get-Item -LiteralPath xdhyp:\connections\SinMoonshot-101
<!--NeedCopy-->
```

> **Hinweis:**
>
> Das Update schlägt fehl, wenn der Befehl `Set-Item` einen falschen Fingerabdruckwert enthält.

So geht es weiter

- Wenn dies die erste Bereitstellung ist, lesen Sie Maschinenkatalog erstellen.
- Spezifische Informationen zu AWS finden Sie unter HPE Moonshot-Maschinenkatalog erstellen

Weitere Informationen

- Verbindungen und Ressourcen

- Maschinenkataloge erstellen

Verbindung zu Microsoft Azure

June 27, 2024

> **Hinweis:**
>
> Seit Juli 2023 hat Microsoft Azure Active Directory (Azure AD) in Microsoft Entra ID umbenannt. In diesem Dokument bezieht sich jeder Verweis auf Azure Active Directory, Azure AD oder AAD jetzt auf Microsoft Entra ID.

Unter Verbindungen und Ressourcen erstellen und verwalten werden die Assistenten zum Erstellen einer Verbindung beschrieben. Die folgenden Informationen beziehen sich speziell auf Azure Resource Manager-Cloudumgebungen.

> **Hinweis:**
>
> Bevor Sie eine Verbindung zu Microsoft Azure herstellen, müssen Sie Ihr Azure-Konto als Ressourcenstandort eingerichtet haben. Siehe Microsoft Azure Resource Manager-Cloudumgebungen.

Dienstprinzipale und Verbindungen erstellen

Bevor Sie Verbindungen erstellen, müssen Sie Dienstprinzipale einrichten, über die Verbindungen auf Azure-Ressourcen zugreifen. Es gibt zwei Optionen zum Erstellen einer Verbindung:

- Dienstprinzipal und Verbindung gemeinsam in Web Studio erstellen
- Verbindung mithilfe eines zuvor erstellten Dienstprinzipals erstellen

In diesem Abschnitt erfahren Sie, wie Sie diese Aufgaben ausführen:

- Dienstprinzipal und Verbindung mit Web Studio erstellen
- Dienstprinzipal mithilfe von PowerShell erstellen
- Anwendungsgeheimnis in Azure abrufen
- Verbindung mithilfe von vorhandenem Dienstprinzipal erstellen

Überlegungen

- Citrix empfiehlt, den Dienstprinzipal mit der Rolle “Mitwirkender”zu verwenden. Beachten Sie jedoch die Liste der Mindestberechtigungen im Abschnitt Mindestberechtigungen.

- 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 finden Sie unter CTX219211.
- Sie können zwar ein bestehendes Microsoft-Konto als Mitglied des Abonnementverzeichnisses hinzufügen und verwenden, doch kann es zu Komplikationen kommen, wenn dem Konto zuvor Gastzugriff auf eine der Verzeichnisressourcen gewährt worden war. In diesem Fall besitzt das Konto möglicherweise einen Platzhaltereintrag im Verzeichnis, der nicht die erforderlichen Berechtigungen gewährt, und es wird ein Fehler zurückgegeben.

  Entfernen Sie zur Behebung die Ressourcen aus dem Verzeichnis und fügen Sie sie 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. Diese Konfiguration gibt es normalerweise bei älteren Verzeichniskonten. Fügen Sie als Workaround dem Verzeichnis jeweils ein Konto hinzu, das den richtigen Mitgliedschaftswert erhält.
- Ressourcengruppen sind Container für Ressourcen und können Ressourcen aus ihrer eigenen und aus anderen Regionen enthalten. Dies kann Verwirrung auslösen, wenn Sie erwarten, dass die in der Region einer Ressourcengruppe angezeigten Ressourcen verfügbar sind.
- Stellen Sie sicher, dass Ihr Netzwerk und Subnetz groß genug zum Hosten der benötigten Maschinenzahl ist. Dies erfordert einiges an Vorausschau, doch Microsoft kann Ihnen bei der Wahl der richtigen Werte und der Planung der erforderlichen Adressraumkapazität helfen.

Dienstprinzipal und Verbindung mit Web Studio erstellen

> **Wichtig:**
>
> Dieses Feature ist für chinesische Azure-Abonnements noch nicht verfügbar.

In Web Studio können Sie Dienstprinzipal und Verbindung in einem einzigen Workflow erstellen. Dienstprinzipale gewähren Verbindungen Zugriff auf Azure-Ressourcen. Wenn Sie sich bei Azure authentifizieren, um einen Dienstprinzipal zu erstellen, wird eine Anwendung in Azure registriert. Für die registrierte Anwendung wird ein geheimer Schlüssel erstellt (geheimer Clientschlüssel oder An-

wendungsgeheimnis). Die registrierte Anwendung (in diesem Fall eine Verbindung) verwendet den geheimen Clientschlüssel zur Authentifizierung bei Azure AD.

Stellen Sie vor Beginn sicher, dass Sie die folgenden Voraussetzungen erfüllen:

- 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.
- Sie haben globale Administrator-, Anwendungsadministrator- oder Anwendungsentwicklerberechtigungen für die Authentifizierung. Diese Berechtigungen können widerrufen werden, wenn Sie eine Hostverbindung erstellt haben. Weitere Informationen zu Rollen finden Sie unter Integrierte Azure AD-Rollen.

Verwenden Sie den Assistenten für **Verbindung und Ressourcen hinzufügen**, um Dienstprinzipal und Verbindung gemeinsam zu erstellen:

1. Wählen Sie auf der Seite **Verbindung** die Option **Neue Verbindung erstellen**, als Verbindungstyp **Microsoft Azure** und Ihre Azure-Umgebung.
2. Wählen Sie die Tools, die zum Erstellen der virtuellen Maschinen verwendet werden sollen, und wählen Sie dann **Weiter**.
3. Geben Sie auf der Seite **Verbindungsdetails** die ID Ihres Azure-Abonnements und einen Namen für die Verbindung ein. Nachdem Sie die Abonnement-ID eingegeben haben, wird die Schaltfläche **Neu erstellen** verfügbar.

   > **Hinweis:**
   >
   > Der Verbindungsname muss aus 1–64 Zeichen bestehen, er darf nicht ausschließlich aus Leerzeichen bestehen und folgende Zeichen nicht enthalten: `\/;:#.*?=<>|[]{ } " '()'`

4. Wählen Sie **Neu erstellen** und geben Sie den Benutzernamen und das Kennwort des Azure Active Directory-Kontos ein.
5. Wählen Sie **Anmelden**.
6. Wählen Sie **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-Ressourcen für den angegebenen Benutzer ermöglicht.
7. Nachdem Sie **Akzeptieren** gewählt haben, kehren Sie auf die Seite **Verbindung** im Assistenten zurück.

   > **Hinweis:**
   >
   > Nachdem Sie sich bei Azure authentifiziert haben, werden die Schaltflächen **Neu erstellen**

> und **Vorhandene verwenden** ausgeblendet. Der Text **Verbindung erfolgreich** und ein grünes Häkchen zeigen die erfolgreiche Verbindung mit Ihrem Azure-Abonnement an.

8. Wählen Sie **Weiter** auf der Seite **Verbindungsdetails**.

   > **Hinweis:**
   >
   > Sie können im Assistenten erst fortfahren, wenn Sie sich bei Azure authentifiziert und die Erteilung der erforderlichen Berechtigungen akzeptiert haben.

9. Konfigurieren Sie Ressourcen für die Verbindung. Ressourcen umfassen Region und Netzwerk.

   - Wählen Sie auf der Seite **Region** eine Region aus.
   - Gehen Sie auf der Seite **Netzwerk** wie folgt vor:
     - Geben Sie einen Ressourcennamen zur Identifizierung der Kombination aus Region und Netzwerk ein. Der Name muss aus 1–64 Zeichen bestehen. Der Ressourcenname darf nicht ausschließlich aus Leerzeichen bestehen und folgende Zeichen nicht enthalten: `\/;:#.*?=<>|[]{ } "'()'`.
     - Wählen Sie eine Kombination aus virtuellem Netzwerk und Ressourcengruppe. (Wenn Sie mehrere virtuelle Netzwerke mit dem gleichen Namen haben, erzielen Sie durch die Kombination aus Netzwerknamen und Ressourcengruppe Einmaligkeit.) Wenn die auf der vorherigen Seite ausgewählte Region keine virtuellen Netzwerke enthält, kehren Sie zu der Seite zurück und wählen Sie eine Region, die virtuelle Netzwerke enthält.

10. Überprüfen Sie auf der Seite **Zusammenfassung** die Einstellungen und wählen Sie **Fertig stellen**, um die Einrichtung abzuschließen.

Anzeigen der Anwendungs-ID Nachdem Sie eine Verbindung erstellt haben, können Sie die Anwendungs-ID einsehen, die die Verbindung für den Zugriff auf Azure-Ressourcen verwendet.

Wählen Sie in der Liste **Verbindung und Ressourcen hinzufügen** die Verbindung aus, um die Details anzuzeigen. Auf der Registerkarte **Details** wird die Anwendungs-ID angezeigt.

Dienstprinzipal mithilfe von PowerShell erstellen

Zum Erstellen eines Dienstprinzipals mit PowerShell stellen Sie zunächst eine Verbindung mit Ihrem Azure Resource Manager-Abonnement her. Verwenden Sie dann die nachfolgend aufgeführten PowerShell-Cmdlets.

Stellen Sie sicher, dass Sie diese Elemente verfügbar haben:

- **SubscriptionId:** Azure Resource Manager-`SubscriptionID` des Abonnements, für das Sie VDAs bereitstellen möchten.
- **ActiveDirectoryID:** Mandanten-ID der Anwendung ein, die Sie bei Azure AD registriert haben.
- **ApplicationName:** Name der Anwendung, die in Azure AD erstellt werden soll.

Verfahren:

Stellen Sie eine Verbindung mit Ihrem Azure Resource Manager-Abonnement her.

```
1 `Connect-AzAccount`
```

1. Wählen Sie das Azure Resource Manager-Abonnement, in dem Sie den Dienstprinzipal erstellen möchten.

   ```
   Get-AzSubscription -SubscriptionId $subscriptionId | Select-
   AzSubscription
   ```

2. Erstellen Sie die Anwendung im AD-Mandanten.

   ```
   $AzureADApplication = New-AzADApplication -DisplayName $ApplicationName
   ```

3. Erstellen Sie einen Dienstprinzipal.

   ```
   New-AzADServicePrincipal -ApplicationId $AzureADApplication.AppId
   ```

4. Weisen Sie dem Dienstprinzipal eine Rolle zu.

   ```
   New-AzRoleAssignment -RoleDefinitionName Contributor -ServicePrincipalName
    $AzureADApplication.AppId –scope /subscriptions/$SubscriptionId
   ```

5. Notieren Sie die im Ausgabefenster der PowerShell-Konsole angezeigte Anwendungs-ID (ApplicationId). Sie müssen diese ID beim Erstellen der Hostverbindung angeben.

Anwendungsgeheimnis in Azure abrufen

Um eine Verbindung über einen vorhandenen Dienstprinzipal herzustellen, müssen Sie zunächst die Anwendungs-ID und das Anwendungsgeheimnis des Dienstprinzipals im Azure-Portal abrufen.

Verfahren:

1. Rufen Sie die **Anwendungs-ID** mithilfe von Web Studio oder PowerShell ab.
2. Melden Sie sich beim Azure-Portal an.
3. Wählen Sie in **Azure Active Directory**.
4. Wählen Sie in Azure AD unter **App registrations** Ihre Anwendung aus.
5. Gehen Sie zu **Certificates & secrets**.
6. Klicken Sie auf **Client secrets**.

Verbindung mithilfe von vorhandenem Dienstprinzipal erstellen

Wenn Sie bereits über einen Dienstprinzipal verfügen, können Sie ihn verwenden, um in Web Studio eine Verbindung herzustellen.

Stellen Sie sicher, dass Sie diese Elemente verfügbar haben:

- Abonnement-ID
- ActiveDirectory-ID (Mandanten-ID)
- Anwendungs-ID
- Anwendungsgeheimnis

  Weitere Informationen finden Sie unter Anwendungsgeheimnis abrufen.
- Ablaufdatum des Geheimnisses

Verfahren:

Führen Sie im Assistenten **Verbindung und Ressourcen hinzufügen** folgende Schritte aus:

1. Wählen Sie auf der Seite **Verbindung** die Option **Neue Verbindung erstellen**, als Verbindungstyp **Microsoft Azure** und Ihre Azure-Umgebung.
2. Wählen Sie die Tools, die zum Erstellen der virtuellen Maschinen verwendet werden sollen, und wählen Sie dann **Weiter**.
3. Geben Sie auf der Seite **Verbindungsdetails** die ID Ihres Azure-Abonnements und einen Namen für die Verbindung ein.

   > **Hinweis:**
   >
   > Der Verbindungsname muss aus 1–64 Zeichen bestehen, er darf nicht ausschließlich aus Leerzeichen bestehen und folgende Zeichen nicht enthalten: `\/;:#.*?=<>|[]{ } " '()'`

4. Wählen Sie **Vorhandene verwenden**. Geben Sie im Fenster **Vorhandene Dienstprinzipaldetails** die folgenden Einstellungen für den bestehenden Dienstprinzipal ein. Nachdem Sie die Details eingegeben haben, ist die Schaltfläche **Speichern** aktiviert. Wählen Sie **Speichern**. Sie können erst fortfahren, wenn Sie gültige Angaben gemacht haben.

   - **Abonnement-ID**. Geben Sie Ihre Azure-Abonnement-ID ein. Um Ihre Abonnement-ID zu erhalten, melden Sie sich beim Azure-Portal an und gehen Sie zu **Abonnements > Übersicht**.
   - **Active Directory-ID** (Mandanten-ID). Geben Sie die Verzeichnis-ID (Mandanten-ID) der Anwendung ein, die Sie bei Azure AD registriert haben.

- **Anwendungs-ID**. Geben Sie die Anwendungs-ID (Client-ID) der Anwendung ein, die Sie bei Azure AD registriert haben.
- **Anwendungsgeheimnis**. Erstellen Sie einen geheimen Clientschlüssel. Die registrierte Anwendung verwendet den Schlüssel zur Authentifizierung bei Azure AD. Es wird empfohlen, Schlüssel aus Sicherheitsgründen regelmäßig zu ändern. Speichern Sie den Schlüssel unbedingt, da Sie ihn später nicht abrufen können.
- **Ablaufdatum des Geheimnisses.** Geben Sie das Datum ein, nach dem das Anwendungsgeheimnis abläuft. Sie erhalten eine Warnung in der Konsole, bevor der geheime Schlüssel abläuft. Wenn der geheime Schlüssel abläuft, erhalten Sie Fehler.

  > **Hinweis:**
  >
  > Aus Sicherheitsgründen darf das Ablaufdatum nicht mehr als zwei Jahre in der Zukunft liegen.

- **Authentifizierungs-URL**. Dieses Feld wird automatisch ausgefüllt und kann nicht bearbeitet werden.
- **Verwaltungs-URL**. Dieses Feld wird automatisch ausgefüllt und kann nicht bearbeitet werden.
- **Speichersuffix**. Dieses Feld wird automatisch ausgefüllt und kann nicht bearbeitet werden.

  Für die Erstellung eines MCS-Katalogs in Azure ist Zugriff auf die folgenden Endpunkte erforderlich. Durch Zugriff auf diese Endpunkte wird die Konnektivität zwischen Ihrem Netzwerk und dem Azure-Portal und seinen Diensten optimiert.

  - Authentifizierungs-URL: https://login.microsoftonline.com/
  - Verwaltungs-URL: https://management.azure.com/. Dies ist eine Anforderungs-URL für Azure Resource Manager-Anbieter-APIs. Der Endpunkt für die Verwaltung hängt von der Umgebung ab. Für Azure Global ist dies beispielsweise https://management.azure.com/, und für Azure US Government ist es https://management.usgovcloudapi.net/.
  - Speichersuffix: https://*.core.windows.net./. Dieses (*) ist ein Platzhalterzeichen für das Speichersuffix. Beispiel: `https://demo.table.core.windows.net/`.

5. Nachdem Sie **Speichern** gewählt haben, wird die Seite **Verbindungsdetails** wieder angezeigt. Wählen Sie **Weiter**, um mit der nächsten Seite fortzufahren.
6. Konfigurieren Sie Ressourcen für die Verbindung. Ressourcen umfassen Region und Netzwerk.

   - Wählen Sie auf der Seite **Region** eine Region aus.
   - Gehen Sie auf der Seite **Netzwerk** wie folgt vor:

- Geben Sie einen Ressourcennamen zur Identifizierung der Kombination aus Region und Netzwerk ein. Der Name muss aus 1–64 Zeichen bestehen. Der Ressourcenname darf nicht ausschließlich aus Leerzeichen bestehen und folgende Zeichen nicht enthalten: `\/;:#.*?=<>|[]{ } "'()'`.
- Wählen Sie eine Kombination aus virtuellem Netzwerk und Ressourcengruppe. (Wenn Sie mehrere virtuelle Netzwerke mit dem gleichen Namen haben, erzielen Sie durch die Kombination aus Netzwerknamen und Ressourcengruppe Einmaligkeit.) Wenn die auf der vorherigen Seite ausgewählte Region keine virtuellen Netzwerke enthält, kehren Sie zu der Seite zurück und wählen Sie eine Region, die virtuelle Netzwerke enthält.

7. Überprüfen Sie auf der Seite **Zusammenfassung** die Einstellungen und wählen Sie **Fertig stellen**, um die Einrichtung abzuschließen.

Dienstprinzipale und Verbindungen verwalten

In diesem Abschnitt erfahren Sie, wie Sie Dienstprinzipale und Verbindungen verwalten können:

- Einstellungen für Azure-Drosselung konfigurieren
- Imagefreigabe in Azure aktivieren
- Gemeinsam genutzte Mandanten mithilfe der vollständigen Konfiguration zu einer Verbindung hinzufügen
- Image-Freigabe mithilfe von PowerShell implementieren
- Anwendungsgeheimnis und Ablaufdatum für Geheimnis verwalten

Einstellungen für Azure-Drosselung konfigurieren

Azure Resource Manager drosselt Anforderungen von Abonnements und Mandanten durch das Routing von Datenverkehr gemäß Grenzwerten, die auf die spezifischen Anforderungen des Anbieters zugeschnitten sind. Weitere Informationen finden Sie auf der Website von Microsoft unter Drosseln von Resource Manager-Anforderungen. Es gibt Grenzwerte für Abonnements und Mandanten, wenn die Verwaltung zahlreicher Maschinen problematisch werden kann. Beispielsweise können bei einem Abonnement mit zahlreichen Maschinen Leistungsprobleme im Zusammenhang mit Energievorgängen auftreten.

> **Tipp:**
>
> Weitere Informationen finden Sie unter Verbessern der Azure-Leistung mit Maschinenerstellungsdiensten.

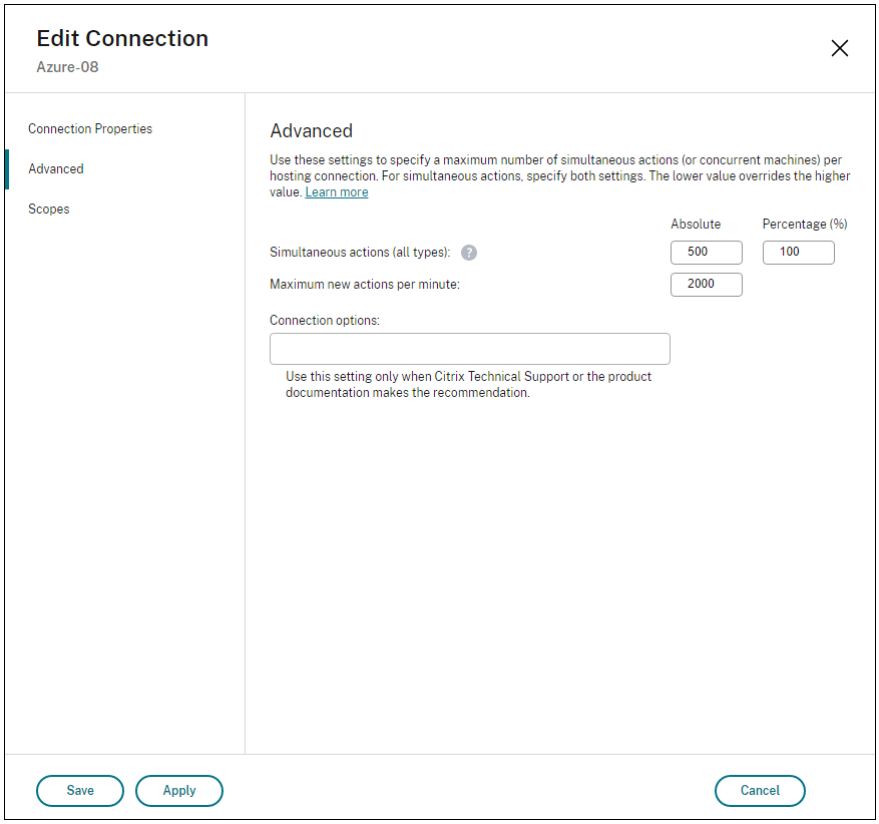
Zur Lösung solcher Probleme können Sie die interne MCS-Drosselung entfernen, um das Azure-Anforderungskontingent stärker zu nutzen.

Für große Abonnements (z. B. mit 1000 oder mehr VMs) empfehlen wir die folgenden optimalen Einstellungen für das Ein- und Ausschalten von VMs:

- Absolute gleichzeitige Operationen: 500
- Maximale neue Operationen pro Minute: 2000
- Maximale Gleichzeitigkeit von Operationen: 500

Gehen Sie zum Konfigurieren von Azure-Operationen für eine Azure-Verbindung mit Web Studio folgendermaßen vor:

1. Wählen Sie in Web Studio im linken Bereich **Hosting**.
2. Wählen Sie die Verbindung aus.
3. Wählen Sie **Erweitert** im Assistenten **Verbindung bearbeiten**.
4. Geben Sie auf der Seite **Erweitert** die Anzahl gleichzeitiger Aktionen, die maximale Anzahl neuer Aktionen pro Minute und ggf. weitere Verbindungsoptionen an.



MCS unterstützt standardmäßig maximal 500 gleichzeitige Vorgänge. Alternativ können Sie mit dem Remote PowerShell SDK die maximale Anzahl gleichzeitiger Vorgänge festlegen.

Geben Sie über die **PowerShell**-Eigenschaft `MaximumConcurrentProvisioningOperations` die maximale Anzahl gleichzeitiger Azure-Provisioningvorgänge an. Beachten Sie Folgendes bei der Verwendung dieser Eigenschaft:

- Der Standardwert von `MaximumConcurrentProvisioningOperations` ist 500.

- Konfigurieren Sie den Parameter `MaximumConcurrentProvisioningOperations` mit dem PowerShell-Befehl `Set-item`.

Imagefreigabe in Azure aktivieren

Beim Erstellen oder Aktualisieren von Maschinenkatalogen können Sie per Azure Compute Gallery freigegebene Images aus anderen Azure-Mandanten und -Abonnements auswählen. Um die Imagefreigabe innerhalb oder zwischen Mandanten zu aktivieren, müssen Sie die erforderlichen Einstellungen in Azure vornehmen:

- Images innerhalb eines Mandanten freigeben (abonnementübergreifend)
- Images mandantenübergreifend freigeben

Images innerhalb eines Mandanten freigeben (abonnementübergreifend) Um ein Image in Azure Compute Gallery auszuwählen, das zu einem anderen Abonnement gehört, muss es für den Dienstprinzipal (SPN) dieses Abonnements freigegeben werden.

Dienstprinzipal SPN 1 ist in Studio beispielsweise wie folgt konfiguriert:

Dienstprinzipal: SPN 1

Abonnement: Abonnement 1

Mandant: Mandant 1

Das Image ist in einem anderen Abonnement, das in Studio wie folgt konfiguriert ist:

Abonnement: Abonnement 2

Mandant: Mandant 1

Wenn Sie das Image in Abonnement 2 für Abonnement 1 (SPN 1) freigeben möchten, gehen Sie zu Abonnement 2 und geben Sie die Ressourcengruppe für SPN1 frei.

Die Imagefreigabe muss über die rollenbasierte Zugriffssteuerung (RBAC) von Azure erfolgen. Azure RBAC ist das bei der Verwaltung des Zugriffs auf Azure-Ressourcen verwendete Autorisierungssystem. Weitere Informationen zu Azure RBAC finden Sie im Microsoft-Dokument Was ist die rollenbasierte Zugriffssteuerung in Azure (Azure Role-Based Access Control, Azure RBAC)?. Um Zugriff zu gewähren, weisen Sie Dienstprinzipals Rollen im Bereich der Ressourcengruppe mit der Rolle "Mitwirkender" zu. Um Azure-Rollen zuzuweisen, benötigen Sie die Berechtigung `Microsoft.Authorization/roleAssignments/write` (z. B. als Benutzerzugriffsadministrator oder Besitzer). Weitere Informationen zum Freigeben von Images für andere SPNs finden Sie im Microsoft-Dokument Zuweisen von Azure-Rollen über das Azure-Portal.

Informationen zum Auswählen von Images aus einem anderen Abonnement mit PowerShell-Befehlen finden Sie unter Image aus einem anderen Abonnement auswählen.

Images mandantenübergreifend freigeben Um Images mit Azure Compute Gallery für andere Mandaten freizugeben, erstellen Sie eine Anwendungsregistrierung.

Wenn beispielsweise zwei Mandanten vorliegen (Mandant 1 und Mandant 2) und Sie Ihren Image-Katalog mit Mandant 1 teilen möchten, gehen Sie wie folgt vor:

1. Erstellen Sie eine Anwendungsregistrierung für Mandant 1. Weitere Informationen finden Sie unter Create the app registration.
2. Fordern Sie über einen Browser eine Anmeldung an, um Mandant 2 Zugriff auf die Anwendung zu geben. Ersetzen Sie `Tenant2 ID` durch die ID von Mandant 1. Ersetzen Sie `Application (client)ID` durch die Anwendungs-ID der von Ihnen erstellten Anwendungsregistrierung. Wenn Sie die IDs ersetzt haben, fügen Sie die URL in einen Browser ein und folgen Sie den Schritten zum Anmelden bei Mandant 2. Beispiel:

   ```
   https://login.microsoftonline.com/<Tenant 2 ID>/oauth2/authorize?
       client_id=<Application (client) ID>&response_type=code&
       redirect_uri=https%3A%2F%2Fwww.microsoft.com%2F
   <!--NeedCopy-->
   ```

   Weitere Informationen finden Sie unter Give Tenant 2 access.
3. Gewähren Sie der Anwendung Zugriff auf die Ressourcengruppe von Mandant 2. Melden Sie sich als Mandant 2 an und gewähren Sie der Anwendungsregistrierung Zugriff auf die Ressourcengruppe, die das Katalogimage enthält. Weitere Informationen finden Sie unter Authenticate requests across tenants.

Zum Erstellen eines Katalogs mithilfe von PowerShell-Befehlen und einem Image von einem anderen Mandanten gehen Sie folgendermaßen vor:

1. Aktualisieren Sie benutzerdefinierte Eigenschaften der Hostverbindung mit IDs für freigegebene Mandanten.
2. Wählen Sie ein Image eines anderen Mandanten aus.

Gemeinsam genutzte Mandanten mithilfe der vollständigen Konfiguration zu einer Verbindung hinzufügen

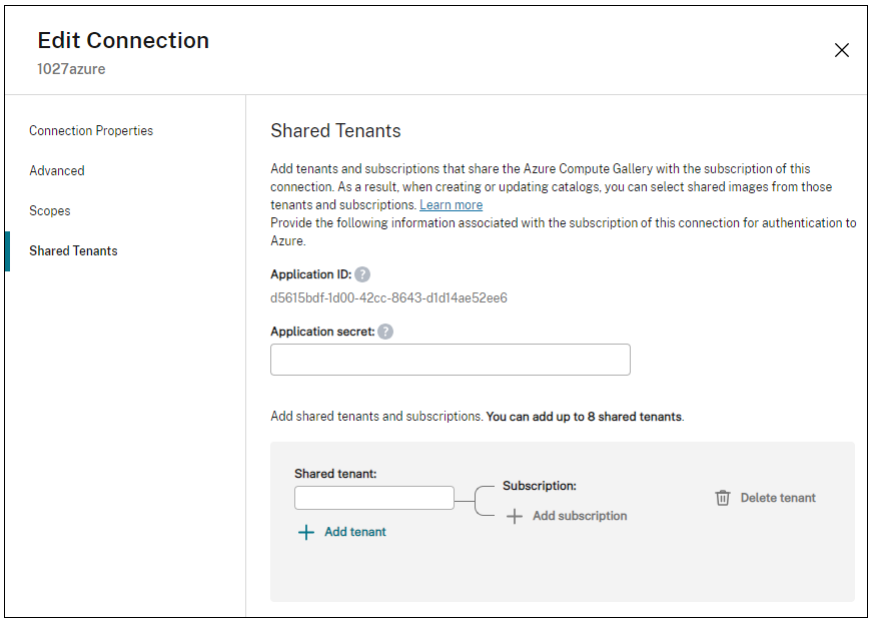
Beim Erstellen oder Aktualisieren von Maschinenkatalogen in Web Studio können Sie per Azure Compute Gallery freigegebene Images aus anderen Azure-Mandanten und -Abonnements auswählen. Für dieses Feature müssen Sie Informationen zu freigegebenen Mandanten und Abonnements für zugehörige Hostverbindungen angeben.

> **Hinweis:**
>
> Vergewissern Sie sich, dass Sie die erforderlichen Einstellungen in Azure vorgenommen haben,

> um die Imagefreigabe innerhalb oder zwischen Mandanten zu aktivieren. Weitere Informationen finden Sie unter Images mandantenübergreifend freigeben.

Führen Sie die folgenden Schritte für eine Verbindung aus:

1. Wählen Sie in Web Studio im linken Bereich **Hosting**.
2. Wählen Sie die Verbindung und dann in der Aktionsleiste **Verbindung bearbeiten** aus.



3. Führen Sie unter **Freigegebene Mandanten** die folgenden Schritte aus:
   - Geben Sie die dem Abonnement der Verbindung zugeordnete Anwendungs-ID und das Anwendungsgeheimnis an. Citrix Virtual Apps and Desktops verwendet diese Informationen zur Authentifizierung bei Azure AD.
   - Fügen Sie Mandanten und Abonnements hinzu, die sich die Azure Compute Gallery mit dem Abonnement der Verbindung teilen. Sie können bis zu acht freigegebene Mandanten und acht Abonnements für jeden Mandanten hinzufügen.
4. Abschließend wählen Sie entweder **Übernehmen**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt, oder **OK**, damit die Änderungen angewendet werden und das Fenster geschlossen wird.

Image-Freigabe mithilfe von PowerShell implementieren

Dieser Abschnitt erläutert die Prozesse zur Image-Freigabe mithilfe von PowerShell:

- Image aus einem anderen Abonnement auswählen

- Benutzerdefinierte Eigenschaften der Hostverbindung mit IDs für freigegebene Mandanten aktualisieren
- Image eines anderen Mandanten auswählen

Image aus einem anderen Abonnement auswählen Sie können in Azure Compute Gallery ein Image auswählen, das zu einem anderen freigegebenen Abonnement im selben Azure-Mandanten gehört, um MCS-Kataloge mit PowerShell-Befehlen zu erstellen und zu aktualisieren.

1. Im Stammordner der Hostingeinheit erstellt Citrix einen neuen freigegebenen Abonnementordner unter dem Namen `sharedsubscription`.
2. Listen Sie alle freigegebenen Abonnements im Mandanten auf.

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\sharedsubscription.
    folder"
<!--NeedCopy-->
```

3. Wählen Sie ein freigegebenes Abonnement und listen Sie dann alle freigegebenen Ressourcengruppen dieses Abonnements auf.

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123
    .sharedsubscription"
<!--NeedCopy-->
```

4. Wählen Sie eine Ressourcengruppe und listen Sie dann alle Kataloge in der Ressourcengruppe auf.

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123
    .sharedsubscription\ xyz.resourcegroup"
<!--NeedCopy-->
```

5. Wählen Sie einen Katalog und listen Sie dann alle Imagedefinitionen des Katalogs auf.

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123
    .sharedsubscription\xyz.resourcegroup\testgallery.gallery"
<!--NeedCopy-->
```

6. Wählen Sie eine Imagedefinition und listen Sie dann alle Imageversionen der Imagedefinition auf.

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123
    .sharedsubscription\xyz.resourcegroup\sigtestdef.
    imagedefinition"
<!--NeedCopy-->
```

7. Zum Erstellen und Aktualisieren eines MCS-Katalogs verwenden Sie die folgenden Elemente:

   - Ressourcengruppe
   - Katalog

- Katalogimagedefinition
- Katalogimageversion

Informationen zum Erstellen eines Katalogs mit dem Remote PowerShell SDK finden Sie unter https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

Benutzerdefinierte Eigenschaften der Hostverbindung mit IDs für freigegebene Mandanten aktualisieren Mit `Set-Item` können Sie die benutzerdefinierten Eigenschaften der Hostverbindung mit den IDs der freigegebenen Mandanten und den Abonnement-IDs aktualisieren. Fügen Sie eine Eigenschaft `SharedTenants` in `CustomProperties` hinzu. Das Format von `Shared Tenants` ist:

```
[{
 "Tenant":"94367291-119e-457c-bc10-25337231f7bd","Subscriptions":["7
    bb42f40-8d7f-4230-a920-be2781f6d5d9"] }
 ,{
 "Tenant":"50e83564-c4e5-4209-b43d-815c45659564","Subscriptions":["06
    ab8944-6a88-47ee-a975-43dd491a37d0"] }
 ]
<!--NeedCopy-->
```

Beispiel:

```
Set-Item -CustomProperties "<CustomProperties xmlns=`"http://schemas.
   citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org
   /2001/XMLSchema-instance`">
<Property xsi:type=`"StringProperty`" Name=`"SubscriptionId`" Value=`"
   123`" />
<Property xsi:type=`"StringProperty`" Name=`"ManagementEndpoint`" Value
   =`"https://management.azure.com/`" />
<Property xsi:type=`"StringProperty`" Name=`"AuthenticationAuthority`"
   Value=`"https://login.microsoftonline.com/`" />
<Property xsi:type=`"StringProperty`" Name=`"StorageSuffix`" Value=`"
   core.windows.net`" />
<Property xsi:type=`"StringProperty`" Name=`"TenantId`" Value=`"123abc`
   " />
<Property xsi:type=`"StringProperty`" Name=`"SharedTenants`" Value=`"`[
    {
  'Tenant':'123abc', 'Subscriptions':['345', '567']  }
  ]`"` />
</CustomProperties>"
-LiteralPath @("XDHyp:\Connections\aazure") -PassThru -UserName "
   advc345" -SecurePassword
$psd
<!--NeedCopy-->
```


> **Hinweis:**
>
> Sie können mehrere Mandanten hinzufügen. Jeder Mandant kann mehrere Abonnements haben.

Image eines anderen Mandanten auswählen Sie können in der Azure Compute Gallery mit PowerShell-Befehlen ein Image auswählen, das zu einem anderen Azure-Mandanten gehört, um MCS-Kataloge zu erstellen und zu aktualisieren.

1. Im Stammordner der Hostingeinheit erstellt Citrix einen neuen freigegebenen Abonnementordner unter dem Namen `sharedsubscription`.
2. Listen Sie alle freigegebenen Abonnements auf.

```
Get-ChildItem XDHyp:\HostingUnits\azres\sharedsubscription.folder
<!--NeedCopy-->
```

3. Wählen Sie ein freigegebenes Abonnement und listen Sie dann alle freigegebenen Ressourcengruppen dieses Abonnements auf.

```
Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
    sharedsubscription
<!--NeedCopy-->
```

4. Wählen Sie eine Ressourcengruppe und listen Sie dann alle Kataloge in der Ressourcengruppe auf.

```
Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
    sharedsubscription\ xyz.resourcegroup
<!--NeedCopy-->
```

5. Wählen Sie einen Katalog und listen Sie dann alle Imagedefinitionen des Katalogs auf.

```
Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
    sharedsubscription\xyz.resourcegroup\efg.gallery
<!--NeedCopy-->
```

6. Wählen Sie eine Imagedefinition und listen Sie dann alle Imageversionen der Imagedefinition auf.

```
Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
    sharedsubscription\xyz.resourcegroup\efg.gallery\hij.
    imagedefinition
<!--NeedCopy-->
```

7. Zum Erstellen und Aktualisieren eines MCS-Katalogs verwenden Sie die folgenden Elemente:
   - Ressourcengruppe
   - Katalog

- Katalogimagedefinition
- Katalogimageversion

Informationen zum Erstellen eines Katalogs mit dem Remote PowerShell SDK finden Sie unter https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

Anwendungsgeheimnis und Ablaufdatum für Geheimnis verwalten

Sie müssen das Anwendungsgeheimnis für eine Verbindung vor Ablauf des Geheimnisses ändern. Sie erhalten eine Warnung in Web Studio, bevor der geheime Schlüssel abläuft.

Anwendungsgeheimnis in Azure erstellen Sie können über das Azure-Portal ein Anwendungsgeheimnis für eine Verbindung erstellen.

1. Wählen Sie **Azure Active Directory**.
2. Wählen Sie in Azure AD unter **App registrations** Ihre Anwendung aus.
3. Gehen Sie zu **Certificates & secrets**.
4. Klicken Sie auf **Client secrets > New client secret**.
5. Geben Sie eine Beschreibung des geheimen Schlüssels ein und legen Sie eine Dauer fest. Wenn Sie fertig sind, wählen Sie **Hinzufügen**.

   > **Hinweis:**
   >
   > Speichern Sie den geheimen Clientschlüssel unbedingt, da Sie ihn später nicht abrufen können.

6. Kopieren Sie das Clientgeheimnis und das Ablaufdatum.
7. Bearbeiten Sie in Web Studio die entsprechende Verbindung und ersetzen Sie den Inhalt in den Feldern **Anwendungsgeheimnis** und **Ablaufdatum des Geheimnisses** durch die Werte, den Sie kopiert haben.

Ändern des Ablaufdatums des Geheimnisses Sie können Web Studio verwenden, um das Ablaufdatum für das verwendete Anwendungsgeheimnis hinzuzufügen oder zu ändern.

1. Klicken Sie im Assistenten **Verbindung und Ressourcen hinzufügen** mit der rechten Maustaste auf eine Verbindung und dann auf **Verbindung bearbeiten**.
2. Klicken Sie auf der Seite **Verbindungseigenschaften** auf **Ablaufdatum des Geheimnisses**, um das Ablaufdatum für das verwendete Anwendungsgeheimnis hinzuzufügen oder zu ändern.

Erforderliche Azure-Berechtigungen

Dieser Abschnitt enthält die für Azure erforderlichen Mindestberechtigungen und allgemeinen Berechtigungen.

Mindestberechtigungen

Mindestberechtigungen ermöglichen eine bessere Sicherheitskontrolle. Was ist neu, die zusätzliche Berechtigungen erfordern, schlagen jedoch fehl, wenn nur die Mindestberechtigungen verwendet werden.

Hostverbindung erstellen Fügen Sie eine neue Hostverbindung unter Verwendung der von Azure abgerufenen Informationen hinzu.

```
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/disks/read",
<!--NeedCopy-->
```

Energieverwaltung virtueller Maschinen Schalten Sie die Maschineninstanzen ein oder aus.

```
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/virtualMachines/start/action",
"Microsoft.Compute/virtualMachines/restart/action",
<!--NeedCopy-->
```

Erstellen, Aktualisieren oder Löschen von VMs Nach dem Erstellen eines Maschinenkatalogs können Sie Maschinen hinzufügen, löschen und aktualisieren und den Maschinenkatalog löschen.

Die folgende Liste umfasst notwendige Mindestberechtigungen, wenn das Masterimage ein verwalteter Datenträger ist oder wenn sich Snapshots in derselben Region wie die Hostverbindung befinden.

```
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/snapshots/read",
"Microsoft.Compute/snapshots/write",
"Microsoft.Compute/snapshots/delete",
"Microsoft.Compute/snapshots/beginGetAccess/action",
```



```
"Microsoft.Compute/snapshots/endGetAccess/action",
"Microsoft.Compute/disks/read",
"Microsoft.Compute/disks/write",
"Microsoft.Compute/disks/delete",
"Microsoft.Compute/disks/beginGetAccess/action",
"Microsoft.Compute/disks/endGetAccess/action",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/join/action",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkInterfaces/join/action",
<!--NeedCopy-->
```

Für die folgenden Features benötigen Sie zusätzlich zu den Mindestberechtigungen die folgenden Berechtigungen:

- Wenn das Masterimage eine virtuelle Festplatte (VHD) in einem Speicherkonto ist, das sich in derselben Region wie die Hostverbindung befindet:

```
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/listKeys/action",
<!--NeedCopy-->
```

- Wenn das Masterimage eine ImageVersion aus der Shared Image Gallery ist:

```
"Microsoft.Compute/galleries/read",
"Microsoft.Compute/galleries/images/read",
"Microsoft.Compute/galleries/images/versions/read",
<!--NeedCopy-->
```

- Wenn das Masterimage ein verwalteter Datenträger ist, befinden sich die Snapshots bzw. die virtuelle Festplatte in einer anderen Region als die Hostverbindung:

```
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/listKeys/action",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/storageAccounts/delete",
<!--NeedCopy-->
```

- Wenn Sie eine von Citrix verwaltete Ressourcengruppe verwenden:

```
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Resources/subscriptions/resourceGroups/delete",
<!--NeedCopy-->
```

- Wenn Sie das Masterimage in der Shared Image Gallery ablegen:


```
"Microsoft.Compute/galleries/write",
"Microsoft.Compute/galleries/images/write",
"Microsoft.Compute/galleries/images/versions/write",
"Microsoft.Compute/galleries/read",
"Microsoft.Compute/galleries/images/read",
"Microsoft.Compute/galleries/images/versions/read",
"Microsoft.Compute/galleries/delete",
"Microsoft.Compute/galleries/images/delete",
"Microsoft.Compute/galleries/images/versions/delete",
<!--NeedCopy-->
```

- Wenn Sie dedizierte Azure-Hosts unterstützen:

```
"Microsoft.Compute/hostGroups/read",
"Microsoft.Compute/hostGroups/write",
"Microsoft.Compute/hostGroups/hosts/read",
<!--NeedCopy-->
```

- Wenn Sie die serverseitige Verschlüsselung (SSE) mit vom Kunden verwalteten Schlüsseln (CMK) verwenden:

```
"Microsoft.Compute/diskEncryptionSets/read",
<!--NeedCopy-->
```

- Wenn Sie VMs mit ARM-Vorlagen (Maschinenprofil) bereitstellen:

```
"Microsoft.Resources/deployments/write",
"Microsoft.Resources/deployments/operationstatuses/read",
"Microsoft.Resources/deployments/read",
"Microsoft.Resources/deployments/delete",
<!--NeedCopy-->
```

- Wenn Sie die Azure-Vorlagenspezifikation als Maschinenprofil verwenden:

```
"Microsoft.Resources/templateSpecs/read",
"Microsoft.Resources/templateSpecs/versions/read",
<!--NeedCopy-->
```

Erstellen, Aktualisieren und Löschen von Maschinen mit nicht verwaltetem Datenträger Die folgende Liste umfasst notwendige Mindestberechtigungen, wenn das Masterimage eine VHD ist und die vom Administrator bereitgestellte Ressourcengruppe verwendet wird:

```
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Storage/storageAccounts/delete",
"Microsoft.Storage/storageAccounts/listKeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Compute/virtualMachines/read",
```



```
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/join/action"
<!--NeedCopy-->
```

Allgemeine Berechtigung

Die Rolle “Mitwirkender”erhält Vollzugriff zur Verwaltung aller Ressourcen. Dieser Satz von Berechtigungen hindert Sie nicht daran, Was ist neu zu erhalten.

Die folgenden Berechtigungen bieten die beste Kompatibilität für die zukünftige Verwendung, obwohl sie mehr Berechtigungen umfassen, als für aktuelle Features erforderlich sind:

```
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Compute/disks/beginGetAccess/action",
"Microsoft.Compute/disks/delete",
"Microsoft.Compute/disks/endGetAccess/action",
"Microsoft.Compute/disks/read",
"Microsoft.Compute/disks/write",
"Microsoft.Compute/galleries/delete",
"Microsoft.Compute/galleries/images/delete",
"Microsoft.Compute/galleries/images/read",
"Microsoft.Compute/galleries/images/versions/delete",
"Microsoft.Compute/galleries/images/versions/read",
"Microsoft.Compute/galleries/images/versions/write",
"Microsoft.Compute/galleries/images/write",
"Microsoft.Compute/galleries/read",
"Microsoft.Compute/galleries/write",
"Microsoft.Compute/hostGroups/hosts/read",
"Microsoft.Compute/hostGroups/read",
"Microsoft.Compute/hostGroups/write",
"Microsoft.Compute/snapshots/beginGetAccess/action",
"Microsoft.Compute/snapshots/delete",
"Microsoft.Compute/snapshots/endGetAccess/action",
"Microsoft.Compute/snapshots/read",
"Microsoft.Compute/snapshots/write",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/restart/action",
"Microsoft.Compute/virtualMachines/start/action",
```



```
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/join/action",
"Microsoft.Resources/deployments/operationstatuses/read",
"Microsoft.Resources/deployments/read",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Resources/deployments/write",
"Microsoft.Resources/deployments/delete",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Resources/subscriptions/resourceGroups/delete",
"Microsoft.Storage/storageAccounts/delete",
"Microsoft.Storage/storageAccounts/listKeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Resources/templateSpecs/read",
"Microsoft.Resources/templateSpecs/versions/read",
<!--NeedCopy-->
```

So geht es weiter

- Wenn dies die erste Bereitstellung ist, lesen Sie Maschinenkatalog erstellen.
- Azure-spezifische Informationen finden Sie unter Microsoft Azure-Katalog erstellen.

Weitere Informationen

- Verbindungen und Ressourcen
- Maschinenkataloge erstellen

Verbindung zu Microsoft System Center Virtual Machine Manager

June 27, 2024

Unter Verbindungen und Ressourcen erstellen und verwalten werden die Assistenten zum Erstellen einer Verbindung beschrieben. Die folgenden Informationen beziehen sich speziell auf Microsoft System Center Virtual Machine Manager (VMM).

> **Hinweis:**
>
> Bevor Sie eine Verbindung zu VMM herstellen, müssen Sie zunächst Ihr VMM-Konto als Ressourcenstandort eingerichtet haben. Siehe Microsoft System Center Virtual Machine Manager-Virtualisierungsumgebungen.

Verbindung erstellen

Wenn Sie VMs mit MCS bereitgestellt haben, führen Sie im Assistenten zur Erstellung von Verbindungen folgende Schritte aus:

- Geben Sie die Adresse als vollqualifizierten Domänennamen des Hostservers ein.
- Geben Sie Anmeldeinformationen für das zuvor erstellte Administratorkonto ein. Das Konto muss Berechtigung zum Erstellen neuer VMs haben.
- Wählen Sie im Dialogfeld "Hostdetails"den Cluster oder eigenständigen Host aus, der beim Erstellen der VMs verwendet werden soll.

  > **Wichtig**
  >
  > Sie müssen auch dann zu einem Cluster oder eigenständigen Host navigieren, wenn Sie eine Bereitstellung mit einem einzelnen Hyper-V-Host verwenden.

So geht es weiter

- Wenn dies die erste Bereitstellung ist, lesen Sie Maschinenkatalog erstellen.
- Informationen zum Erstellen von Maschinenkatalogen mit MCS auf SMB 3-Dateifreigaben finden Sie unter Microsoft System Center Virtual Machine Manager-Katalog erstellen.

Weitere Informationen

- Verbindungen und Ressourcen
- Maschinenkataloge erstellen

Verbindung zu Nutanix

June 27, 2024

Unter Verbindungen und Ressourcen erstellen und verwalten werden die Assistenten zum Erstellen einer Verbindung beschrieben. Die folgenden Informationen beziehen sich speziell auf Nutanix.

> **Hinweis:**
>
> Bevor Sie eine Verbindung zu Nutanix herstellen, müssen Sie zunächst Ihr Nutanix-Konto als Ressourcenstandort eingerichtet haben. Siehe Nutanix-Virtualisierungsumgebungen.

Erstellen einer Verbindung mit Nutanix

Die folgenden Informationen ergänzen die Anweisungen unter Verbindungen und Ressourcen. Folgen Sie zum Erstellen einer Nutanix-Verbindung den allgemeinen Anweisungen in dem Artikel. Beachten Sie besonders die Nutanix-spezifischen Details.

Wählen Sie im Assistenten zum Hinzufügen einer Verbindung und Ressourcen auf der Seite **Verbindung** den Verbindungstyp **Nutanix**. Geben Sie dann die Adresse und Anmeldeinformationen sowie einen Namen für die Verbindung ein. Wählen Sie auf der Seite **Netzwerk** ein Netzwerk für die Hostingeinheit aus.

Folgende Anschlusstypen stehen zur Auswahl: **Nutanix AHV**, **Nutanix AHV DRaaS** und **Nutanix AHV PC**.

- Geben Sie für **Nutanix AHV** die Prism Element (PE)-Clusteradresse und die Anmeldeinformationen an.
- Geben Sie für **Nutanix AHV PC** die Prism Central (PC)-Adresse und die Anmeldeinformationen an.

  > **Hinweis:**
  >
  > Derzeit wird der Verbindungstyp Nutanix AHV PC nur zum Herstellen einer Verbindung zum Nutanix Cloud Cluster (NC2) auf Azure verwendet. Außerdem kann ein Maschinenkatalog nur auf einem einzelnen Cluster in einer NC2-on-Azure-Verbindung gehostet werden.

- Geben Sie für **Nutanix AHV DRaaS** die DRaaS-Mandantenadresse und den Benutzernamen an. Importieren Sie Ihre privaten und öffentlichen Nutanix DRaaS-Anmeldedateien (`.pem`).

> **Tipp:**
>
> Wenn Sie Maschinen mit Nutanix AHV (Prism Element) als Ressource bereitstellen, wählen Sie den Container aus, in dem sich der VM-Datenträger befindet.

So geht es weiter

- Wenn dies die erste Bereitstellung ist, lesen Sie Maschinenkatalog erstellen.
- Spezielle Informationen zu Nutanix finden Sie unter Nutanix-Katalog erstellen.

Weitere Informationen

- Verbindungen und Ressourcen
- Maschinenkataloge erstellen

Verbindung zu Nutanix-Cloud und Partnerlösungen

June 27, 2024

Unter Verbindungen und Ressourcen erstellen und verwalten werden die Assistenten zum Erstellen einer Verbindung beschrieben. Die folgenden Informationen beziehen sich speziell auf Nutanix-Cloud und Partnerlösungen.

Citrix Virtual Apps and Desktops unterstützt die folgende Nutanix-Cloud und Partnerlösung:

- Nutanix Cloud Clusters in AWS

> **Hinweis:**
>
> Bevor Sie eine Verbindung zu Nutanix-Cloud und Partnerlösung herstellen, müssen Sie zunächst Ihr entsprechendes Konto als Ressourcenstandort eingerichtet haben. Siehe Nutanix-Cloud und Partnerlösungen.

Herstellen einer Verbindung zu Nutanix Prism

Nachdem Sie einen Nutanix-Cluster erstellt haben, stellen Sie eine Verbindung zu Nutanix Prism her.

Schrittfolge zum Herstellen einer Verbindung zu Nutanix Prism:

1. Erstellen Sie eine Bastion-VM im Subnetz 10.0.129.0/24.
2. Stellen Sie mit RDP eine Verbindung zur Bastion-VM her und rufen Sie die URL von **Prism Element** auf, die Sie im vorherigen Abschnitt kopiert haben.
3. Melden Sie sich mit den Standardanmeldeinformationen an: `admin:nutanix/4u`. Denken Sie daran, das Kennwort zu ändern.

Erstellen einer VM im Nutanix-Cluster

Nachdem Sie eine Verbindung zu **Nutanix Prism** hergestellt haben, erstellen Sie VMs im Nutanix-Cluster.

Wenn die VM einen Internetzugang benötigt

1. Rufen Sie die AWS-Konsole auf.
2. Erstellen Sie das neue Subnetz 10.0.130.0/24 in derselben virtuellen privaten Cloud, die von Nutanix CFS erstellt wurde.
3. Fügen Sie der Routing-Tabelle dieses Subnetzes eine Route hinzu, um den gesamten nicht lokalen Datenverkehr zum oben genannten NAT-Gateway zu leiten.
4. Stellen Sie mit RDP eine Verbindung zur Bastion-VM her, rufen Sie die URL von **Prism Element** auf, die Sie im vorherigen Abschnitt kopiert haben und melden Sie sich an.
5. Fügen Sie ein neues Netzwerk hinzu. Gehen Sie zu **Settings > Network Configuration > Create Subnet**. Verwenden Sie dasselbe Subnetz 10.0.130.0/24, das auch in AWS verwendet wird.
6. Erstellen Sie alle virtuellen Maschinen (AD, CC, VDA usw.) in diesem neuen Subnetz.

Wenn die VM keinen Internetzugang benötigt

1. Stellen Sie mit RDP eine Verbindung zur Bastion-VM her, rufen Sie die URL von **Prism Element** auf, die Sie im vorherigen Abschnitt kopiert haben und melden Sie sich an.
2. Fügen Sie ein neues Netzwerk hinzu. Gehen Sie zu **Settings > Network Configuration > Create Subnet**. Verwenden Sie das Subnetz 10.0.129.0/24.
3. Erstellen Sie alle virtuellen Maschinen (AD, CC, VDA usw.) in diesem Subnetz.

> **Tipp:**
>
> Stellen Sie sicher, dass Uhrzeit und Zeitzone in den VMs korrekt eingerichtet sind. Dies gilt insbesondere für AD.

Erstellen der Hostverbindung

1. Starten Sie Web Studio.
2. Wählen Sie den Hostingknoten und klicken Sie auf **Verbindung und Ressourcen hinzufügen**.
3. Wählen Sie im Bildschirm **Verbindung** die Option **Neue Verbindung erstellen** und geben Sie unter **Verbindungsadresse** Folgendes ein: `https://xxx.xxx.xxx.xxx:9440`.
4. Folgen Sie der Benutzeroberfläche, um den Assistenten abzuschließen.

> **Hinweis:**
>
> Um die Option für Nutanix in Web Studio anzuzeigen, muss auf allen Connector-VMs das Nutanix-Plug-In installiert sein, auch wenn sie nicht in der Nutanix-Zone verwendet werden.

So geht es weiter

- Wenn dies die erste Bereitstellung ist, lesen Sie Maschinenkatalog erstellen.
- Spezielle Informationen zu Nutanix finden Sie unter Nutanix-Katalog erstellen.

Weitere Informationen

- Verbindungen und Ressourcen
- Maschinenkataloge erstellen

Verbindung zu VMware

June 27, 2024

Unter Verbindungen und Ressourcen erstellen und verwalten werden die Assistenten zum Erstellen einer Verbindung beschrieben. Die folgenden Informationen beziehen sich speziell auf VMware-Virtualisierungsumgebungen.

> **Hinweis:**
>
> Bevor Sie eine Verbindung zu VMware herstellen, müssen Sie zunächst Ihr VMware-Konto als Ressourcenstandort eingerichtet haben. Siehe VMware-Virtualisierungsumgebungen.

Verbindung erstellen

Führen Sie im Assistenten für die Verbindungserstellung folgende Schritte aus:

1. Wählen Sie den Verbindungstyp "VMware".
2. Geben Sie die Adresse des Zugriffspunkts für das vCenter SDK an.
3. Geben Sie die Anmeldeinformationen für ein zuvor eingerichtetes VMware-Konto ein, das Berechtigungen zum Erstellen von VMs hat. Geben Sie den Benutzernamen im Format Domäne/Benutzername ein.

VMware SSL-Fingerabdruck

Der VMware SSL-Fingerabdruck macht das manuelle Erstellen einer Hostverbindung zu einem VMware vSphere-Hypervisor überflüssig. Es ist nicht mehr erforderlich, dass der Administrator eine Vertrauensstellung zwischen den Site-Delivery Controllern und dem Hypervisor-Zertifikat vor dem Erstellen einer Verbindung manuell erstellt.

Das VMware SSL-Fingerabdruckfeature speichert den Fingerabdruck des nicht vertrauenswürdigen Zertifikats in der Sitedatenbank. Diese Konfiguration gewährleistet, dass der Hypervisor dauerhaft von Citrix Virtual Apps and Desktops als vertrauenswürdig identifiziert werden kann, selbst wenn die Controller dies nicht können.

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.

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
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

SDK	Benutzeroberfläche
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

SDK	Benutzeroberfläche
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:

> **Hinweis:**
>
> Diese Berechtigungen sind für die Erstellung von MCS-Maschinenkatalogen mit VMs mit vTPM 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

SDK	Benutzeroberfläche
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.

Zertifikat beschaffen und importieren

Um die vSphere-Kommunikation zu schützen, empfiehlt Citrix die Verwendung von HTTPS statt HTTP.

HTTPS benötigt digitale Zertifikate. Verwenden Sie ein digitales Zertifikat von einer Zertifizierungsstelle, das den Sicherheitsrichtlinien Ihrer Organisation entspricht.

Wenn Sie kein digitales Zertifikat verwenden können, das von einer Zertifizierungsstelle ausgestellt wurde, können Sie das mit VMware installierte selbstsignierte Zertifikat verwenden. Tun Sie das nur, wenn die Sicherheitsrichtlinie Ihrer Organisation es zulässt. 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 klicken Sie in Internet Explorer mit der rechten Maustaste und wählen Sie **Als Administrator ausführen**, um das Zertifikat herunterzuladen oder 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.

So geht es weiter

- Wenn dies die erste Bereitstellung ist, lesen Sie Maschinenkatalog erstellen.
- VMware-spezifische Informationen finden Sie unter VMware-Katalog erstellen.

Weitere Informationen

- Verbindungen und Ressourcen

- Maschinenkataloge erstellen

Verbindung zu VMware-Cloud und Partnerlösungen

June 27, 2024

Nachdem Sie den Azure VMware Solution (AVS)-Cluster, die Google Cloud VMware Engine und VMware Cloud auf AWS eingerichtet haben, erstellen Sie die Verbindungen. Informationen zum Erstellen von Verbindungen finden Sie im Artikel zur Verbindung zu VMware.

So geht es weiter

- Wenn dies die erste Bereitstellung ist, lesen Sie Maschinenkatalog erstellen.
- VMware-spezifische Informationen finden Sie unter VMware-Katalog erstellen.

Weitere Informationen

- Verbindungen und Ressourcen
- Maschinenkataloge erstellen

Imageverwaltung (Preview)

June 27, 2024

Einführung

Der MCS-Katalogerstellungs- oder Aktualisierungsprozess besteht aus zwei Phasen:

- Mastering: Ein Quellimage wird in ein veröffentlichtes Image umgewandelt
- Klonen: Neue VMs werden aus dem veröffentlichten Image erstellt

Mit der Imageverwaltungsfunktion trennt MCS die Masteringphase vom gesamten Bereitstellungsworkflow.

Sie können verschiedene MCS-Imageversionen (Vorbereitetes Image) aus einem einzigen Quellimage vorbereiten und es in mehreren verschiedenen MCS-Maschinenkatalogen verwenden. Diese Implementierung reduziert die Speicher- und Zeitkosten erheblich und vereinfacht die VM-Bereitstellung und den Imageaktualisierungsprozess.

Die Verwendung dieser Imageverwaltungsfunktion bietet folgende Vorteile:

- Generieren Sie vorbereitete Images im Voraus, ohne einen Katalog zu erstellen.
- Wiederverwenden Sie vorbereitete Images in mehreren Szenarien, z. B. beim Erstellen und Aktualisieren eines Katalogs.
- Reduzieren Sie die Zeit für die Katalogerstellung oder Aktualisierung erheblich.

> **Hinweis:**
>
> - Derzeit ist dieses Feature auf Azure-, GCP- und VMware-Virtualisierungsumgebungen anwendbar.
> - Sie können einen MCS-Maschinenkatalog erstellen, ohne vorbereitete Images zu verwenden. In diesem Fall können Sie die Vorteile des Features nicht nutzen.

Anwendungsfälle

Einige der Anwendungsfälle der Imageverwaltungsfunktionen sind:

- *Versionsverwaltung*: Mit Imageversionen haben Sie folgenden Möglichkeiten:
  - Verschiedene Iterationen oder Aktualisierungen eines bestimmten Images verwalten.
  - Mehrere Versionen eines Images für verschiedene Zwecke verwalten.
- *Logische Gruppierung*: Sie können für folgende Zwecke mehrere Imagedefinitionen erstellen:
  - Imageversionen logisch anhand verschiedener Kriterien wie Projekt, Abteilung oder Anwendung und Desktoptyp gruppieren.
  - Images innerhalb einer Organisation effizienter verwalten.

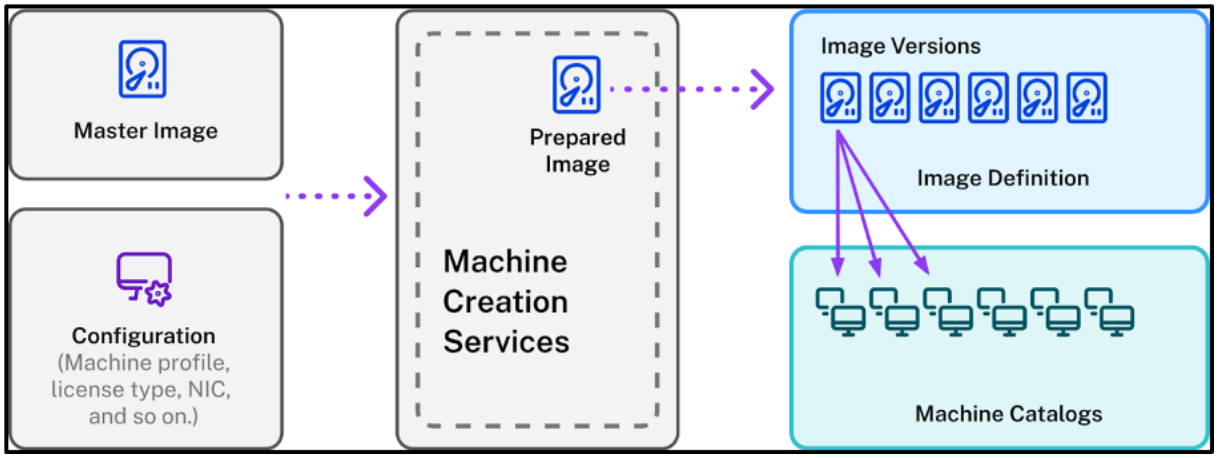
Was ist ein vorbereitetes Image?

Mit der Imageverwaltungsfunktion entkoppelt MCS die Mastering-Phase vom gesamten Workflow zur Katalogerstellung oder Aktualisierung und unterteilt den Prozess in zwei Phasen:

1. Vorbereitete Images aus einem einzigen Quellimage.
2. Vorbereitetes Image verwenden, um einen MCS-Maschinenkatalog zu erstellen oder zu aktualisieren.

Sie können die vorbereiteten Images im Voraus erstellen. Sie können ein einzelnes vorbereitetes Image verwenden, um mehrere von MCS bereitgestellte Maschinenkataloge zu erstellen oder zu aktualisieren.

Erfahren Sie, wie ein vorbereitetes Image in mehreren MCS-Maschinenkatalogen verwendet wird, wenn Sie das Web Studio vom Image aus verwenden:



Imagedefinition: Imagedefinitionen sind eine logische Gruppierung von Versionen eines Images. Die Imagedefinition enthält Informationen über:

- warum das Image erstellt wurde
- für welches Betriebssystem es erstellt wurde
- weitere Informationen zur Verwendung des Images.

Ein Katalog wird nicht aus einer Imagedefinition erstellt, sondern aus den Imageversionen, die auf der Grundlage der Imagedefinition erstellt werden.

Imageversion: Imageversionen verwalten Versionierungen für die Imagedefinition. Eine Imagedefinition kann mehrere Imageversionen haben. Verwenden Sie die Imageversionen als vorbereitete Images, um einen Katalog zu erstellen oder zu aktualisieren.

Wenn Sie PowerShell-Befehle verwenden möchten, um ein Provisioningschema zum Erstellen oder Aktualisieren eines Katalogs zu erstellen, müssen Sie alternativ eine vorbereitete Imageversionsspezifikation erstellen, die auf der Masterimageversionsspezifikation basiert, je nach Bedarf für Ihre Umgebung.

An Technical Preview teilnehmen

Wenn Sie an der Technical Preview teilnehmen möchten, geben Sie bitte hier Ihre Kontaktinformationen ein.

Wir helfen Ihnen bei der Einrichtung der Testumgebung und bieten bei Bedarf technischen Support.

Voraussetzung

- Für das Windows-Masterimage werden nur VDA-Images mit Version 2311 und höher und aktiviertem MCS/IO unterstützt.

Einschränkungen

Derzeit unterstützt das Feature Folgendes nicht:

- Mehrere Netzwerkkarten in Azure
- Feature für persistente Datenträger
- Ruhezustand für mehrere Sitzungen
- Änderung des Imagetyps

Imagelebenszyklusverwaltung mit dem Web Studio

Der Lebenszyklus des Images bei Verwendung des Web Studio ist:

1. Erstellen Sie ein vorbereitetes Image: Erstellen Sie eine Imagedefinition und ihre ursprüngliche Imageversion.
2. Erstellen Sie Imageversionen aus der ursprünglichen Imageversion.
3. Verwenden Sie eine Imageversion als vorbereitetes Image, um Kataloge zu erstellen.
4. Aktualisieren Sie einen Maschinenkatalog mit einem anderen vorbereiteten Image.
5. Verwalten Sie die Imagedefinitionen und Versionen: Bearbeiten Sie den Namen und die Beschreibung der Imageversionen sowie die Beschreibung einer Imagedefinition.
6. Löschen Sie eine Imageversion.
7. Löschen Sie eine Imagedefinition.

Alternativ können Sie Images auch mit PowerShell verwalten. Weitere Informationen finden Sie unter Imagelebenszyklusverwaltung mit PowerShell.

Katalog mit einem vorbereiteten Image erstellen oder aktualisieren

Erstellen Sie vorbereitete Images und verwenden Sie die vorbereiteten Images, um einen MCS-Maschinenkatalog zu erstellen oder zu aktualisieren. Verwenden Sie dazu:

- Web Studio
- PowerShell-Befehle

Web Studio verwenden

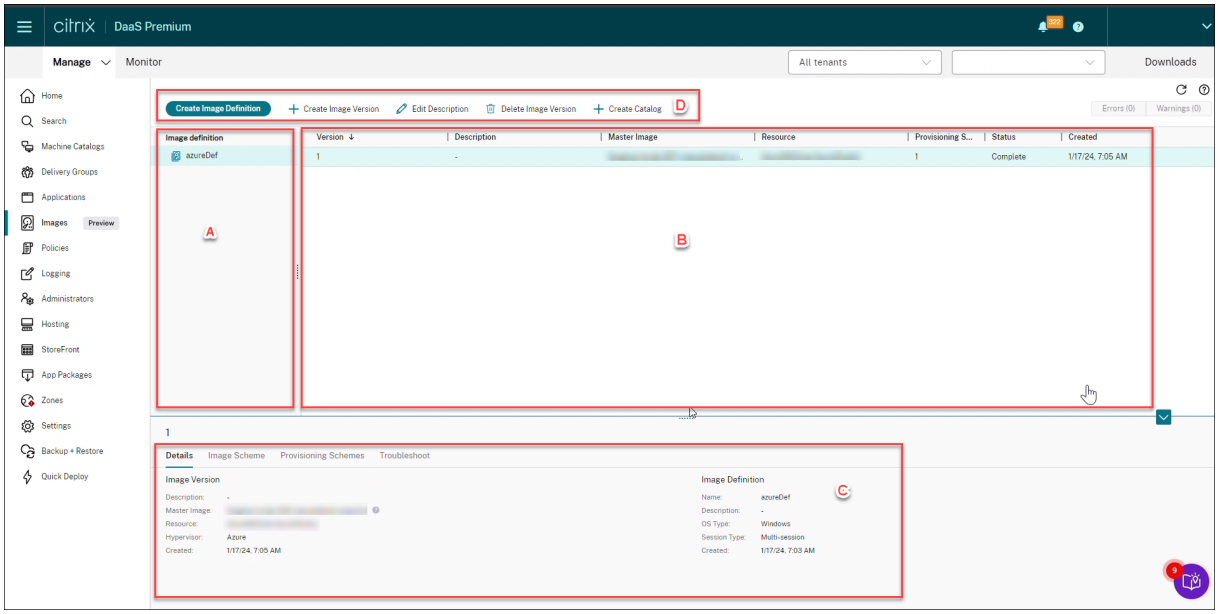
Lesen Sie die folgenden Artikel:

- Imageknoten verstehen
- Imagedefinition und eine erste Imageversion erstellen
- Imageversionen erstellen

- Maschinenkatalog über den Imageknoten erstellen
- Maschinenkatalog über den Maschinenkatalogknoten erstellen
- Maschinenkatalog mit einem anderen vorbereiteten Image aktualisieren
- Imagedefinitionen und -versionen verwalten

Imageknoten verstehen

Verwenden Sie den Knoten **Images**, um MCS-vorbereitete Images zu erstellen und zu verwalten. Seine Hauptansicht ist in vier Teile gegliedert:



Bezeichnung	Teil	Beschreibung
A	Imagedefinitionen	Listet die zuvor erstellten Imagedefinitionen auf.
B	Imageversionen	Zeigt Imageversionen der ausgewählten Imagedefinition an.
C	Details	• Auf der Registerkarte **Details** werden detaillierte Informationen zur ausgewählten Imagedefinition oder Version angezeigt, z. B. Masterimage, Ressource, Hypervisor, Name der Imagedefinition, Betriebssystemtyp und Sitzungstyp. • Auf der Registerkarte **Imageschema** werden Informationen zu der

Bezeichnung	Teil	Beschreibung
D	Aktionsleiste	Listet die Aktionen auf, die Sie für Imagedefinitionen und -versionen ausführen können, z. B. **Imageversion erstellen**, **Beschreibung bearbeiten**, **Imageversion löschen** und **Katalog erstellen**.

Maschinenkatalog mit dem vorbereiteten Image erstellen

Die wichtigsten Schritte zum Erstellen eines MCS-Maschinenkatalogs mit dem vorbereiteten Image sind:

1. Imagedefinition und die ersten Imageversionen erstellen.
2. Imageversion als vorbereitetes Image verwenden, um einen Katalog zu erstellen.

Imagedefinition und eine erste Imageversion erstellen

Gehen Sie wie folgt vor, um eine Imagedefinition und die erste Imageversion zu erstellen:

1. Melden Sie sich bei Web Studio an und wählen Sie den Knoten **Images** aus. Klicken Sie auf der Seite **Einführung** auf **Weiter**.
2. Geben Sie auf der Seite **Imagedefinition** den **Betriebssystemtyp** und den **Sitzungstyp** für die Imagedefinition an.
3. Wählen Sie auf der Seite **Image** die Option **Ressourcen** und ein Masterimage aus, das Sie als Vorlage für die Erstellung der Imageversion verwenden möchten. Sie können das Kontrollkästchen **Maschinenprofil verwenden** aktivieren und ein Maschinenprofil auswählen.

   > **Hinweis:**
   >
   > Stellen Sie vor der Auswahl eines Images sicher, dass auf dem Masterimage VDA 2311 oder höher und auf dem VDA der MCSIO-Treiber installiert ist.

4. (Nur für Azure) Wählen Sie auf der Seite **Speicher- und Lizenztypen** den Speicher- und Lizenztyp aus, der im Rahmen der Imagevorbereitung verwendet werden soll.

   > **Hinweis:**
   >
   > Wenn Sie auf der Seite **Image** ein Maschinenprofil auswählen, wird der Lizenztyp des

> Maschinenprofils basierend auf der Profileinstellung vorab ausgewählt.

5. Auf der Seite mit den **Maschinenspezifikationen**:
   - Wählen Sie für Azure eine Maschinengröße aus. Wenn Sie auf der Seite **Image** ein Maschinenprofil auswählen, wird die Maschinengröße des Maschinenprofils standardmäßig ausgewählt.
   - Wenn Sie für VMware ein Maschinenprofil auswählen, können Sie die Anzahl der virtuellen CPUs sehen, die aus dem Maschinenprofil abgeleitet wurde. Sie ist unveränderlich. Wenn Sie kein Maschinenprofil auswählen, wird nur die Speichergröße angezeigt, die vom Masterimage abgeleitet wurde.
6. Wählen Sie auf der Seite **Netzwerkkarten** mindestens eine Netzwerkkarte für das Vorbereitungsimage aus oder fügen Sie sie hinzu. Wählen Sie für jede Netzwerkkarte ein zugeordnetes virtuelles Netzwerk aus.

   Wenn Sie für VMware kein Maschinenprofil auswählen, wird die dem Masterimage zugeordnete Netzwerkkarte standardmäßig ausgewählt. Wenn Sie ein Maschinenprofil auswählen, werden die Netzwerkkarten aus dem Maschinenprofil abgeleitet und die Anzahl ist unveränderlich.

   > **Hinweis:**
   >
   > Mehrere Netzwerkkarten werden in Azure nicht unterstützt.

7. (Nur für Azure) Wählen Sie auf der Seite **Datenträgereinstellungen** den vom Kunden verwalteten Verschlüsselungsschlüssel (CMEK) aus. Wenn das Maschinenprofil kein CMEK hat, das Masterimage aber schon, wählt es das CMEK vorab aus dem Masterimage aus.
8. Geben Sie auf der Seite **Versionsbeschreibung** eine Beschreibung für die ursprünglich erstellte Imageversion ein.
9. Überprüfen Sie auf der Seite **Zusammenfassung** die Details der Imagedefinition und der ursprünglich erstellten Imageversion. Geben Sie einen Namen und eine Beschreibung für die Imagedefinition ein. Klicken Sie auf **Fertigstellen**.

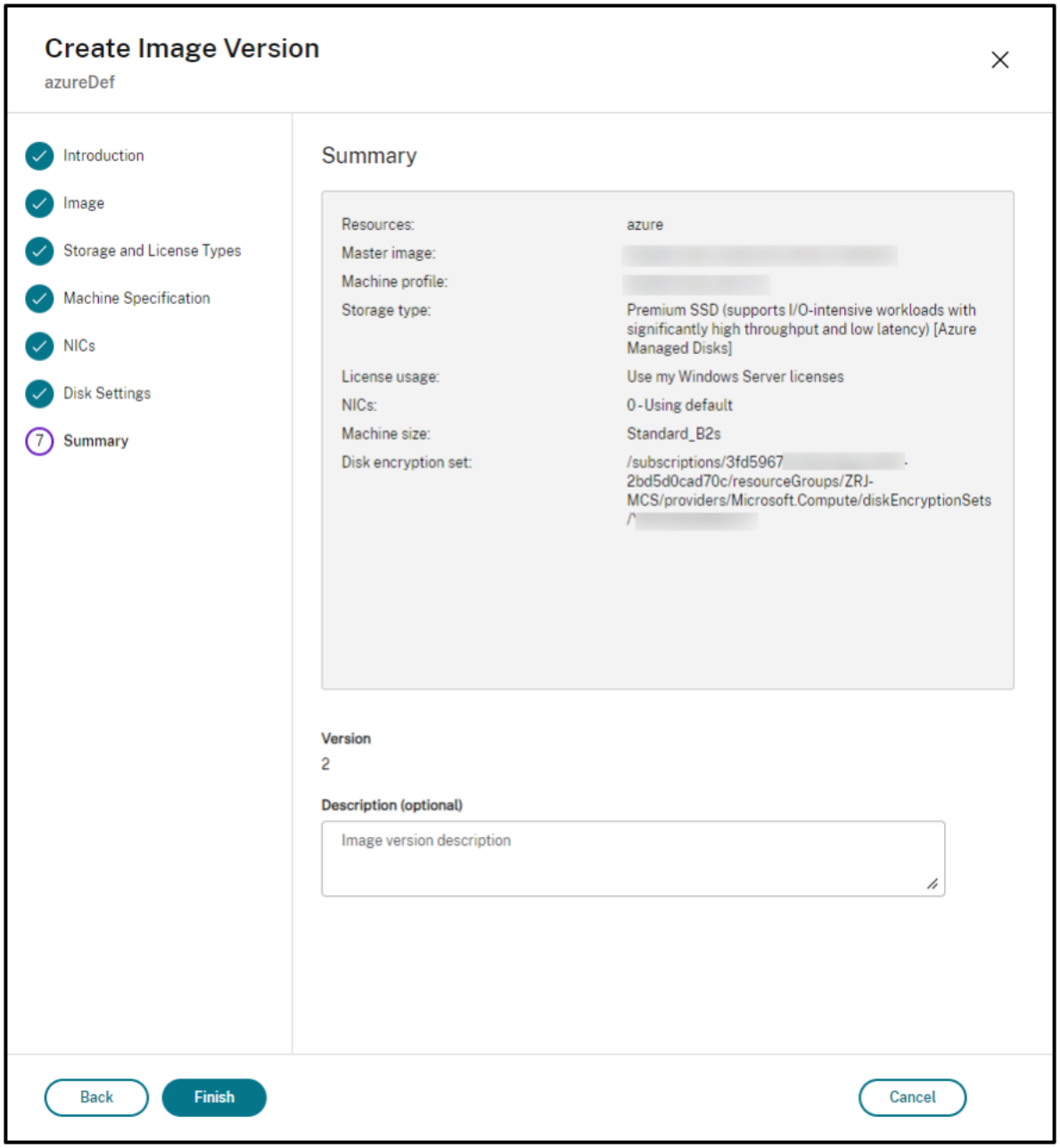
Imageversionen erstellen

Imageversionen ermöglichen die Verwaltung verschiedener Iterationen oder Aktualisierungen eines bestimmten Images. Mit dieser Funktion können Sie mehrere Versionen eines Images für verschiedene Zwecke verwalten.

Gehen Sie wie folgt vor, um Imageversionen aus der ursprünglichen Imageversion zu erstellen:

> **Hinweis:**
>
> Die Hostingeinheit aller Imageversionen muss identisch sein.

1. Gehen Sie zum Knoten **Images**, wählen Sie eine Imageversion aus und wählen Sie **Imageversion erstellen** aus.
2. Wenn Sie möchten, dass sich die Konfiguration der Imageversion von der ursprünglich konfigurierten Imageversion unterscheidet, konfigurieren Sie die Einstellungen auf den Seiten **Image**, **Speicher- und Lizenztypen**, **Maschinenspezifikation**, **Netzwerkkarten** und **Datenträgereinstellunge** des Dialogfelds **Imageversion erstellen**.
3. Fügen Sie eine Beschreibung für die Imageversion hinzu. Klicken Sie auf **Fertigstellen**.



Maschinenkatalog über den Imageknoten erstellen

Verwenden Sie die Option **Katalog erstellen** im Knoten **Images**, um einen Katalog mit der Imageversion zu erstellen.

Alternativ können Sie die Version auswählen, wenn Sie einen Katalog im Knoten **Maschinenkataloge erstellen** und eine Verknüpfung zur Option für das vorbereitete Image im Workflow zur Katalogerstellung herstellen. Weitere Informationen finden Sie unter Maschinenkatalog über den Knoten Maschinenkataloge erstellen.

Gehen Sie wie folgt vor, um einen MCS-Maschinenkatalog über den Knoten **Images** zu erstellen:

1. Wählen Sie eine Imageversion aus und klicken Sie auf **Katalog erstellen**. Klicken Sie auf der Seite **Einführung** auf **Weiter**.
2. Wählen Sie auf der Seite **Desktoperfahrung** die gewünschte Benutzeroberfläche für den Desktop aus.
3. Von der Seite **Image** zur Seite **Datenträgereinstellungen** sind die Einstellungen auf der Grundlage der ausgewählten Imageversion vorab ausgewählt.
4. (Für Azure) Auf der Seite **Ressourcengruppe** können Sie wählen, ob Sie eine neue Ressourcengruppe erstellen oder eine vorhandene Ressourcengruppe verwenden möchten, um die Ressourcen dieses Katalogs zu platzieren.
5. Ergänzen Sie die Einstellungen auf den folgenden Seiten.
6. Überprüfen Sie auf der Seite **Zusammenfassung** die Details des Maschinenkatalogs. Geben Sie einen Namen und eine Beschreibung für den Maschinenkatalog ein. Klicken Sie auf **Fertigstellen**.
7. Gehen Sie zum Knoten **Maschinenkataloge**, um den erstellten Maschinenkatalog anzuzeigen.

Maschinenkatalog über den Maschinenkatalogknoten erstellen

Gehen Sie wie folgt vor, um einen MCS-Maschinenkatalog über den Knoten **Maschinenkataloge** zu erstellen:

1. Klicken Sie im linken Navigationsbereich auf **Maschinenkataloge**.
2. Klicken Sie auf **Maschinenkatalog erstellen**. Die Seite **Maschinenkatalogerstellung** wird angezeigt. Klicken Sie auf den Seiten **Einführung**, **Maschinentyp** und **Maschinenverwaltung** immer auf **Weiter**.
3. Auf der Seite **Image**:

    a) Wählen Sie ein **vorbereitetes Image** aus.
    b) Wählen Sie unter **Vorbereitetes Image** eine Imageversion einer Imagedefinition aus.
    c) Klicken Sie auf den Namen der Imageversion. Um weitere Details zur ausgewählten Imageversion anzuzeigen, klicken Sie auf die Versionsnummer, die unterstrichen ist.
    d) Wenn die ausgewählte Imageversion mit einem Maschinenprofil konfiguriert ist, wählen Sie ein Maschinenprofil aus. Wenn die ausgewählte Imageversion nicht mit einem Maschinenprofil konfiguriert ist, können Sie sich nicht für die Verwendung eines Maschinenprofils entscheiden.

4. Konfigurieren Sie die Einstellungen auf den folgenden Seiten.
5. Wenn das ausgewählte vorbereitete Image auf der Seite **Datenträgereinstellungen** einen Datenträgerverschlüsselungssatz verwendet, können Sie den Verschlüsselungssatz nicht entfernen, aber Sie können den Schlüssel in einen anderen Verschlüsselungsschlüssel ändern.

6. (Für Azure) Auf der Seite **Ressourcengruppe** können Sie wählen, ob Sie eine neue Ressourcengruppe erstellen oder eine vorhandene Ressourcengruppe verwenden möchten, um die Ressourcen dieses Katalogs zu platzieren.
7. Ergänzen Sie die Einstellungen auf den folgenden Seiten.
8. Überprüfen Sie auf der Seite **Zusammenfassung** die Details des Maschinenkatalogs. Geben Sie einen Namen und eine Beschreibung für den Maschinenkatalog ein. Klicken Sie auf **Fertigstellen**.

Maschinenkatalog mit einem anderen vorbereiteten Image aktualisieren

Gehen Sie wie folgt vor, um einen vorhandenen MCS-Maschinenkatalog mit einem anderen vorbereiteten Image zu aktualisieren:

1. Klicken Sie im linken Navigationsbereich auf **Maschinenkataloge** und wählen Sie einen Maschinenkatalog aus, den Sie aktualisieren möchten. Klicken Sie mit der rechten Maustaste und wählen Sie **Vorbereitetes Image ändern**.
2. Wählen Sie auf der Seite **Image** ein vorbereitetes Image aus.
3. Wählen Sie auf der Seite **Rolloutstrategie** aus, wann Sie diesen Katalog mit dem ausgewählten vorbereiteten Image aktualisieren möchten.
4. Überprüfen Sie auf der Seite **Zusammenfassung** die Details. Klicken Sie auf **Fertigstellen**.

Sie können den Verlauf der an einem Katalog vorgenommenen Imageänderungen einsehen. Gehen Sie wie folgt vor, um den Verlauf anzuzeigen:

1. Wählen Sie einen Maschinenkatalog.
2. Klicken Sie auf der Registerkarte **Vorlageneigenschaften** im Feld **Vorbereitetes Image** auf **Imageverlauf anzeigen**.

Imagedefinitionen und -versionen verwalten

Sie können die Imagedefinitionen und -versionen bearbeiten und löschen, um die Verwendung verschiedener erstellter Imageversionen und -definitionen zu verwalten.

Imagedefinition bearbeiten Sie können den Namen und die Beschreibung einer Imagedefinition bearbeiten.

Gehen Sie wie folgt vor, um eine Imagedefinition zu bearbeiten:

1. Gehen Sie zum Knoten **Images**, wählen Sie eine Imagedefinition aus und wählen Sie **Imagedefinition bearbeiten** aus.

Imageversion bearbeiten Sie können die Beschreibung einer Imageversion bearbeiten, um den Zweck dieser Imageversion anzugeben.

Gehen Sie wie folgt vor, um eine Imageversion zu bearbeiten:

1. Gehen Sie zum Knoten **Images**, wählen Sie eine Imageversion und dann **Beschreibung bearbeiten** aus.

Imageversion löschen Gehen Sie wie folgt vor, um eine Imageversion zu löschen:

1. Gehen Sie zum Knoten **Images**, wählen Sie eine Imageversion und **Imageversion löschen** aus.

> **Hinweis:**
>
> Sie können eine Imageversion nicht löschen, wenn sie von einem Maschinenkatalog verwendet wird.

Imagedefinition löschen Gehen Sie wie folgt vor, um eine Imagedefinition zu löschen:

1. Gehen Sie zum Knoten **Images**, wählen Sie eine Imagedefinition aus und wählen Sie **Imagedefinition löschen** aus.

> **Hinweis:**
>
> Sie können eine Imagedefinition nicht löschen, wenn sie eine Imageversion enthält.

Imagelebenszyklusverwaltung mit PowerShell Wenn Sie PowerShell-Befehle verwenden möchten, um ein Provisioningschema zu erstellen, müssen Sie eine vorbereitete Imageversionsspezifikation erstellen, die auf der Masterimageversionsspezifikation basiert, je nach Bedarf für Ihre Umgebung.

Masterimageversionsspezifikation: Eine Masterimageversionsspezifikation ist ein bestimmtes Image, das unter einer Imageversion hinzugefügt oder erstellt wurde. Sie können ein vorhandenes Image im Hypervisor als Masterimageversionsspezifikation hinzufügen oder eine vorbereitete Imageversionsspezifikation erstellen, die auf der Masterimageversionsspezifikation basiert, je nach Bedarf für Ihre Umgebung. Die Spezifikation für die vorbereitete Imageversion kann für mehrere Provisioningschemata verwendet werden.

Der Lebenszyklus eines Images bei Verwendung von PowerShell-Befehlen ist:

1. Image erstellen:
    a) Erstellen Sie eine Imagedefinition.
    b) Erstellen Sie eine Imageversion.
    c) Fügen Sie eine Masterimageversionsspezifikation hinzu.

   d) Erstellen Sie eine vorbereitete Imageversionsspezifikation.

2. Erstellen Sie einen MCS-Maschinenkatalog mit einer vorbereiteten Imageversionsspezifikation:

   a) Erstellen Sie einen Brokerkatalog.
   b) Erstellen Sie einen Identitätspool.
   c) Erstellen Sie mit dem Befehl `New-ProvScheme` ein Provisioningschema mit dem Parameter der UID der vorbereiteten Imageversionsspezifikation.
   d) Verknüpfen Sie den Brokerkatalog mit dem Provisioningschema.

3. Erstellen Sie virtuelle Maschinen im MCS-Maschinenkatalog.
4. Ändern Sie die Versionsspezifikation für das vorbereitete Image eines Provisioningschemas mit dem Befehl `Set-ProvScheme`.
5. Verwaltung der Imagedefinitionen und Versionen: Bearbeiten Sie die Imageversionen und Imagedefinitionen.
6. Löschen eines MCS-Maschinenkatalogs: Die Löschreihenfolge lautet: Versionsspezifikation des vorbereiteten Images > Versionsspezifikation des Masterimages > Imageversion > Imagedefinition. Stellen Sie vor dem Löschen der Imageversionsspezifikation sicher, dass die vorbereitete Imageversionsspezifikation keinem MCS-Maschinenkatalog zugeordnet ist.

PowerShell verwenden

Sie können PowerShell-Befehle für Folgendes verwenden:

- Vorbereitetes Image erstellen
- Katalog mit der Versionsspezifikation für das vorbereitete Image erstellen
- Katalog mit einer Versionsspezifikation für das vorbereitete Image aktualisieren
- Imagedefinition, Imageversion und Versionsspezifikation für das vorbereitete Image löschen
- Imagedefinition und Imageversion verwalten
- Imagedefinition, Imageversion, Versionsspezifikation für das vorbereitete Image und das Provisioningschema abrufen

Vorbereitetes Image erstellen

Die detaillierten PowerShell-Befehle zum Erstellen einer Versionsspezifikation für das vorbereitete Image lauten wie folgt:

1. Überprüfen Sie die verfügbaren Imagedefinitionsnamen mit dem Befehl `Test-ProvImageDefinitionN command`. Beispiel:


```
Test-ProvImageDefinitionNameAvailable -ImageDefinitionName <string
    []>
<!--NeedCopy-->
```

2. Erstellen Sie eine Imagedefinition mit dem Befehl `New-ProvImageDefinition`. Beispiel:

```
New-ProvImageDefinition -ImageDefinitionName image1 -OsType
    Windows -VdaSessionSupport MultiSession
<!--NeedCopy-->
```

3. Erstellen Sie eine Imageversion mit dem Befehl `New-ProvImageVersion`. Beispiel:

```
New-ProvImageVersion -ImageDefinitionName image1 -Description "
    version 1"
<!--NeedCopy-->
```

4. Fügen Sie der Imageversion mithilfe des Befehls `Add-ProvImageVersionSpec` eine Masterimageversionsspezifikation hinzu. Beispiel:

```
Add-ProvImageVersionSpec -ImageDefinitionName  image1  -
    ImageVersionNumber  1 -HostingUnitName azure -MasterImagePath "
    XDHyp:\HostingUnits\azure\image.folder\azureresourcegroup.
    resourcegroup\win2022-snapshot.snapshot"
<!--NeedCopy-->
```

> **Hinweis:**
>
> Sie können einer Imageversion für eine Hostingeinheit nur eine Masterimageversionsspezifikation hinzufügen.

5. Erstellen Sie mit dem Befehls `New-ProvImageVersionSpec` eine Versionsspezifikation für das vorbereitete Image aus der Masterimageversionsspezifikation. Beispiel:

```
New-ProvImageVersionSpec
-SourceImageVersionSpecUid  c6e7384c-b2f8-46d6-9519-29a2c57ed3cb
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\azure\virtualprivatecloud.folder\
     azureresourcegroup.resourcegroup\azure-vnet-eastus.
     virtualprivatecloud\dev.network"
-ServiceOffering "XDHyp:\HostingUnits\azure\serviceoffering.folder
    \Standard_B2ms.serviceoffering" -CustomProperties "<
    CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
    machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
    instance`"></CustomProperties>" -RunAsynchronously
<!--NeedCopy-->
```

> **Hinweis:**
>
> Eine Hostingeinheit und ein Vorbereitungstyp können nur eine vorbereitete Instanz haben.

Beispiel für den vollständigen Satz von Powershell-Befehlen zum Erstellen von Imagedefinition, Imageversion und Versionsspezifikation des vorbereiteten Images in Azure:

```
$ImageDefintion = New-ProvImageDefinition
-ImageDefinitionName image1 -OsType Windows -VdaSessionSupport
    MultiSession
 $ImageVersion = New-ProvImageVersion -ImageDefinitionName
     $ImageDefintion.ImageDefinitionName -Description "version 1"
$MasterImagePath = "XDHyp:\HostingUnits\azure\image.folder\
    azureresourcegroup.resourcegroup\win2022-snapshot.snapshot"
$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageDefinitionName
     $ImageVersion.ImageDefinitionName -ImageVersionNumber $ImageVersion
    .ImageVersionNumber -HostingUnitName azure -MasterImagePath
    $MasterImagePath
$Task = New-ProvImageVersionSpec -SourceImageVersionSpecUid
    $SourceImageVersionSpec.ImageVersionSpecUid -NetworkMapping @{
 "0"="XDHyp:\HostingUnits\azure\virtualprivatecloud.folder\
     azureresourcegroup.resourcegroup\azure-vnet-eastus.
     virtualprivatecloud\dev.network" }
  -ServiceOffering "XDHyp:\HostingUnits\azure\serviceoffering.folder\
      Standard_B2ms.serviceoffering" -CustomProperties "<
      CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
      machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
      instance`"></CustomProperties>" -RunAsynchronously
Get-ProvTask -TaskId $Task.TaskId
<!--NeedCopy-->
```

Beispiel für den vollständigen Satz von Powershell-Befehlen zum Erstellen von Imagedefinition, Imageversion und Versionsspezifikation des vorbereiteten Images in VMware:

```
$ImageDefintion = New-ProvImageDefinition -ImageDefinitionName image2 -
    OsType Windows -VdaSessionSupport SingleSession
$ImageVersion = New-ProvImageVersion -ImageDefinitionName
    $ImageDefintion.ImageDefinitionName -Description "version 1"
$MasterImagePath = "XDHyp:\HostingUnits\vmware\win10-master.vm\win10-
    master-snap.snapshot"
$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageDefinitionName
     $ImageVersion.ImageDefinitionName -ImageVersionNumber $ImageVersion
    .ImageVersionNumber -HostingUnitName vmware -MasterImagePath
    $MasterImagePath
$Task = New-ProvImageVersionSpec -SourceImageVersionSpecUid
    $SourceImageVersionSpec.ImageVersionSpecUid -NetworkMapping @{
 "0"="XDHyp:\HostingUnits\vmware\DSwitch-VM Network.network" }
  -VMCpuCount 2 -VMMemoryMB 4096 -RunAsynchronously
Get-ProvTask -TaskId $Task.TaskId
<!--NeedCopy-->
```

> **Hinweis:**
>
> - Alle Imageversionsspezifikationen in einer Imagedefinition müssen zu derselben Hostingeinheit gehören.

> - Eine Imageversion kann nur eine Masterimageversionsspezifikation und eine Versionsspezifikation für das vorbereitete Image haben.
> - Entweder müssen alle Imageversionsspezifikationen ein Maschinenprofil haben oder keine.
> - Sie können beim Erstellen einer Imageversionsspezifikation keine Ressourcengruppe angeben.

Katalog mit einer Versionsspezifikation für ein vorbereitetes Image erstellen

Erstellen Sie mit dem Befehl `New-ProvScheme` einen MCS-Maschinenkatalog aus der vorbereiteten Imageversionsspezifikation. Beispiel:

```
1 New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid <
      Guid> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> [-VMCpuCount <
      int>] [-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping <
      Hashtable>] [-CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable
      >] [-ServiceOffering <string>] [-SecurityGroup <string[]>] [-
      TenancyType <string>] [-MachineProfile <string>] [-CustomProperties
      <string>] [-ResetAdministratorPasswords] [-
      UseFullDiskCloneProvisioning] [-RunAsynchronously] [-
      PurgeJobOnSuccess] [-ProvisioningSchemeType <ProvisioningSchemeType
      >]
2 <!--NeedCopy-->
```

Oder

```
1 New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid <
      Guid> -HostingUnitName <string> -IdentityPoolName <string> [-
      VMCpuCount <int>] [-VMMemoryMB <int>] [-UseWriteBackCache] [-
      NetworkMapping <Hashtable>] [-CleanOnBoot] [-Scope <string[]>] [-
      Metadata <Hashtable>] [-ServiceOffering <string>] [-SecurityGroup <
      string[]>] [-TenancyType <string>] [-MachineProfile <string>] [-
      CustomProperties <string>] [-ResetAdministratorPasswords] [-
      UseFullDiskCloneProvisioning] [-RunAsynchronously] [-
      PurgeJobOnSuccess] [-ProvisioningSchemeType <ProvisioningSchemeType
      >]
2 <!--NeedCopy-->
```

Beispiel für den vollständigen Satz von Powershell-Befehlen zum Erstellen eines Katalogs in Azure:

```
1 $Catalog = New-BrokerCatalog  -AllocationType "Random"  -IsRemotePC
      $False  -MinimumFunctionalLevel "L7_20" -Name "azurecatalog" -
      PersistUserChanges "Discard" -ProvisioningType "MCS" -Scope @() -
      SessionSupport "MultiSession"
2 $IdentityPool = New-AcctIdentityPool  -AllowUnicode  -Domain "azure.
      local" -IdentityPoolName "azurecatalog" -IdentityType "
      ActiveDirectory"  -NamingScheme "azure##" -NamingSchemeType "Numeric
      " -Scope @()
```



```
$PreparedImageVersionSpec = Get-ProvImageVersionSpec -
    ImageDefinitionName image1 -ImageVersionNumber 1 -Filter "
    PreparationType -eq 'Mcs'"
$Task = New-ProvScheme -ProvisioningSchemeName azurecatalog -
    ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid -
    HostingUnitName azure -IdentityPoolName azurecatalog -CleanOnBoot -
    Scope @() -SecurityGroup @() -ServiceOffering "XDHyp:\HostingUnits\
    azure\serviceoffering.folder\Standard_B2s.serviceoffering" -
    NetworkMapping @{
 "0"="XDHyp:\HostingUnits\azure\virtualprivatecloud.folder\
     azureresourcegroup.resourcegroup\azure-vnet-eastus.
     virtualprivatecloud\dev.network" }
  -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=`"StandardSSD_LRS`" /></
     CustomProperties>" -RunAsynchronously
Get-ProvTask -TaskId $Task.TaskId
$ProvScheme = Get-ProvScheme -ProvisioningSchemeName azurecatalog
Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId $ProvScheme
    .ProvisioningSchemeUid
<!--NeedCopy-->
```

Beispiel für den vollständigen Satz von Powershell-Befehlen zum Erstellen eines Katalogs in VMware:

```
$Catalog = New-BrokerCatalog  -AllocationType "Random"  -IsRemotePC
    $False  -MinimumFunctionalLevel "L7_20" -Name "vmwarecatalog" -
    PersistUserChanges "Discard" -ProvisioningType "MCS" -Scope @() -
    SessionSupport "MultiSession"
$IdentityPool = New-AcctIdentityPool  -AllowUnicode  -Domain "vmware.
    local" -IdentityPoolName "vmwarecatalog" -IdentityType "
    ActiveDirectory"  -NamingScheme "vmware##" -NamingSchemeType "
    Numeric" -Scope @()
$PreparedImageVersionSpec = Get-ProvImageVersionSpec -
    ImageDefinitionName image2 -ImageVersionNumber 1 -Filter "
    PreparationType -eq 'Mcs'"
$Task = New-ProvScheme -ProvisioningSchemeName vmwarecatalog -
    ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid -
    HostingUnitName vmware -IdentityPoolName vmwarecatalog -CleanOnBoot
    -Scope @() -SecurityGroup @() -NetworkMapping @{
 "0"="XDHyp:\HostingUnits\vmware\DSwitch-VM Network.network" }
  -VMCpuCount 2 -VMMemoryMB 4096 -RunAsynchronously
Get-ProvTask -TaskId $Task.TaskId
$ProvScheme = Get-ProvScheme -ProvisioningSchemeName vmwarecatalog
Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId $ProvScheme
    .ProvisioningSchemeUid
<!--NeedCopy-->
```


Katalog mit einer Versionsspezifikation für das vorbereitete Image aktualisieren

Mit dem Befehl `Set-ProvSchemeImage` können Sie einen Katalog aktualisieren. Beispiel:

```
Set-ProvSchemeImage -ProvisioningSchemeUid <Guid> -ImageVersionSpecUid
    <Guid> [-DoNotStoreOldImage] [-RunAsynchronously] [-
    PurgeJobOnSuccess]
<!--NeedCopy-->
```

Oder

```
Set-ProvSchemeImage -ProvisioningSchemeName <string> -
    ImageVersionSpecUid <Guid> [-DoNotStoreOldImage] [-RunAsynchronously
    ] [-PurgeJobOnSuccess]
<!--NeedCopy-->
```

Beispiel für den vollständigen Satz von Powershell-Befehlen zum Aktualisieren eines Katalogs:

```
$PreparedImageVersionSpec = Get-ProvImageVersionSpec -
    ImageDefinitionName image1 -ImageVersionNumber 2 -Filter "
    PreparationType -eq 'Mcs'"
Set-ProvSchemeImage -ProvisioningSchemeName azurecatalog -
    ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid -
    RunAsynchronously
<!--NeedCopy-->
```

Imagedefinition, Imageversion und Versionsspezifikation für das vorbereitete Image löschen

Beachten Sie Folgendes, bevor Sie eine Imagedefinition, eine Imageversion und eine Versionsspezifikation für das vorbereitete Image löschen:

- Eine Imagedefinition kann nicht gelöscht werden, wenn sie eine Imageversion enthält.
- Eine Imageversion kann nicht gelöscht werden, wenn sie eine Imageversionsspezifikation enthält.
- Eine Masterimageversionsspezifikation kann nicht gelöscht werden, wenn sie von einer anderen Versionsspezifikation für das vorbereitete Image verwendet wird.
- Eine Versionsspezifikation für das vorbereitete Image kann nicht gelöscht werden, wenn sie von einem Provisioningschema verwendet wird.

Verfahren:

1. Entfernen Sie eine Versionsspezifikation für das vorbereitete Image. Beispiel:

```
$PreparedImageVersionSpec = Get-ProvImageVersionSpec -
    ImageDefinitionName image1 -ImageVersionNumber 1 -Filter "
    PreparationType -eq 'Mcs'"
```



```
Remove-ProvImageVersionSpec -ImageVersionSpecUid
    $PreparedImageVersionSpec.ImageVersionSpecUid -
    RunAsynchronously
<!--NeedCopy-->
```

> **Hinweis:**
>
> Die Masterimageversionsspezifikation kann nur gelöscht werden, wenn keine Versionsspezifikation für das vorbereitete Image vorhanden ist.

2. Entfernen Sie die Masterimageversionsspezifikation. Beispiel:

```
$MasterImageVersionSpec = Get-ProvImageVersionSpec -
    ImageDefinitionName image1 -ImageVersionNumber 1 -Filter "
    PreparationType -eq 'None'"
Remove-ProvImageVersionSpec -ImageVersionSpecUid
    $PreparedImageVersionSpec.ImageVersionSpecUid -
    RunAsynchronously
<!--NeedCopy-->
```

3. Entfernen Sie eine Imageversion. Beispiel:

```
Remove-ProvImageVersion -ImageDefinitionName image1 -
    ImageVersionNumber 1
<!--NeedCopy-->
```

4. Entfernen Sie eine Imagedefinition. Beispiel:

```
Remove-ProvImageDefinition -ImageDefinitionName image1
<!--NeedCopy-->
```

Beispiel für den vollständigen Satz von PowerShell-Befehlen:

```
$PreparedImageVersionSpec = Get-ProvImageVersionSpec -
    ImageDefinitionName image1 -ImageVersionNumber 1 -Filter "
    PreparationType -eq 'Mcs'"
$Task = Remove-ProvImageVersionSpec -ImageVersionSpecUid
    $PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously
$MasterImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
     image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'None'"
$Task = Remove-ProvImageVersionSpec -ImageVersionSpecUid
    $PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously
Remove-ProvImageVersion -ImageDefinitionName image1 -ImageVersionNumber
     1
Remove-ProvImageDefinition -ImageDefinitionName image1
<!--NeedCopy-->
```


Imagedefinition und Imageversion verwalten

Sie können eine Imagedefinition umbenennen und bearbeiten sowie eine Imageversion bearbeiten.

- Benennen Sie eine Imagedefinition mit dem Befehl `Rename-ProvImageDefinition` um. Beispiel:

```
Rename-ProvImageDefinition -ImageDefinitionUid <Guid> -
    NewImageDefinitionName <string>
<!--NeedCopy-->
```

  Oder

```
Rename-ProvImageDefinition -ImageDefinitionName <string> -
    NewImageDefinitionName <string>
<!--NeedCopy-->
```

- Bearbeiten Sie eine Imagedefinition mit dem Befehl `Set-ProvImageDefinition`. Beispiel:

```
Set-ProvImageDefinition -ImageDefinitionUid <Guid> [-Description
    <string>]
<!--NeedCopy-->
```

  Oder

```
Set-ProvImageDefinition -ImageDefinitionName <string> [-
    Description <string>]
<!--NeedCopy-->
```

- Bearbeiten Sie eine Imageversion mit dem Befehl `Set-ProvImageVersion`. Beispiel:

```
Set-ProvImageVersion -ImageVersionUid <Guid> [-Description <
    string>]
<!--NeedCopy-->
```

  Oder

```
Set-ProvImageVersion -ImageDefinitionName <string> -
    ImageVersionNumber <int> [-Description <string>]
<!--NeedCopy-->
```

Imagedefinition, Imageversion, Versionsspezifikation für das vorbereitete Image und das Provisioningschema abrufen

- Rufen Sie die Imagedefinitionsdetails mit dem Befehl `Get-ProvImageDefinition` ab. Beispiel:


```
Get-ProvImageDefinition [-ImageDefinitionName <string>] [-
    ImageDefinitionUid <Guid>] [-ReturnTotalRecordCount] [-
    MaxRecordCount <int>] [-Skip <int>] [-SortBy <string>] [-
    Filter <string>]
<!--NeedCopy-->
```

- Rufen Sie die Imageversionsdetails mit dem Befehl `Get-ProvImageVersion` ab. Beispiel:
  - Um Imageversionen in einer Imagedefinition aufzulisten,

    ```
    Get-ProvImageVersion -ImageDefinitionUid <Guid>
    <!--NeedCopy-->
    ```

    Oder

    ```
    Get-ProvImageVersion -ImageDefinitionName <string>
    <!--NeedCopy-->
    ```

  - Um ein Detail der Imageversion zu erhalten,

    ```
    Get-ProvImageVersion -ImageVersionUid <Guid>
    <!--NeedCopy-->
    ```

    Oder

    ```
    Get-ProvImageVersion -ImageDefinitionName <string> -
        ImageVersionNumber <int>
    <!--NeedCopy-->
    ```

- Rufen Sie die Versionsspezifikation des vorbereiteten Images mit dem Befehl `Get-ProvImageVersionSpec` ab. Beispiel:
  - Um alle Versionsspezifikationen des vorbereiteten Images in einer Imageversion aufzulisten,

    ```
    Get-ProvImageVersionSpec -ImageVersionUid <Guid>
    <!--NeedCopy-->
    ```

  - Um die Masterimageversionsspezifikationen in einer Versionsspezifikation des vorbereiteten Images aufzulisten,

    ```
    Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter '
        PreparationType -eq "None"'
    <!--NeedCopy-->
    ```

  - Um die Versionsspezifikationen des vorbereiteten Images in einer Imageversion aufzulisten, die einem Masterimage zugeordnet ist,

    ```
    Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter '
        PreparationType -eq "MCS" -and SourceImageVersionSpecUid -
        eq "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"'
    ```



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

- Um Versionsspezifikationen eines erfolgreich vorbereitete Images in einer Imageversion zu erhalten,

```
Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter '
    PreparationType -eq "MCS" -and SourceImageVersionSpecUid -
    eq "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" -and
    ImageVersionSpecStatus -eq "Complete"'
<!--NeedCopy-->
```

- Um ein Versionsspezifikationsdetail für das vorbereitete Image zu erhalten,

```
Get-ProvImageVersionSpec -ImageVersionSpecUid <Guid>
<!--NeedCopy-->
```

- Rufen Sie mit dem Befehl `Get-ProvScheme` Details zum Provisioningschema ab. Beispiel:

```
Get-ProvScheme [[-ProvisioningSchemeName] <String>] [-
    ProvisioningSchemeUid <Guid>] [-ScopeId <Guid>] [-ScopeName <
    String>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>]
    [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-
    FilterScope <Guid>]
<!--NeedCopy-->
```

- Rufen Sie den Verlauf der Versionsspezifikation für das vorbereitete Image eines Provisioningschemas mit dem Befehl `Get-ProvSchemeImageVersionSpecHistory` ab. Beispiel:

```
Get-ProvSchemeImageVersionSpecHistory [-ProvisioningSchemeName <
    String>] [-ProvisioningSchemeUid <Guid>] [-ImageVersionSpecUid
     <Guid>] [-ImageVersionSpecHistoryUid <Guid>] [-
    ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <
    Int32>] [-SortBy <String>] [-Filter <String>] [-FilterScope <
    Guid>]
<!--NeedCopy-->
```

Maschinenkataloge erstellen

June 28, 2024

> **Wichtig:**
>
> Ab Citrix Virtual Apps and Desktops 7 2006 können Bereitstellung mit einer der folgenden Technologien erst dann auf die aktuelle Version aktualisiert werden, nachdem Elemente am Ende des Lebenszyklus (EOL), die diese Technologien verwenden, entfernt wurden.

- Persönliche vDisks (PvDs)
- AppDisks
- Hosts öffentlicher Clouds: Citrix CloudPlatform, Microsoft Azure Classic

Weitere Informationen finden Sie unter Entfernen von persönlichen vDisks, AppDisks und nicht unterstützten Hosts.

Hinweis:

Sie können Ihre Citrix Virtual Apps and Desktops-Bereitstellung mithilfe von zwei Verwaltungskonsolen verwalten: Web Studio (webbasiert) und Citrix Studio (Windows-basiert). Dieser Artikel behandelt nur Web Studio. Informationen zu Citrix Studio finden Sie im entsprechenden Artikel in Citrix Virtual Apps and Desktops 7 2212 oder früher.

Um in Ihrer Bereitstellung Verbindungen mit Hosts öffentlicher Clouds zu verwenden, benötigen Sie eine Hybrid Rights-Lizenz, um Ihre Neuinstallation oder das Upgrade auf die aktuelle Version abzuschließen.

Wenn das Installationsprogramm eine nicht unterstützte Technologie oder Hostverbindung ohne Hybrid Rights-Lizenz erkennt, wird das Upgrade angehalten oder beendet. Es wird eine Meldung mit einer Erläuterung angezeigt. Die Installationsprotokolle enthalten die Details. Weitere Informationen finden Sie unter Upgrade einer Bereitstellung.

Einführung

Sammlungen von physischen oder virtuellen Maschinen werden als Einheit in einem sogenannten Maschinenkatalog verwaltet. Alle Maschinen in einem Katalog haben den gleichen Betriebssystemtyp: Multisitzungs-OS oder Einzelsitzungs-OS sowie Windows- und Linux-Maschinen.

Nach dem Erstellen der Site werden Sie von Web Studio durch das Erstellen des ersten Maschinenkatalogs geführt. Nach dem Erstellen des ersten Maschinenkatalogs werden Sie in Web Studio durch das Erstellen der ersten Bereitstellungsgruppe geführt. Später können Sie den erstellten Katalog ändern und weitere Kataloge erstellen.

Tipp:

Beim Upgrade einer vorhandenen Bereitstellung wird die MCS-Speicheroptimierung (MCS E/A) aktiviert und es ist keine zusätzliche Konfiguration erforderlich. Das VDA- und das Delivery Controller-Upgrade sorgen für das MCS-E/A-Upgrade.

Übersicht

Wenn Sie einen Katalog virtueller Maschinen erstellen, geben Sie an, wie diese VMs bereitgestellt werden sollen. Sie können Maschinenerstellungsdienste (MCS) 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.
- 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 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 Web 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.
- Verwenden einer Vorlage für das Provisioning eines Katalogs wird als experimentelles Feature betrachtet. Bei dieser Methode kann die Vorbereitung der virtuellen Maschine fehlschlagen. Daher kann der Katalog nicht mit der Vorlage veröffentlicht werden.

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 Web 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 Web 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** an. Das Fenster findet sich auf der Seite **Maschinendetails und Benutzerdetails**. Weitere Informationen finden Sie unter Microsoft RDS-Lizenzstatus.

VDA-Registrierung

Ein VDA muss beim Start gebrokerter Sitzungen bei einem Delivery Controller registriert sein. 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. Web Studio bietet Informationen zur Problembehandlung im Assistenten zum Erstellen von Maschinenkatalogen und nach dem Hinzufügen von Maschinen eines Katalogs zu einer Bereitstellungsgruppe.

Nach dem Hinzufügen vorhandener Maschinen im Assistenten wird 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, entfernen Sie diese oder fügen Sie sie hinzu. Wird beispielsweise gemeldet, dass die Maschineninformationen nicht abgerufen werden konnten 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:

  - Die MCS-Speicheroptimierung erstellt einen Schreibcachedatenträger für jede VM.
  - Bei MCS können jetzt vollständige Klons verwendet werden, im Gegensatz zum Szenario mit Deltadatenträgern, das im vorherigen Abschnitt beschrieben wurde.

  Hypervisorfeatures spielen auch eine Rolle. Beispiel:

  - XenServer IntelliCache erstellt für jeden XenServer einen Lesedatenträger im lokalen Speicher. Diese Option spart IOPS gegen das Masterimage, 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 virtuellen Datenträger, 16 GB für die Auslagerungsdatei der virtuellen Maschine und 100 MB für Protokolldateien (insgesamt 36,1 GB).
  - 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.
  - Beim Aktualisieren des Katalogs wird für jeden Speicherort ein zusätzlicher Basisdatenträger erstellt. 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`.
- Verbesserte Diagnose durch die Unterstützung einer im Schreibcachedatenträger gespeicherten Windows-Absturzabbilddatei.
- 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:

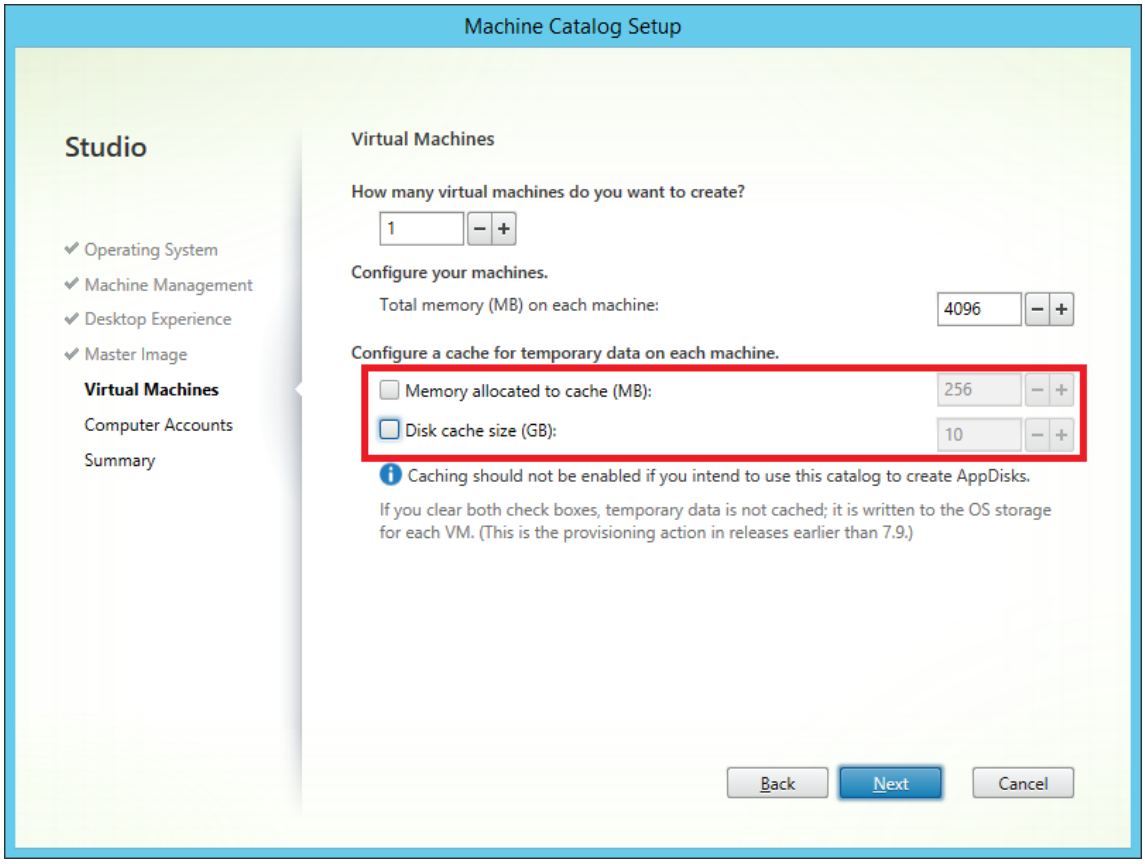
1. MCS-E/A unterstützt einen ausschließlich RAM-basierten Cache nicht mehr. Geben Sie beim Erstellen des Maschinenkatalogs eine Datenträgergröße in Web Studio an.
2. Der VM-Schreibcachedatenträger wird beim ersten Starten einer VM automatisch erstellt und formatiert. Sobald die VM läuft, wird die Schreibcachedatei `mcsdif.vhdx` in das formatierte Volume `MCSWCDisk` geschrieben.
3. Die Auslagerungsdatei wird an das formatierte Volume `MCSWCDisk` umgeleitet. Daher umfasst diese Datenträgergröße die Gesamtmenge des Speichers. Sie umfasst somit die Differenz zwischen der Datenträgergröße und der generierten Workload plus Auslagerungsdatei. Dies ist in der Regel mit der VM-RAM-Größe verknüpft.

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.



- Wird ein Maschinenkatalog auf einen neuen VM-Snapshot aktualisiert, der einen für Version 1903 konfigurierten VDA enthält, verwendet der neue Snapshot die MCS-E/A-Einstellung des Katalogs für RAM und Datenträgergröße weiter. Der bestehende Rohdatenträger wird formatiert.

> **Wichtig:**
>
> Die MCS-Speicheroptimierung wurde in Citrix Virtual Apps and Desktops 1903 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 Maschinenkatalog und weisen einen größeren Schreibcachedatenträger zu.

Laufwerksbuchstaben zu einem MCS-E/A-Zurückschreibcache-Datenträger zuweisen

Sie können dem MCS-E/A-Zurückschreibcache-Datenträger einen Laufwerksbuchstaben zuweisen. Diese Implementierung hilft bei der Vermeidung von Konflikten zwischen dem Laufwerksbuchstaben

verwendeter Anwendungen und dem Laufwerksbuchstaben des MCS-E/A-Zurückschreibcache-Datenträgers. Sie können mit PowerShell-Befehlen dem MCS-I/O-Zurückschreibcache-Datenträger einen Laufwerksbuchstaben zuweisen. Die unterstützten Hypervisors sind Azure, GCP, VMware, SCVMM und XenServer.

> **Hinweis:**
>
> Für dieses Feature ist VDA-Version 2305 oder höher erforderlich.

Einschränkungen

- Gilt nur für Windows-Betriebssysteme
- Möglicher Laufwerksbuchstabe für Zurückschreibcache-Datenträger: E bis Z
- Nicht möglich bei Verwendung des temporären Azure-Datenträgers als Zurückschreibcache-Datenträger
- Gilt nur, wenn Sie einen neuen Maschinenkatalog erstellen

Zurückschreibcache-Datenträger einen Laufwerksbuchstaben zuweisen

So weisen Sie dem Zurückschreibcache-Datenträger einen Laufwerksbuchstaben zu:

1. Öffnen Sie das **PowerShell**-Fenster.
2. Führen Sie `asnp citrix*` aus.
3. Erstellen Sie einen Identitätspool, falls noch nicht vorhanden.
4. Erstellen Sie mit dem Befehl `New-ProvScheme` mit der Eigenschaft `WriteBackCacheDriveLetter` ein Provisioningschema. Beispiel:

```
New-ProvScheme -CleanOnBoot `
-HostingUnitName "<name>" `
-IdentityPoolName $schemeName `
-ProvisioningSchemeName $schemeName `
-InitialBatchSizeHint 1 `
-UseWriteBackCache -WriteBackCacheDiskSize 127 -
   WriteBackCacheMemorySize 256 -WriteBackCacheDriveLetter E `
-MasterImageVM "XDHyp:\HostingUnits<name>\image.folder\abcd-
   resources.resourcegroup\
   MCSIOMasterVm_OsDisk_1_d3e2d6352xxxxxxxx2130aa145ec77.
   manageddisk" `
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\name\virtualprivatecloud.folder\East US.
    region\virtualprivatecloud.folder\abcd-resources.resourcegroup
    \abcd-resources-vnet.virtualprivatecloud\default.network" }
  `
-ServiceOffering "XDHyp:\HostingUnits\<name>\serviceoffering.
   folder\Standard_D2s_v5.serviceoffering" `
```



```
-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="OsType" Value="Windows" />
<Property xsi:type="StringProperty" Name="StorageType" Value="Premium_LRS"/>
<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false" />
<Property xsi:type="StringProperty" Name="PersistVm" Value="false" />
<Property xsi:type="StringProperty" Name="WBCDiskStorageType" Value="Premium_LRS" />
<Property xsi:type="StringProperty" Name="UseTempDiskForWBC" Value="false" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="abcd-group1" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="Windows_Client" />
<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />
</CustomProperties>'
<!--NeedCopy-->
```

5. Beenden Sie die Erstellung des Maschinenkatalogs. Weitere Informationen finden Sie unter https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

Vorbereiten eines Masterimages

Hinweise zum Erstellen von Hostverbindungen 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 verwenden andere Bezeichnungen.
- Vergewissern Sie sich, dass der Host 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.

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 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 Web 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. Vergewissern Sie sich, 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. Wenn Sie MCS nicht verwenden, fügen Sie das Masterimage der Domäne hinzu, zu der die Anwendungen und Desktops gehören. Vergewissern Sie sich, 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.

5. Citrix empfiehlt, dass Sie einen Snapshot des Masterimages erstellen und benennen. Wenn Sie ein Masterimage anstelle eines Snapshots beim Erstellen eines Maschinenkatalogs angeben, erstellt Web Studio automatisch einen Snapshot. Sie können es nicht benennen.

Aktivierung der Volumenlizenzierung

MCS unterstützt die Aktivierung der Volumenlizenzierung, mit der die Aktivierung von Windows-Betriebssystemen und Microsoft Office automatisiert und verwaltet werden kann. Es werden drei Modelle zur Aktivierung der Volumenlizenzierung unterstützt:

- Key Management Service (KMS)
- Active Directory-basierte Aktivierung (ADBA)
- Multiple Activation Key (MAK)

Sie können die Aktivierungseinstellung ändern, nachdem Sie den Maschinenkatalog erstellt haben.

Key Management Service (KMS)

Der KMS-Dienst erfordert kein dediziertes System und kann problemlos mit anderen Diensten auf einem System gehostet werden. Die Funktion wird von allen von Citrix unterstützten Windows-Versionen unterstützt. Während der Image-Vorbereitung werden Microsoft Windows KMS und Microsoft Office KMS durch MCS zurückgesetzt. Mit dem Befehl `Set-Provserviceconfigurationdata` können Sie das Zurücksetzen überspringen. Weitere Informationen zum Zurücksetzen von Microsoft Windows KMS und Microsoft Office KMS während der Image-Vorbereitung finden Sie unter Machine Creation Services: Image Preparation Overview and Fault-Finding. Weitere Informationen zur KMS-Aktivierung finden Sie unter Aktivieren mit dem Schlüsselverwaltungsdienst.

> **Hinweis:**
>
> Alle Maschinenkataloge, die nach dem Ausführen des Befehls `Set-Provserviceconfigurationdata` erstellt wurden, verwenden die im Befehl angegebene Einstellung.

Active Directory-basierte Aktivierung (ADBA)

Mit ADBA können Sie Maschinen über deren Domänenverbindungen aktivieren. Die Maschinen werden sofort aktiviert, wenn sie einer Domäne beitreten. Die Maschinen bleiben so lange aktiviert, wie

sie mit der Domäne verbunden und in Kontakt bleiben. Die Funktion wird von allen von Citrix unterstützten Windows-Versionen außer Windows Server 2022 unterstützt. Weitere Informationen zur Active Directory-basierten Aktivierung finden Sie unter Aktivierung über Active Directory.

Multiple Activation Key (MAK)

Mit dem Mehrfachaktivierungsschlüssel (oder MAK-Schlüssel) können Sie den Microsoft-Server nutzen, um Volumes zu aktivieren und das Windows-System zu authentifizieren. Der MAK-Schlüssel muss von Microsoft erworben werden, und jedem Schlüssel ist eine feste Anzahl von Aktivierungen zugewiesen. Mit jeder Aktivierung eines Windows-Systems verringert sich die Aktivierungsanzahl. Es gibt zwei Möglichkeiten zur Aktivierung des Systems:

- Online-Aktivierung: Wenn das Windows-System, das Sie aktivieren möchten, über einen Internetzugang verfügt, wird Windows automatisch bei der Installation des Produktschlüssels aktiviert. Dabei verringert sich die Aktivierungsanzahl für den entsprechenden MAK-Schlüssel um 1.
- Offline-Aktivierung: Wenn das Windows-System keine Verbindung zum Internet herstellen kann, erhält MCS vom Microsoft-Server eine Bestätigungs-ID und eine Installations-ID, um so das Windows-System zu aktivieren. Diese Art der Aktivierung ist für nicht-persistente Maschinenkataloge geeignet.

> **Hinweis:**
>
> - MCS unterstützt die Microsoft Office-Aktivierung mit MAK nicht.
> - Die erforderliche Mindestversion des VDA ist 2303.

Hauptanforderungen

- Der Delivery Controller muss über einen Internetzugang verfügen.
- Erstellen Sie einen neuen Katalog, wenn das Update einen anderen MAK-Schlüssel als das Original-Image verwendet.
- Installieren Sie den MAK-Schlüssel auf dem Masterimage. Die Schritte zur Installation des MAK-Schlüssels auf einem Windows-System finden Sie unter Deploy MAK Activation.
- Wenn Sie keine Imagevorbereitung verwenden:

  1. Fügen Sie den Registrierungs-DWORD-Wert `Manual` unter `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatfo\Activation` hinzu.
  2. Setzen Sie den Wert auf 1.

Anzahl der Aktivierungen Verwenden Sie das Tool für die Volumenaktivierungsverwaltung (VAMT), um die Anzahl der verbleibenden Aktivierungen für den MAK-Schlüssel anzuzeigen oder um zu überprüfen, ob eine VM mehrere Aktivierungen verbraucht. Siehe Installieren von VAMT.

Windows-System mit MAK-Schlüssel aktivieren Aktivieren des Windows-Systems mit MAK-Schlüssel:

1. Installieren Sie den Produktschlüssel auf dem Masterimage. Dabei verringert sich die Aktualisierungsanzahl um 1.
2. Erstellen Sie einen MCS-Maschinenkatalog.
3. Wenn Sie keine Imagevorbereitung verwenden:

   a) Fügen Sie den Registrierungs-DWORD-Wert `Manual` unter `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatfo\Activation` hinzu.
   b) Setzen Sie den Wert auf 1.

   Dadurch wird die Option der Online-Aktivierung deaktiviert.
4. Fügen Sie dem Maschinenkatalog virtuelle Maschinen hinzu.
5. Schalten Sie die VMs ein.
6. Das Windows-System wird nun je nach geplanter Aktivierungsart (online oder offline) aktiviert.

   - Bei einer Online-Aktivierung wird das Windows-System aktiviert, nachdem der Produktschlüssel installiert wurde.
   - Bei einer Offline-Aktivierung kommuniziert MCS mit den bereitgestellten VMs, um den Aktivierungsstatus des Windows-Systems abzurufen. MCS ruft dann vom Microsoft-Server eine Bestätigungs-ID und eine Installations-ID ab. Diese IDs werden verwendet, um das Windows-System zu aktivieren.

Problembehandlung Wenn die bereitgestellte VM nicht mit dem installierten MAK-Schlüssel aktiviert ist, führen Sie den Befehl `Get-ProvVM` oder `Get-ProvScheme` in einem PowerShell-Fenster aus.

- Befehl `Get-ProvScheme`: Siehe Parameter `WindowsActivationType`, der dem MCS-Maschinenkatalog vom neuesten Masterimage zugeordnet ist.
- Befehl `Get-ProvVM`. Siehe Parameter `WindowsActivationType`, `WindowsActivationStatus`, `WindowsActivationStatusErrorCode` und `WindowsActivationStatusError`.

Sie können den Fehler und die Schritte zur Behebung des Problems überprüfen.

Maschinenkatalog mit Web Studio erstellen

Vor dem Erstellen eines Katalogs:

- Lesen Sie diesen Abschnitt über die Optionen, die Sie auswählen, und welche Informationen Sie angeben müssen.
- Vergewissern Sie sich, dass Sie eine Verbindung zum Hypervisor, Cloudservice und anderen Ressourcen hergestellt haben, die Ihre Maschinen hosten.
- Wenn Sie ein Masterimage für das Provisioning von Maschinen erstellt haben, vergewissern Sie sich, dass Sie einen VDA auf diesem Image installiert haben.

Starten Sie den Assistenten zum Erstellen von Katalogen:

1. Wenn Sie den ersten Katalog erstellen, werden Sie zur richtigen Auswahl weitergeleitet (z. B. "Einrichten der Maschinen und Erstellen von Maschinenkatalogen zum Ausführen von Apps und Desktops"). Der Assistent zum Erstellen von Katalogen wird geöffnet.
2. Wenn Sie bereits einen Katalog erstellt haben und einen weiteren erstellen möchten, gehen Sie wie folgt vor:

    a) Melden Sie sich bei Web Studio an, wählen Sie im linken Bereich **Maschinenkataloge** und dann in der Aktionsleiste **Maschinenkatalog erstellen**.

    b) Um Kataloge mit Ordnern zu organisieren, erstellen Sie Ordner im Standardordner **Maschinenkataloge**. Weitere Informationen finden Sie unter Erstellen von Katalogordnern.

    c) Wählen Sie den Ordner aus, in dem Sie den Katalog erstellen möchten, und klicken Sie dann auf **Maschinenkatalog erstellen**. Der Assistent zum Erstellen von Katalogen wird geöffnet.

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 welchen Tools sie bereitgestellt werden.

Wählen Sie, ob für Maschinen im Katalog die Energieverwaltung über Web Studio ausgeführt wird.

- Maschinen mit Energieverwaltung über Web Studio (z. B. virtuelle Maschinen oder Blade-PC). Diese Option ist nur verfügbar, wenn Sie bereits eine Verbindung zu einem Host konfiguriert haben.
- Maschinen ohne Energieverwaltung über Web Studio (z. B. physische Maschinen).

Wenn Sie angegeben haben, dass die Energieverwaltung der Maschinen über Web Studio erfolgen soll, wählen Sie aus, welches Tool zum Erstellen von VMs verwendet werden soll.

- **Citrix Maschinenerstellungsdienste (MCS):** verwendet ein Masterimage zum Erstellen und Verwalten virtueller Maschinen. MCS ist für physische Maschinen nicht verfügbar.
- **Sonstiges:** Ein Tool, das Maschinen verwaltet, die bereits im Rechenzentrum sind. Citrix empfiehlt die Verwendung von Microsoft System Center Configuration Manager oder einer anderen Drittanbieteranwendung, um sicherzustellen, dass die Maschinen im Katalog konsistent sind.

Desktoptypen (Desktoperfahrung)

Diese Seite wird nur angezeigt, wenn Sie einen Maschinenkatalog mit 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.

Image

Diese Seite wird nur angezeigt, wenn Sie VMs mit MCS erstellen.

1. Wählen Sie einen Imagetyp für den Maschinenkatalog und dann ein Image aus. Zwei Imagetypen sind verfügbar:

   - **Masterimage.** Dies ist ein Image, das den Imagevorbereitungsprozess nicht durchlaufen hat. Der Imagevorbereitungsprozess wird automatisch eingeleitet, wenn die Katalogerstellung beginnt.

     > **Hinweis:**
     >
     > – Wenn Sie MCS verwenden, führen Sie auf den Masterimages nicht Sysprep aus.
     > – Wenn Sie ein Masterimage anstelle eines Snapshots angeben, erstellt Web Studio automatisch einen Snapshot, der jedoch nicht umbenannt werden kann.

   - **Vorbereitetes Image.** Ein Image, das den Imagevorbereitungsprozess durchlaufen hat und direkt für die VM-Erstellung verwendet werden kann. Wenn Sie sich bei der Katalogerstellung für vorbereitete Images statt für Masterimages entscheiden, wird eine schnellere und zuverlässigere Maschinenkatalogerstellung sowie eine optimierte Imagelebenszyklusverwaltung gewährleistet.

     > **Hinweis:**
     >
     > – VMs, die mit vorbereiteten Images erstellt wurden, unterstützen den Ruhezustand nicht.
     > – Derzeit ist das Erstellen von Katalogen mit vorbereiteten Images nur in Azure- und VMware-Umgebungen verfügbar.

   Weitere Informationen zum Erstellen vorbereiteter Bilder finden Sie unter Imageverwaltung (Preview).

   Wenn Sie ein Image auswählen, können Sie bei Bedarf eine Notiz für das ausgewählte Image hinzufügen.

   Vergewissern Sie sich, 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.

2. Um eine vorhandene VM als Maschinenprofil zu verwenden, wählen Sie **Maschinenprofil verwenden** und anschließend die VM aus.

> **Hinweis:**
>
> Derzeit ist die Verwendung von Maschinenprofilen auf Azure-, AWS-, GCP- und VMware-VMs beschränkt.

Bei VMware-Bereitstellungen müssen Sie beim Erstellen eines Maschinenkatalogs mit einem Maschinenprofil den Ordner angeben, in dem Sie die virtuellen Maschinen aufbewahren möchten.

Um den Speicherort des Ordners für virtuelle Maschinen anzugeben, gehen Sie im Assistenten zur Katalogerstellung zur Seite **Virtuelle Maschinen** und gehen Sie zum Abschnitt **Ordner auswählen, um die Maschinen zu platzieren**. Wählen Sie den Speicherort des Ordners der virtuellen Maschine aus. Wenn nicht angegeben, betrachtet das System den Ordner des ausgewählten Maschinenprofils als Standardspeicherort.

3. Wählen Sie die Mindestfunktionsebene für den Katalog. Damit Sie die neuesten Produktfeatures verwenden können, muss auf dem Masterimage die aktuelle VDA-Version installiert sein.

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. Geben Sie **0** (Null) ein, wenn Sie keine Maschine erstellen möchten. Später können Sie mit **Maschinen hinzufügen** virtuelle Maschinen für einen leeren Katalog erstellen.
- 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 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 vDisks erstellen, können Sie einen Cache für temporäre Daten auf jeder Maschine konfigurieren. Weitere Informationen finden Sie unter Konfigurieren eines Cache für temporäre Daten.

Bei Verwendung 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 anderer Tools (nicht MCS) führen Sie folgende Schritte aus:

Ein Symbol und eine QuickInfo für jede hinzugefügte (bzw. importierte) 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.

SIDs beim Erstellen virtueller Maschinen hinzufügen

Sie können jetzt den Parameter `ADAccountSid` hinzufügen, um die Maschinen beim Erstellen neuer virtueller Maschinen eindeutig zu identifizieren.

Gehen Sie hierzu folgendermaßen vor:

1. Erstellen Sie einen Katalog mit dem unterstützten Identitätstyp.
2. Fügen Sie dem Katalog mit `NewProvVM` Maschinen hinzu. Beispiel:

```
1 New-ProvVM  -ProvisioningSchemeName "name"  -ADAccountSid @("SID "
     )  -RunAsynchronously
2 <!--NeedCopy-->
```

Folgendes können Sie nicht auf einer Maschine bereitstellen:

- Ein AD-Konto, das sich nicht im Katalogidentitätspool befindet.
- Ein AD-Konto, das nicht im Status “Verfügbar”ist

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. Unter Neue Features werden für jede Version eventuelle Änderungen der Standardfunktionsebene aufgeführt.

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:**
>
> In Release 1811 wurde eine zusätzliche Funktionsebene hinzugefügt: **1811 (oder neuer)**. Die Ebene ist für die Verwendung mit künftigen Citrix Virtual Apps and Desktops-Features vorgese-

> hen. Die Standardebene ist weiterhin **7.9 (oder neuer)**. Die Standardebene gilt derzeit für alle Bereitstellungen.
>
> Wenn Sie **1811 (oder höher)** auswählen, können sich VDAs älterer Versionen in dem Katalog nicht mehr bei einem Controller registrieren. Wenn der Katalog jedoch nur VDAs der Version 1811 oder neuer enthält, können sich alle registrieren. Dazu gehören Kataloge mit VDAs, die für spätere Citrix Virtual Apps and Desktops-Releases konfiguriert sind, einschließlich Version 1903 und andere 19XX-Releases vor dem aktuellen Release.

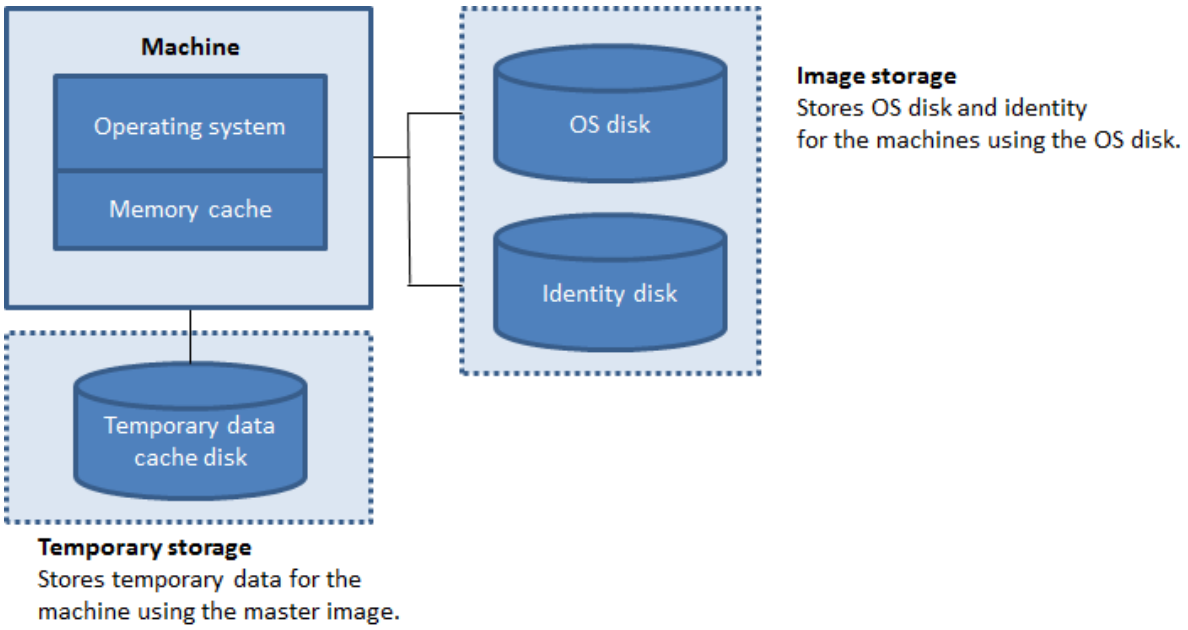
Konfigurieren eines Cache für temporäre Daten

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



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 "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.
> - 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:**
>
> - Die Konfiguration des Zurückschreibcaches mit nur einem Datenträgercache und ohne Speichercache ist veraltet. Um einen Cache für temporäre Daten zu aktivieren, wird empfohlen, sowohl die **Datenträgercachegröße (GB)** als auch die Größe des dem

> **Cache zugewiesenen Speichers (MB)** auszuwählen und einen Wert größer als 0 für den Speichercache anzugeben.
> - 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.

Netzwerkkarte

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.

Beim Hinzufügen von Organisationseinheiten können Sie Folgendes tun, wenn die Domäne nicht in der Liste angezeigt wird:

- Suchen Sie anhand einer exakten Übereinstimmung danach.
- Durchsuchen Sie alle Domänen, um die Domäne zu finden.

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.

Maschinenidentitäten

Diese Seite wird nur angezeigt, wenn Sie VMs mit MCS erstellen.

Jede Maschine im Katalog muss eine eindeutige Identität haben. Auf dieser Seite können Sie Identitäten für Maschinen im Katalog konfigurieren. Die Maschinen werden nach ihrem Provisioning mit der Identität verbunden. Sie können den Identitätstyp nicht mehr ändern, wenn Sie den Katalog erstellt haben.

Der allgemeine Workflow zum Konfigurieren von Einstellungen auf dieser Seite ist folgender:

1. Sie wählen eine Identität aus der Liste aus.
2. Sie geben an, ob neue Konten erstellt oder vorhandene Konten verwendet werden sollen, und Sie geben den Speicherort (Domäne) für diese Konten an.

Sie können eine der folgenden Optionen auswählen:

- **On-Premises-Active Directory.** Maschinen, die der Organisation gehören und mit einem Active Directory-Konto dieser Organisation angemeldet sind. Sie existieren on-premises.
- **Azure Active Directory-Hybrideinbindung**. Maschinen, die der Organisation gehören und mit einem Active Directory Domain Services-Konto dieser Organisation angemeldet sind. Sie existieren in der Cloud und on-premises. Informationen zu Anforderungen, Einschränkungen und Überlegungen finden Sie unter Azure Active Directory-Hybrideinbindung.

  > **Hinweis:**
  >
  > - Vor Verwendung der Azure Active Directory-Hybrideinbindung müssen Sie sicherstellen, dass Ihre Azure-Umgebung die Voraussetzungen erfüllt. Siehe https://docs.microsoft.com/en-us/azure/active-directory/devices/hybrid-azuread-join-managed-domains.
  > - Für diese Option muss das Masterimage die Voraussetzung für das Betriebssystem erfüllen. Informationen hierzu finden Sie in der Dokumentation von Microsoft: https://learn.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-join-hybrid

> **Wichtig:**
>
> - Wenn Sie **On-Premises-Active Directory** oder **Azure Active Directory-Hybrideinbindung** als Identitättstyp auswählen, benötigt jede Maschine im Maschinenkatalog ein Active Directory-Computerkonto.

Beim Erstellen von Konten müssen Sie berechtigt sein, Computerkonten in der Organisationseinheit zu erstellen, in der sich die Maschinen befinden. Jede Maschine im Katalog muss einen eindeutigen Namen haben. Geben Sie das Kontobenennungsschema für die Maschinen an, die Sie erstellen möchten. Weitere Informationen finden Sie unter Benennungsschema für Maschinenkonten.

> **Hinweis:**
>
> Vergewissern Sie sich, dass OU-Namen keine Schrägstriche (/) enthalten.

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. Der Inhalt der importierten Datei muss folgendes Format haben:

- [ADComputerAccount] ADcomputeraccountname.domain

Vergewissern Sie sich, dass Sie ausreichend Konten für die hinzuzufügenden Maschinen haben. Die Web Studio-Oberfläche verwaltet diese Konten. Gestatten Sie darum der Oberfläche, die Kennwörter für alle Konten zurückzusetzen, oder geben Sie das Kontokennwort an (muss für alle Konten gleich sein).

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.

Benennungsschema für Maschinenkonten

Jede Maschine in einem Katalog muss einen eindeutigen Namen haben. Sie müssen ein Benennungsschema für Maschinenkonten angeben, wenn Sie einen Katalog erstellen. Verwenden Sie Platzhalter (Rauten) für fortlaufende Zahlen oder Buchstaben, die im Namen vorkommen.

Beachten Sie bei der Angabe eines Benennungsschemas die folgenden Regeln:

- Das Benennungsschema muss mindestens einen Platzhalter enthalten. Alle Platzhalter müssen zusammen sein.
- Der Name muss einschließlich Platzhaltern aus 2 bis 15 Zeichen bestehen. Es muss mindestens ein nicht numerisches Zeichen und ein #-Zeichen (Platzhalter) enthalten.
- Der Name darf keine Leerzeichen und keines der folgenden Zeichen enthalten: `,~!@'$%^&.()} { \/*?"<>|=+[];:_".`.
- Der Name darf nicht mit einem Bindestrich (-) enden.

Lassen Sie beim Angeben des Benennungsschemas außerdem ausreichend Platz für Wachstum. Beispiel: Wenn Sie 1000 Maschinenkonten mit dem Schema “veryverylong#”erstellen, enthält der letzte Kontoname (veryverylong1000) 16 Zeichen. Das Benennungsschema führt daher zu mindestens einem Maschinennamen, der das Maximum von 15 Zeichen überschreitet.

Sie können angeben, ob es sich bei den sequentiellen Werten um Zahlen (0–9) oder Buchstaben (A–Z) handelt.

- **0-9**. Bei Auswahl dieser Option werden die angegebenen Platzhalter in fortlaufende Nummern aufgelöst.

> **Hinweis:**
>
> Wenn nur ein Platzhalter (#) vorhanden ist, beginnen Kontonamen mit 1. Bei zwei vorhandenen Platzhaltern beginnen Kontonamen mit 01. Bei drei vorhandenen Platzhaltern beginnen Kontonamen mit 001 usw.

- **A-Z**. Bei Auswahl dieser Option werden die angegebenen Platzhalter in fortlaufende Buchstaben aufgelöst.

Beispiel: Das Benennungsschema "PC-Vertrieb-##"(und Aktivieren von **0-9**) bewirkt eine Benennung der Konten als "PC-Vertrieb-01", "PC-Vertrieb-02", "PC-Vertrieb-03"usw.

Optional können Sie angeben, womit die Kontonamen beginnen sollen.

- Wenn Sie **0-9** auswählen, werden die Konten sequentiell, beginnend mit den angegebenen Zahlen benannt. Geben Sie eine oder mehrere Zahlen ein, je nachdem, wie viele Platzhalter Sie verwenden. Wenn Sie beispielsweise zwei Platzhalter verwenden, geben Sie mindestens zwei Zahlen ein.
- Wenn Sie **A-Z** auswählen, werden die Konten sequentiell, beginnend mit den angegebenen Buchstaben benannt. Geben Sie eine oder mehrere Buchstaben ein, je nachdem, wie viele Platzhalter Sie verwenden. Wenn Sie beispielsweise zwei Platzhalter verwenden, geben Sie mindestens zwei Buchstaben ein.

Domänenanmeldeinformationen

Wählen Sie **Anmeldeinformationen eingeben** und geben Sie die Anmeldeinformationen eines Administrators mit der Berechtigung zum Ausführen von Kontovorgängen in der Active Directory-Zieldomäne ein.

Überprüfen Sie mit der Option **Name überprüfen**, ob der Benutzername gültig oder eindeutig ist. Diese Option kann in folgenden Situationen von Nutzen sein:

- Der Benutzername existiert in mehreren Domänen. Sie werden aufgefordert, den gewünschten Benutzer auszuwählen.
- Sie können sich nicht an den Domänennamen erinnern. Sie können den Benutzernamen ohne Angabe des Domänennamens eingeben. Bei erfolgreicher Überprüfung wird der Domänenname automatisch eingegeben.

> **Hinweis:**
>
> Wenn Sie unter **Maschinenidentitäten** den Identitätstyp **Azure Active Directory-Hybrideinbindung** ausgewählt haben, muss den von Ihnen eingegebenen Anmeldeinformationen die Berechtigung `Write userCertificate` erteilt worden sein.

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 Web Studio angezeigt.

Wenn Sie fertig sind, klicken Sie auf **Fertigstellen**, um das Erstellen des Katalogs zu starten.
Wenn Sie fertig sind, wählen Sie **Fertigstellen**, um das Erstellen des Katalogs zu starten.

In **Maschinenkataloge** wird der neue Katalog mit einem Fortschrittsbalken angezeigt.

Gehen Sie zum Anzeigen von Details zum Erstellungsfortschritt folgendermaßen vor:

1. Zeigen Sie mit der Maus auf den Maschinenkatalog.
2. Klicken Sie in der angezeigten QuickInfo auf **Details anzeigen**.

   Ein Fortschrittsdiagramm wird angezeigt, in dem Sie Folgendes sehen können:

   - Geschichte der Schritte
   - Fortschritt und Laufzeit des aktuellen Schritts
   - Restliche Schritte

MCS-Zeitsynchronisierung

Die Zeitsynchronisierung wird durch das Masterimage und den Typ des mit Maschinenidentität verbundenen Katalogs bestimmt. Je nach Masterimage und Katalog erhalten Sie die folgende Methode zur Zeitsynchronisierung:

Masterimage	Katalog	Zugehörige Methode zur Zeitsynchronisierung
NDJ	AD oder Hybrid Azure AD	Die Standardeinstellung ist NT5DS. Mit den Registrierungseinstellungen im Masterimage können Sie verhindern, dass die Einstellungen für die Zeitsynchronisierung von MCS geändert werden.
NDJ	NDJ oder Azure AD	Entspricht der ursprünglichen Einstellung für die Zeitsynchronisierung.

Masterimage	Katalog	Zugehörige Methode zur Zeitsynchronisierung
AD oder Hybrid Azure AD	AD oder Hybrid Azure AD	Entspricht der ursprünglichen Einstellung für die Zeitsynchronisierung.
Azure AD	Azure AD	Entspricht der ursprünglichen Einstellung für die Zeitsynchronisierung.

> **Hinweis:**
>
> Die ursprüngliche Zeitsynchronisierung wird durch die folgende Registrierungseinstellung gesteuert und kann nicht geändert werden:
>
> - Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config
>
> Wert: MaxAllowedPhaseOffset, MaxNegPhaseCorrection und MaxPosPhaseCorrection
>
> - Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters
>
> Wert: Typ

Um zu verhindern, dass die Einstellung für die Zeitsynchronisierung von MCS geändert wird, legen Sie den Wert der folgenden Registrierungseinstellung im Masterimage fest:

- `Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix`
- Name: TimeSyncMethodKeep
- Typ: DWORD
- 0 (oder der Wert TimeSyncMethodKeep ist nicht konfiguriert): Die ursprüngliche Einstellung für die Zeitsynchronisierung wird nicht beibehalten.
- 1: Die ursprüngliche Einstellung für die Zeitsynchronisierung und die Standardparameterwerte werden beibehalten.

Richtlinien zum Festlegen benutzerdefinierter Eigenschaften

Benutzerdefinierte Eigenschaften müssen bei `New-ProvScheme` und `Set-ProvScheme` in GCP- und Azure-Umgebungen korrekt festgelegt sein. Wenn Sie nicht vorhandene benutzerdefinierte Eigenschaften angeben, wird die folgende Fehlermeldung angezeigt, und die Befehle werden nicht ausgeführt.

- Azure: `Invalid property found: <invalid property>. Ensure that the CustomProperties parameter supports the property.`
- GCP: `Invalid property found: <invalid property>. Ensure that the value supplied for the property is supported in the Hypervisor.`

Problembehandlung

> **Wichtig:**
>
> Wenn Sie den Maschinenkatalog mit Web Studio erstellt haben, können Sie den PowerShell-Befehl `Get-ProvTask` nicht mehr zum Abrufen der Aufgaben für die Erstellung des Maschinenkatalogs verwenden. Der Grund dafür ist, dass die Aufgaben nach der Erstellung des Maschinenkatalogs von Web Studio gelöscht werden, unabhängig davon, ob der Katalog erstellt wurde oder nicht.

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`.

Probleme bei der Imagevorbereitung

Da MCS viele Maschinen aus einem Image erstellt, werden diverse Schritte ausgeführt, um sicherzustellen, dass alle Maschinen einmalig und korrekt lizenziert sind. Die Imagevorbereitung ist

Teil der Katalogerstellung. Die Vorbereitung gewährleistet, dass alle bereitgestellten Maschinen eine eindeutige IP-Adresse haben und sich dem KMS-Server korrekt als eindeutige Instanz ankündigen. In MCS erfolgt die Imagevorbereitung nach Auswahl des Masterimage-Snapshots. Es wird eine Kopie erstellt, um die Isolierung des Katalogs von der ausgewählten Maschine zu ermöglichen. Basierend auf der ursprünglichen VM wird eine *Vorbereitungs*-VM mit getrennter Netzwerkverbindung erstellt. Das Trennen der Netzwerkverbindung verhindert Konflikte mit anderen Maschinen und stellt sicher, dass die vorbereitete VM nur an den neu kopierten Datenträger angefügt ist.

Ein kleiner *Anweisungsdatenträger* mit den zum Ausführen der Imagevorbereitung erforderlichen Schritten wird an die vorbereitete VM angefügt. Die vorbereitete VM wird gestartet und die Imagevorbereitung beginnt. Die Imagevorbereitung umfasst die folgenden Prozesse:

- Aktivieren von DHCP. Durch das Aktivieren von DHCP wird sichergestellt, dass bereitgestellte Maschinen keine IP-Adresskonflikte verursachen. DHCP wird für alle Netzwerkkarten aktiviert.
- Zurücksetzen von Microsoft Windows KMS. Das Zurücksetzen von KMS stellt sicher, dass Microsoft Windows korrekt lizenziert wird. Das zurückgesetzte Betriebssystem wird aufgerufen, sodass es korrekt als neue Instanz an den KMS-Lizenzserver gemeldet wird.
- Zurücksetzen von Microsoft Office KMS (wenn Microsoft Office installiert ist). Das Zurücksetzen von Microsoft Office stellt sicher, dass jegliche Microsoft Office-Version (ab 2010) korrekt beim entsprechenden KMS-Server registriert wird. Beim Aufrufen des Zurücksetzens von Microsoft Office wird dieses als neue Instanz an den KMS-Lizenzserver gemeldet.

> **Tipp:**
>
> Nach Abschluss der Imagevorbereitung wird der Anweisungsdatenträger vom Hypervisor bezogen. Der Hypervisor enthält die aus der Imagevorbereitung gewonnenen Informationen.

Es gibt verschiedene Gründe, warum die Imagevorbereitung fehlschlagen kann. Eine Fehlermeldung ähnlich der folgenden wird angezeigt: Office-Rearming bei Imagevorbereitung fehlgeschlagen.

Diese Fehler werden in den folgenden Abschnitten behandelt.

Aktivieren von DHCP Diese Fehler werden durch Netzwerkkarten verursacht, die keine statischen IP-Adressen unterstützen. Beispiel: ältere Versionen von Dell SonicWall-Netzwerkkarten. Der Vorgang schlägt fehl, da SonicWall-Karten Firewall-Netzwerkkarten sind, deren Einstellung auf DHCP keinen Sinn ergibt, da nur DHCP unterstützt wird. Dies wurde spätere Versionen von Citrix Virtual Apps and Desktops behoben. Wird der Fehler bei anderen Arten von Netzwerkkarten beobachtet, muss das an Citrix über die Foren oder den Supportkontakt gemeldet werden.

> **Hinweis:**
>
> Die PowerShell-Einstellung in den folgenden Beispielen wird auf die Citrix Virtual Apps and Desktops-Site angewendet und wirkt sich auf alle neuen Kataloge sowie Imageupdates an

> vorhandenen Katalogen aus.

Wenn das Problem bei anderen Netzwerkkarten auftritt, können Sie es durch Ausführung eines PowerShell-Befehls auf dem Delivery Controller lösen:

```
Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps
 -Value EnableDHCP
```

Zurücksetzen von Microsoft Office Beim Zurücksetzen von KMS können im Stadium der Microsoft Office-Zurücksetzung diverse Fehler auftreten. Dabei handelt es sich hauptsächlich um folgende Fehler:

- Einige Microsoft Office-Runtimes (z. B. **Access Runtime**) können das Zurücksetzen von Office aufrufen und so zu dessen Fehlschlagen führen.
- Es ist keine KMS-Version von Microsoft Office installiert.
- Die Anzahl Zurücksetzungen wurde überschritten.

Handelt es sich bei einem Fehler um einen falschen Alarm, können Sie ihn beheben, indem Sie den folgenden PowerShell-Befehl auf dem Delivery Controller ausführen:

```
Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps
 -Value OfficeRearm
```

Microsoft Windows Rearm Beim Zurücksetzen von Microsoft Windows können diverse KMS-Fehler auftreten. Dabei handelt es sich hauptsächlich um folgende Fehler:

- Die installierte Version von Windows wird nicht mit KMS aktiviert. Beispielsweise wird ein Mehrfachaktivierungsschlüssel (MAK) verwendet.
- Die Anzahl Zurücksetzungen wurde überschritten.

Wenn die Microsoft Windows-Version korrekt lizenziert ist, können Sie das Zurücksetzen des Betriebssystems überspringen, indem Sie folgenden PowerShell-Befehl auf dem Delivery Controller ausführen:

```
Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps
 -Value OsRearm
```

Kompletter Fehlschlag Da die Imagevorbereitungsengine nicht standardmäßig mit dem Netzwerk verbunden ist, kann in der Imagevorbereitungsphase manchmal nur ein kompletter Fehlschlag gemeldet werden. Ein Beispiel für diesen Fehlertyp ist: Die Vorbereitung des VM-Masterimages ist fehlgeschlagen. Stellen Sie sicher, dass das ausgewählte Image ein unterstütztes Betriebssystem verwendet (beispielsweise Windows 7) und dass die richtige VDA-Version (7.0 oder höher) installiert ist.

Die Ursachen eines kompletten Fehlschlags sind in der Hauptsache folgende:

Virtual Delivery Agent (VDA) ist nicht oder in der Version 5.x installiert Wenn der VDA 7.x nicht auf dem Masterimage installiert ist, tritt bei der Imagevorbereitung nach 20 Minuten ein Timeout ein und es wird der obige Fehler gemeldet. Dies liegt daran, dass auf dem Masterimage keine Software installiert ist, die die Imagevorbereitung ausführen und einen Erfolg oder Misserfolg melden kann. Um den Fehler zu beheben, vergewissern Sie sich, dass der VDA (Mindestversion 7) auf dem Snapshot installiert ist, der als Masterimage ausgewählt wurde.

Richtlinie `DISKPART SAN` Die gesamte Imagevorbereitung kann aufgrund der Einstellung der Richtlinie `DISKPART SAN` auf dem Masterimage fehlschlagen. Ist sie nicht so eingestellt, dass der Anweisungsdatenträger zur Imagevorbereitung online geschaltet wird, wird die Maschine nach 20 Minuten heruntergefahren und die Imagevorbereitung meldet einen Fehler. Um dies auf dem Masterimage zu überprüfen, führen Sie folgenden Befehl aus:

```
C:>; Diskpart.exe
DISKPART>; San
<!--NeedCopy-->
```

Dieser Befehl gibt die aktuelle Richtlinie zurück. Wenn die Richtlinie nicht auf *Online All* festgelegt ist, ändern Sie die Einstellung, indem Sie den folgenden Befehl ausführen:

```
DISKPART>; San policy=OnlineAll
```

Fahren Sie das Masterimage herunter, erstellen Sie einen Snapshot der Maschine und verwenden Sie diesen dann als Basisimage für MCS.

Bildvorbereitung schlägt aus einem anderen Grund fehl Wenn die Imagevorbereitung aus unbekanntem Grund fehlschlägt , können Sie die Imagevorbereitung beim Erstellen des MCS-Katalogs umgehen. Die Umgehung kann jedoch zu Probleme mit der KMS-Lizenzierung und dem Netzwerk (DHCP) in der Site führen. Verwenden Sie den folgenden PowerShell-Befehl:

```
Set-ProvServiceConfigurationData -Name
    ImageManagementPrep_DoImagePreparation -Value $false
<!--NeedCopy-->
```

Sammeln Sie nach Möglichkeit Protokolle für das Citrix Support-Team. Melden Sie Probleme über die Foren oder über Ihren Supportkontakt an Citrix. Sammeln von Protokollen:

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. Starten Sie PowerShell auf dem Delivery Controller mit den geladenen Snap-Ins von Citrix PowerShell und führen Sie `Set-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown -Value $True` aus:

3. Erstellen Sie einen Katalog basierend auf diesem Snapshot.
4. Wenn die Vorbereitungs-VM auf dem Hypervisor erstellt wurde, melden Sie sich an und extrahieren Sie aus dem Stammverzeichnis von C:\:

```
Image-prep.log
PvsVmAgentLog.txt
<!--NeedCopy-->
```

Fahren Sie die Maschine herunter. Nun wird der Fehlschlag gemeldet.

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

Informationen zum Erstellen bestimmter Cloudservices-Kataloge finden Sie unter:

- AWS-Katalog erstellen
- XenServer-Katalog erstellen
- Google Cloud Platform-Katalog erstellen
- Microsoft Azure-Katalog erstellen
- Microsoft System Center Virtual Machine Manager-Katalog erstellen
- Nutanix-Katalog erstellen
- VMware-Katalog erstellen

Wenn Sie den ersten Katalog erstellen, werden Sie von Web Studio zum Erstellen einer Bereitstellungsgruppe geleitet.

Informationen zum gesamten Konfigurationsprozess finden Sie unter Installation und Konfiguration.

Sie können einen Citrix Provisioning-Katalog mithilfe der Benutzeroberfläche “Vollständige Konfiguration”und PowerShell erstellen.
Diese Implementierung bietet Ihnen die folgenden Vorteile:

- Eine einzige, einheitliche Konsole zur Verwaltung von MCS- und Citrix Provisioning-Katalogen.
- Neue Features für Citrix Provisioning-Kataloge, wie eine Identitätsverwaltungslösung, On-Demand-Provisioning und so weiter.

Derzeit ist dieses Feature nur für Azure- und VMware-Workloads verfügbar. In VMware-Umgebungen können Sie die Kataloge derzeit jedoch nur mit PowerShell-Befehlen erstellen. Weitere Informationen finden Sie unter Citrix Provisioning-Kataloge in Citrix Studio erstellen.

Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Kataloge mit verschiedenen Einbindungstypen erstellen
- Maschinenkataloge verwalten

AWS-Katalog erstellen

June 27, 2024

Unter Maschinenkataloge erstellen werden die Assistenten zum Erstellen eines Maschinenkatalogs beschrieben. Die folgenden Informationen beziehen sich speziell auf AWS-Virtualisierungsumgebungen.

> **Hinweis:**
>
> Bevor Sie einen AWS-Katalog erstellen, müssen Sie eine Verbindung zu AWS hergestellt haben. Siehe Verbindung zu AWS.

Netzwerkeinstellung während der Imagevorbereitung

Während der Imagevorbereitung wird eine virtuelle Vorbereitungsmaschine (Vorbereitungs-VM) basierend auf der ursprünglichen VM erstellt. Diese Vorbereitungs-VM ist vom Netzwerk getrennt. Zum Trennen des Netzwerks von der Vorbereitungs-VM wird eine Netzwerksicherheitsgruppe erstellt, um den gesamten eingehenden und ausgehenden Datenverkehr zu blockieren. Diese Netzwerksicherheitsgruppe bleibt bestehen und wird wiederverwendet. Der Name der Netzwerksicherheitsgruppe lautet `Citrix.XenDesktop.IsolationGroup-GUID`, wobei die GUID nach dem Zufallsprinzip generiert wird.

AWS-Tenancy konfigurieren

AWS bietet die folgenden Tenancy-Optionen:

- Bei einer freigegebenen Tenancy (Standardtyp) können sich die Amazon EC2-Instanzen mehrerer Kunden auf derselben physischen Hardware befinden.
- Bei der dedizierten Tenancy ist die Hardware zur Ausführung Ihrer EC2-Instanzen und anderer, vom Kunden entwickelter Instanzen nur einem Kunden vorbehalten. Sie wird nicht von anderen Kunden verwendet.

Sie können mit MCS dedizierte AWS-Hosts über PowerShell bereitstellen.

Dedizierte AWS-Hostmandanten mit PowerShell konfigurieren

Sie können einen Katalog mit Maschinen erstellen, deren Hostmandanten 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.

Maschineneigenschaften von AMIs erfassen

Wenn Sie einen Katalog für die Bereitstellung von Maschinen über Maschinenerstellungsdienste (MCS) in AWS erstellen, wählen Sie ein AMI (Amazon Machine Image) als Master-/Gold-Image des Katalogs. Von diesem AMI verwendet MCS einen Snapshot des Datenträgers. In früheren Versionen mussten Rollen oder Tags auf Maschinen individuell über die die AWS-Konsole festgelegt werden. Diese Funktion ist standardmäßig aktiviert.

> **Tipp:**
>
> Zur Verwendung der Erfassung der AWS-Instanzeigenschaft benötigen Sie eine VM, die dem AMI zugeordnet ist.

Zur Verbesserung dieses Prozesses **liest MCS** Eigenschaften aus der Instanz, aus der das AMI stammt, und wendet die IAM-Rolle und -Tags (Identity and Access Management) der Maschine auf die für einen bestimmten Katalog bereitgestellten Maschinen an. Wenn Sie dieses optionale Feature verwenden, findet der Katalogerstellungsprozess die ausgewählte AMI-Quellinstanz und liest einen begrenzten Satz von Eigenschaften. Diese Eigenschaften werden dann in einer AWS-Startvorlage gespeichert, mit der Maschinen für den Katalog bereitgestellt werden. Alle Maschinen im Katalog erben die erfassten Instanzeigenschaften.

Erfasste Eigenschaften sind:

- IAM-Rollen —auf bereitgestellte Instanzen angewendet.
- Tags –auf bereitgestellte Instanzen, deren Datenträger und Netzwerkkarten angewendet. Die Tags werden auf flüchtige Citrix Ressourcen angewendet: S3-Bucket und -Objekte sowie AMIs, Snapshots und Startvorlagen.

> **Tipp:**
>
> Das Tagging flüchtiger Citrix Ressourcen ist optional und kann über die benutzerdefinierte Eigenschaft `AwsOperationalResourcesTagging` konfiguriert werden.

AWS-Instanzeigenschaft erfassen

Sie können dieses Feature über die Spezifizierung der benutzerdefinierten Eigenschaft `AwsCaptureInstanceP` beim Erstellen eines Provisioningschemas für eine AWS-Hostingverbindung nutzen:

```
New-ProvScheme -CustomProperties "AwsCaptureInstanceProperties,true"
...<standard provscheme parameters
```

Weitere Informationen finden Sie in der Citrix Dokumentation für Entwickler.

> **Hinweis:**
>
> `AwsCaptureInstanceProperties` ist veraltet. Wir empfehlen, stattdessen Maschinenprofile zu verwenden, um Maschineneigenschaften für virtuelle Maschinen anzugeben.

Maschineneigenschaften aus Maschinenprofilen erfassen

Wenn Sie einen Katalog für die Bereitstellung von AWS-Maschinen mithilfe von MCS erstellen, können Sie ein Maschinenprofil verwenden, um bestimmte Einstellungen für Maschineneigenschaften vorzugeben.

Führen Sie hierzu folgende Schritte aus:

1. Speichern Sie die Maschinenprofile in derselben Verfügbarkeitszone wie die Ressourcen, in denen Sie diesen Katalog erstellen.
2. Wählen Sie auf der Seite **Maschinenvorlage** des Assistenten zur Katalogerstellung die Option **Maschinenprofil verwenden** aus. Maschinenprofile, die sich in derselben verfügbaren Zone wie die ausgewählten Ressourcen befinden, werden angezeigt.
3. Wählen Sie nach Bedarf ein Maschinenprofil aus.

> **Hinweis:**
>
> Sie können entweder ein Maschinenprofil oder ein AMI verwenden, um Maschineneigenschaften zu erfassen. Wenn Sie in Web Studio die Option **Ein Maschinenprofil verwenden** auswählen, wird die Option **Maschinenvorlageneigenschaften auf virtuelle Maschinen anwenden** automatisch ausgeblendet.

AWS-Betriebsressource taggen

Wenn Sie einen Katalog zum Bereitstellen von Maschinen in AWS über die Maschinenerstellungsdienste erstellen, können Sie festlegen, ob Sie auf diese Maschinen die IAM-Rolle und Tag-Eigenschaften anwenden. Außerdem können Sie festlegen, ob Sie Maschinen-Tags auf Betriebsressourcen anwenden.

Ein Amazon Machine Image (AMI) ist eine virtuelle Appliance, die zum Erstellen einer virtuellen Maschine in der Amazon Cloud-Umgebung EC2 verwendet wird. Sie verwenden ein AMI, um Dienste bereitzustellen, die die EC2-Umgebung verwenden. Wenn Sie einen Katalog für die Bereitstellung von Maschinen über MCS für AWS erstellen, wählen Sie ein **AMI** als Gold-Image des Katalogs.

> **Wichtig:**
>
> Das Erstellen von Katalogen durch Erfassen einer Instanzeigenschaft und einer Startvorlage ist für die Verwendung des Taggings von Betriebsressourcen erforderlich.

Um einen AWS-Katalog zu erstellen, müssen Sie zunächst ein AMI für die Instanz erstellen, die als Gold-Image fungieren soll. MCS liest die Tags dieser Instanz und fügt sie in die Startvorlage ein. Die Startvorlagen-Tags werden dann auf alle in der AWS-Umgebung erstellten Citrix Ressourcen angewendet:

- Virtuelle Maschinen
- VM-Datenträger
- VM-Netzwerkschnittstellen
- S3-Buckets
- S3-Objekte
- Startvorlagen
- AMIs

Betriebsressource taggen

Tagging von Ressourcen mit PowerShell:

1. Öffnen Sie ein PowerShell-Fenster vom DDC-Host aus.

2. Führen Sie den Befehl `asnp citrix` aus, um Citrix spezifische PowerShell-Module zu laden.

Verwenden Sie die neue benutzerdefinierte Eigenschaft `AwsOperationalResourcesTagging`, um eine Ressource für eine bereitgestellte VM zu taggen. Eigenschaftssyntax:

```
New-ProvScheme -CustomProperties "AwsCaptureInstanceProperties,true;
AwsOperationalResourcesTagging,true"...<standard provscheme parameters
>
```

So geht es weiter

- Wenn Sie den ersten Katalog erstellen, werden Sie von Web Studio zum Erstellen einer Bereitstellungsgruppe geleitet.
- Informationen zum gesamten Konfigurationsprozess finden Sie unter Installation und Konfiguration
- Informationen zur Verwaltung von Katalogen finden Sie unter Maschinenkataloge verwalten und AWS-Katalog verwalten

Tags auf VMs kopieren

Sie können im Maschinenprofil angegebene Tags auf Netzwerkkarten und Datenträgern (Identitätsdatenträger, Zurückschreibcachedatenträger und OS-Datenträger) auf neu erstellte VMs in einem MCS-Maschinenkatalog kopieren. Sie können diese Tags in jeder Maschinenprofilquelle (AWS VM-Instanz oder AWS-Startvorlagenversion) angeben. Dieses Feature gilt für persistente und nicht persistente Maschinenkataloge und VMs.

> **Hinweis:**
>
> - Auf der AWS EC2-Konsole können Sie die Werte für **Tag Network Interfaces** unter den **Launch Template Version Resource Tags** nicht sehen. Sie können jedoch den PowerShell-Befehl `aws ec2 describe-launch-template-versions --launch-template-id lt-0bb652503d45dcbcd --versions 12` ausführen, um die Tagspezifikationen anzuzeigen.
> - Wenn eine Maschinenprofilquelle (VM- oder Startvorlagenversion) zwei Netzwerkschnittstellen (eni-1 und eni-2) hat, eni-1 das Tag t1 und eni-2 das Tag t2 hat, dann erhält die VM die Tags der beiden Netzwerkschnittstellen.

Katalog mithilfe eines Maschinenprofils erstellen

Wenn Sie einen Katalog für das Provisioning von Maschinen mit MCS in AWS erstellen, können Sie jetzt ein Maschinenprofil verwenden, das die Hardwareeigenschaften einer EC2-Instanz (VM) oder

einer Startvorlagenversion erfasst und auf die bereitgestellten VMs anwendet. Erfasst werden können beispielsweise EBS-Volumeeigenschaften, Instanztyp, EBS-Optimierung und weitere unterstützte AWS-Konfigurationen. Beim Bearbeiten eines Katalogs kann das Maschinenprofil der Maschinen geändert werden, indem eine andere VM oder Startvorlage bereitgestellt wird.

> **Hinweis:**
>
> EBS-Volumeeigenschaften werden nur aus einem Maschinenprofil abgeleitet.

Wichtige Überlegungen

Wichtige Überlegungen bei der Erstellung eines MCS-Maschinenkatalogs:

- Wenn Sie die Parameter für die Maschinenhardware-Eigenschaft in den Befehlen `New-ProvScheme` und `Set-ProvScheme` hinzufügen, überschreiben die in den Parametern angegebenen Werte die Werte im Maschinenprofil.
- Wenn Sie `AwsCaptureInstanceProperties` auf **`true`** festlegen, die Eigenschaft `MachineProfile` jedoch nicht festlegen, werden nur IAM-Rollen und -Tags erfasst.
- Sie können `AwsCaptureInstanceProperties` und `MachineProfile` nicht gleichzeitig festlegen.

  > **Hinweis:
  >
  > `AwsCaptureInstanceProperties` ist veraltet.

- Sie müssen die Werte der folgenden Eigenschaften explizit angeben:
  - TenancyType
  - Sicherheitsgruppe
  - NIC oder virtuelles Netzwerk
- Sie können `AwsOperationalResourcesTagging` nur aktivieren, wenn Sie `AwsCaptureInstanceP` aktivieren oder ein Maschinenprofil angeben.

Wichtige Überlegungen nach der Erstellung eines MCS-Maschinenkatalogs:

- Nur die neuen virtuellen Maschinen, die dem Katalog hinzugefügt wurden, sind von der Änderung betroffen.
- Ein Maschinenkatalog, der auf einem Maschinenprofil basiert, kann nicht in einen Maschinenkatalog geändert werden, der nicht auf einem Maschinenprofil basiert.

Maschinenkatalog mit einem Maschinenprofil erstellen

So erstellen Sie einen Maschinenkatalog mit einem Maschinenprofil:

1. Öffnen Sie ein **PowerShell**-Fenster.
2. Führen Sie `asnp citrix*` aus, um die Citrix-spezifischen PowerShell-Module zu laden.
3. Erstellen Sie einen Identitätspool, falls noch nicht vorhanden. Beispiel:

```
1 New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms## -
     Domain abcdf -NamingSchemeType Numeric
2 <!--NeedCopy-->
```

4. Führen Sie den Befehl New-ProvScheme aus. Beispiel:

```
1 New-ProvScheme -ProvisioningSchemeName demet-test-1
2 -HostingUnitUid aa633238-9xxd-4cf6-80e8-232a758a1xx1
3 -IdentityPoolUid 34d5b088-e312-416f-907d-16573xxxxxc4
4 -CleanOnBoot
5 -MasterImageVM 'XDHyp:\HostingUnits\cvad-test-scalestress\citrix-
     demet-ami.0 (ami-0ca813xxxxxx061ef).template'
6 -MachineProfile 'XdHyp:\HostingUnits\cvad-test-scalestress\us-east
     -1a.availabilityzone\machine-profile-instance i (i-0xxxxxxxx).
     vm'
7 <!--NeedCopy-->
```

5. Schließen Sie das Erstellen des Katalogs ab. Weitere Informationen finden Sie unter Citrix PowerShell SDK.

Aktualisieren des Maschinenprofils in einem Katalog, der mit einem Maschinenprofil bereitgestellt wurde:

1. Führen Sie den Befehl `Set-ProvScheme` aus. Beispiel:

```
1 Set-ProvScheme `
2 -ProvisioningSchemeUid "<ID" `
3 -MachineProfile "XDHyp:\HostingUnits\abc\us-east-1a.
     availabilityzone\citrix-cvad-machineprofile-instance (i-0
     xxxxxxxx).vm"
4 <!--NeedCopy-->
```

Katalog mit Startvorlagenversion erstellen

Sie können einen MCS-Maschinenkatalog mit einer Startvorlagenversion als Maschinenprofileingabe erstellen. Sie können auch die Eingabe eines Maschinenprofilkatalogs von einer VM auf eine Startvorlagenversion und von einer Startvorlagenversion auf eine VM aktualisieren.

Auf der AWS EC2-Konsole können Sie die Instanzkonfigurationsangaben einer Startvorlage zusammen mit der Versionsnummer angeben. Wenn Sie beim Erstellen oder Aktualisieren eines Maschinenkatalogs die Startvorlagenversion als Maschinenprofileingabe angeben, werden die Eigenschaften aus dieser Startvorlagenversion auf die bereitgestellten VDA-VMs kopiert.

Die folgenden Eigenschaften können mithilfe der Maschinenprofileingabe oder explizit als Parameter in `New-ProvScheme`- oder `Set-ProvScheme`-Befehlen bereitgestellt werden. Wenn sie in `New-ProvScheme`- oder `Set-ProvScheme`-Befehlen bereitgestellt werden, haben sie Vorrang vor den Eigenschaftswerten im Maschinenprofil.

- Dienstangebot
- Netzwerke
- Sicherheitsgruppen
- Mandantenmodell

> **Hinweis:**
>
> Wenn das Dienstangebot nicht in der Startvorlage für das Maschinenprofil oder als Parameter im Befehl `New-ProvScheme` angegeben ist, wird eine Fehlermeldung angezeigt.

Erstellen eines Katalog mit der Startvorlagenversion als Maschinenprofileingabe:

1. Öffnen Sie ein **PowerShell**-Fenster.
2. Führen Sie `asnp citrix*` aus, um die Citrix-spezifischen PowerShell-Module zu laden.
3. Rufen Sie die Liste der Startvorlagenversionen einer Startvorlage auf. Beispiel:

```
XDHyp:\HostingUnits\test\test-mp-sard (lt-01xxxxx).launchtemplate>
    ls | Select FullPath
<!--NeedCopy-->
```

4. Erstellen Sie einen Identitätspool (falls nicht vorhanden). Beispiel:

```
New-AcctIdentityPool `
-IdentityPoolName "abc11" `
-NamingScheme "abc1-##" `
-NamingSchemeType Numeric `
-Domain "citrix-xxxxxx.local" `
-ZoneUid "xxxxxxxx" `
<!--NeedCopy-->
```

5. Erstellen Sie ein Provisioningschema mit einer Startvorlagenversion als Maschinenprofileingabe. Beispiel:

```
New-ProvScheme `
-ProvisioningSchemeName "MPLT1" `
-HostingUnitUid "c7f71f6a-3f45-4xxx-xxxx-xxxxxxxxxx" `
-IdentityPoolUid "bf3a6ba2-1f80-4xxx-xxxx-xxxxxxxxx" `
-MasterImageVM "XDHyp:\HostingUnits\xxxd-ue1a\apollo-non-
   persistent-vda-win2022 (ami-0axxxxxxxxxx).template" `
-CleanOnBoot `
-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
   (lt-01xxxxx).launchtemplate\lt-01xxxxx (1).
   launchtemplateversion"
<!--NeedCopy-->
```


Sie können Parameter wie Dienstangebot, Sicherheitsgruppen, Mandantenmodell und Netzwerke auch überschreiben. Beispiel:

```
New-ProvScheme `
-ProvisioningSchemeName "MPLT1" `
-HostingUnitUid " c7f71f6a-3f45-4xxx-xxxx-xxxxxxxxxx" `
-IdentityPoolUid " bf3a6ba2-1f80-4xxx-xxxx-xxxxxxxxx" `
-MasterImageVM "XDHyp:\HostingUnits\xxxd-ue1a\apollo-non-
   persistent-vda-win2022 (ami-0axxxxxxxxxx).template" `
-CleanOnBoot `
-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
   (lt-01xxxx).launchtemplate\lt-01xxxx (1).launchtemplateversion"
    `
-ServiceOffering "XDHyp:\HostingUnits\xxxd-ue1a\T3 Large Instance.
   serviceoffering"
<!--NeedCopy-->
```

6. Registrieren Sie das Provisioningsschema als Brokerkatalog. Beispiel:

```
New-BrokerCatalog -Name "MPLT1" `
-AllocationType Random `
-Description "Machine profile catalog" `
-ProvisioningSchemeId fe7df345-244e-4xxxx-xxxxxxxxx `
-ProvisioningType Mcs `
-SessionSupport MultiSession `
-PersistUserChanges Discard
<!--NeedCopy-->
```

7. Schließen Sie das Erstellen des Katalogs ab. Weitere Informationen finden Sie unter Citrix PowerShell SDK.

Sie können auch die Eingabe eines Maschinenprofilkatalogs von einer VM auf eine Startvorlagenversion und von einer Startvorlagenversion auf eine VM aktualisieren. Beispiel:

- Aktualisieren der Eingabe eines Maschinenprofilkatalogs von einer VM auf eine Startvorlagenversion:

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest"
    `
-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
    (lt-0bxxxxxxxxxxxx).launchtemplate\lt-0bxxxxxxxxxxx (1).
   launchtemplateversion"
<!--NeedCopy-->
```

- Aktualisieren der Eingabe eines Maschinenprofilkatalogs von einer Startvorlagenversion auf eine VM:

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest"
    `
-MachineProfile "XDHyp:\HostingUnits\sard-ue1a\us-east-1a.
   availabilityzone\apollo-non-persistent-vda-win2022-2 (i-08
   xxxxxxxxx).vm"
```



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

VM-Instanzen filtern

Eine AWS EC2-Instanz, die Sie als Maschinenprofil-VM verwenden, muss kompatibel sein, damit der Maschinenkatalog erstellt werden kann und ordnungsgemäß funktioniert. Zum Auflisten der AWS EC2-Instanzen, die als Eingabe-VMs für Maschinenprofile verwendet werden können, können Sie den Befehl `Get-HypInventoryItem` verwenden. Mit dem Befehl kann der Bestand der auf einer Hostingeinheit verfügbaren virtuellen Maschinen paginiert und gefiltert werden.

Paginierung:

Get-HypInventoryItem unterstützt zwei Paginierungsmodi:

- Der Seitenmodus verwendet die Parameter `-MaxRecords` und `-Skip`, um Gruppen von Elementen zurückzugeben:
  - `-MaxRecords`: Der Standardwert ist **1**. Dies steuert, wie viele Elemente zurückgegeben werden sollen.
  - `-Skip`: Der Standardwert ist **0**. Dies steuert, wie viele Elemente ab dem absoluten Anfang (oder absoluten Ende) der Liste im Hypervisor übersprungen werden sollen.
- Der Scrollmodus verwendet die Parameter `-MaxRecords`, `-ForwardDirection` und `-ContinuationToken`, um das Scrollen der Datensätze zu ermöglichen:
  - `-ForwardDirection`: Der Standardwert ist **True**. Dies wird zusammen mit `-MaxRecords` verwendet, um den nächsten Satz oder den vorherigen Satz übereinstimmender Datensätze zurückzugeben.
  - `-ContinuationToken`: Gibt die Elemente unmittelbar danach zurück (oder davor, falls `ForwardDirection` = **false**), jedoch ohne das in `ContinuationToken` angegebenen Element.

Beispiele der Paginierung:

- Um einen einzelnen Datensatz mit der Maschinenvorlage mit dem niedrigsten Namen zurückzugeben. Das Feld `AdditionalData` enthält `TotalItemsCount` und `TotalFilteredItemsCount`:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template
<!--NeedCopy-->
```

- Ausgabe von 10 Datensätzen der Maschinenvorlage mit dem niedrigsten Namen:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -MaxRecords 10 | select Name
```



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

- Um ein Array von Datensätzen zurückzugeben, die mit dem höchsten Namen enden:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -ForwardDirection $False -MaxRecords 10
     | select Name
<!--NeedCopy-->
```

- Um ein Array von Datensätzen zurückzugeben, beginnend mit der Maschinenvorlage, die dem `ContinuationToken` zugeordnet ist:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -ContinuationToken "ami-07xxxxxxxxx" -
    MaxRecords 10
<!--NeedCopy-->
```

Filtern:

Die folgenden zusätzlichen optionalen Parameter werden für die Filterung unterstützt. Sie können diese Parameter mit den Paginierungsoptionen kombinieren.

- `-ContainsName "my_name"`: Wenn die angegebene Zeichenfolge einem Teil eines AMI-Namens entspricht, wird das AMI in das `Get`-Ergebnis aufgenommen. Beispiel:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -MaxRecords 100 -ContainName ‘ apollo ’
     | select Name
<!--NeedCopy-->
```

- `-Tags '{ "Key0": "Value0", "Key1": "Value1", "Key2": "Value2" } '` : Wenn ein AMI mindestens eines dieser Tags hat, wird es in das `Get` -Ergebnis aufgenommen. Beispiel:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -MaxRecords 100 -Tags '{
"opex owner": "Not tagged" }
' | select Name
<!--NeedCopy-->
```

> **Hinweis:**
>
> Zwei Tag-Werte werden unterstützt. Der Wert **Not Tagged** entspricht Elementen, die das angegebene Tag nicht in ihrer Tag-Liste haben. Der Wert **All Values** entspricht Elementen, die das Tag haben, unabhängig von dessen Wert. Andernfalls gilt es nur als Übereinstimmung, wenn das Element das Tag hat und der Wert der Angabe im Filter entspricht.

- `-Id "ami-0a2d913927e0352f3"`: Wenn das AMI mit der angegebenen ID übereinstimmt, wird es in das `Get`-Ergebnis aufgenommen. Beispiel:


```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -Id ami-xxxxxxxxxxxx
<!--NeedCopy-->
```

Filtern nach dem Parameter “AdditionalData”:

Der Filterparameter `AdditionalData` listet Vorlagen oder VMs auf der Grundlage ihrer Funktionen, ihres Dienstangebots oder einer beliebigen Eigenschaft in “AdditionalData”auf. Beispiel:

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -
    LiteralPath "XDHyp:\HostingUnits\aws" -MaxRecords 200).
    AdditionalData
<!--NeedCopy-->
```

Sie können auch einen Parameter `-Warn` hinzufügen, um die nicht kompatiblen VMs anzugeben. Die VMs sind in einem `AdditionalData`-Feld mit dem Namen **Warning** enthalten. Beispiel:

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -
    LiteralPath "XDHyp:\HostingUnits\aws" -MaxRecords 200 -Template "ami
    -015xxxxxxxxx" -Warn $true).AdditionalData
<!--NeedCopy-->
```

Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Verbindung zu AWS
- Maschinenkataloge erstellen

XenServer-Katalog erstellen

June 27, 2024

Unter Maschinenkataloge erstellen werden die Assistenten zum Erstellen eines Maschinenkatalogs beschrieben. Die folgenden Informationen beziehen sich speziell auf XenServer-Virtualisierungsumgebungen.

> **Hinweis:**
>
> Bevor Sie einen XenServer-Katalog erstellen, müssen Sie eine Verbindung zu XenServer hergestellt haben. Weitere Informationen finden Sie unter Verbindung zu XenServer.

Erstellen eines Maschinenkatalogs über eine XenServer-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.

Einschränkungen

- Wenn eine Citrix Virtual Apps and Desktops-Bereitstellung mit auf Citrix Hypervisor 8.2 gehosteten VMs mehrere GFS2-Speicherrepositorys in einem einzigen MCS-Katalog verwendet, können die VMs im Katalog während der Bereitstellung nicht auf die VDIs zugreifen. Die Fehlermeldung “VDI is currently in use”wird angezeigt.
- XenServer unterstützt keine mit MCS erstellten vollständigen Klon-VMs mit GFS2-SRs.

Weitere Informationen finden Sie unter Einschränkungen.

Maschinenkatalog mit einem Maschinenprofil erstellen

Wenn Sie einen Katalog für das Provisioning von Maschinen mit MCS erstellen, können Sie ein Maschinenprofil verwenden, das die Hardwareeigenschaften einer virtuellen Maschine erfasst und auf neu bereitgestellte VMs im Katalog anwendet. Wenn der Parameter `MachineProfile` nicht verwendet wird, werden die Hardwareeigenschaften von der Masterimage-VM oder dem Snapshot erfasst.

> **Hinweis:**
>
> Derzeit können Sie nur eine VM als Maschinenprofileingabe verwenden.

Sie können die folgenden Parameter explizit konfigurieren, um die Werte der Parameter in der Maschinenprofileingabe außer Kraft zu setzen:

- `VMCpuCount`
- `VMMemory`
- `NetworkMapping`

Katalog mit einem Maschinenprofil erstellen:

1. Öffnen Sie das PowerShell-Fenster.
2. Führen Sie `asnp citrix*` aus.
3. Erstellen Sie einen Identitätspool. Der Identitätspool ist ein Container für die Active Directory-Konten der zu erstellenden VMs. Beispiel:

```
1 New-AcctIdentityPool -Domain "citrix-xxxxxx.local" -
      IdentityPoolName "ExampleIdentityPool" -NamingScheme "abc1-##"
      -NamingSchemeType "Numeric" -Scope @() -ZoneUid "xxxxxxxx"
2 <!--NeedCopy-->
```

4. Erstellen Sie die erforderlichen AD-Computerkonten in Active Directory.

```
1 $password = "password123" | ConvertTo-SecureString -AsPlainText -
      Force
2 New-AcctADAccount -IdentityPoolName "ExampleIdentityPool" -Count
      10 -ADUserName "citrix-xxxxxx\admin1" -ADPassword $password
3 Set-AcctAdAccountUserCert -IdentityPoolName "ExampleIdentityPool"
      -ADUserName "citrix-xxxxxx\admin1" -ADPassword $password
4 <!--NeedCopy-->
```

5. Führen Sie den Befehl `New-ProvScheme` aus, um einen Katalog zu erstellen. Beispiel:

```
1 New-ProvScheme -CleanOnBoot -HostingUnitName "ExampleHostingUnit"
      -IdentityPoolName "ExampleIdentityPool" -InitialBatchSizeHint 2
       -CustomProperties '<CustomProperties xmlns="http://schemas.
      citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
      org/2001/XMLSchema-instance">
2 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="
      true" />
3 </CustomProperties>'
4 -MasterImageVM "XDHyp:\HostingUnits\ExampleHostingUnit\ExampleVDA.
      vm\ExampleVDA.snapshot" -ProvisioningSchemeName "ExampleCatalog
      " -Scope @() -SecurityGroup @()
5 -MachineProfile "XDHyp:\HostingUnits\ExampleHostingUnit\
      ExampleMachineProfile.vm"
6 <!--NeedCopy-->
```

6. Registrieren Sie das Provisioningsschema als Brokerkatalog. Beispiel:

```
1 $ConfigZone = Get-ConfigZone | Where-Object {
2   $_.Name -eq "xxxxxx"  }
```



```
3
4 New-BrokerCatalog -Name "MPLT1" -AllocationType Random -
      Description "Machine profile catalog" -ProvisioningSchemeId
      fe7df345-244e-4xxxx-xxxxxxxxx -ProvisioningType Mcs -
      SessionSupport MultiSession -PersistUserChanges Discard -
      ZoneUid ($ConfigZone.Uid)
5 <!--NeedCopy-->
```

7. Fügen Sie die VMs zum Katalog hinzu.

Katalog mit einem neuen Maschinenprofil aktualisieren:

1. Führen Sie den Befehl `Set-ProvScheme` aus. Beispiel:

```
1 Set-ProvScheme -ProvisioningSchemeName "ExampleCatalog" -
      MachineProfile "XDHyp:\HostingUnits\ExampleHostingUnit\
      ExampleMachineProfileVm.vm\ExampleMachineProfileSnapshot.
      snapshot"
2 <!--NeedCopy-->
```

   Weitere Informationen zum Befehl Set-ProvScheme finden Sie unter Set-ProvScheme.

> **Hinweis:**
>
> - Der Befehl `Set-ProvScheme` ändert in diesem Fall das Maschinenprofil der vorhandenen VMs im Katalog nicht. Nur neu erstellte VMs, die dem Katalog hinzugefügt werden, haben das neue Maschinenprofil.
> - Sie können keinen auf einem Maschinenprofil basierenden Maschinenkatalog in einen Maschinenkatalog konvertieren, der nicht auf Maschinenprofilen basiert.

So geht es weiter

- Wenn Sie den ersten Katalog erstellen, werden Sie von Web Studio zum Erstellen einer Bereitstellungsgruppe geleitet.
- Informationen zum gesamten Konfigurationsprozess finden Sie unter Installation und Konfiguration
- Informationen zur Verwaltung von Katalogen finden Sie unter Maschinenkataloge verwalten und XenServer-Katalog verwalten

Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Verbindung zu XenServer
- Maschinenkataloge erstellen

Google Cloud Platform-Katalog erstellen

June 28, 2024

Unter Maschinenkataloge erstellen werden die Assistenten zum Erstellen eines Maschinenkatalogs beschrieben. Die folgenden Informationen beziehen sich speziell auf Google-Cloudumgebungen.

> **Hinweis:**
>
> Bevor Sie einen Google Cloud Platform (GCP)-Katalog erstellen, müssen Sie eine Verbindung zu GCP hergestellt haben. Siehe Verbindung zu Google-Cloudumgebungen.

Vorbereiten einer Master-VM-Instanz und eines nichtflüchtigen Speichers

> **Tipp:**
>
> Nichtflüchtiger Speicher (Persistent Disk) ist der Google Cloud-Begriff für den virtuellen Datenträger.

Zur Vorbereitung Ihrer Master-VM-Instanz erstellen und konfigurieren Sie zunächst eine VM-Instanz mit Eigenschaften, die der gewünschten Konfiguration für die geklonten VDA-Instanzen im geplanten Maschinenkatalog entsprechen. Die Konfiguration gilt nicht nur für Größe und Typ der Instanz. Sie umfasst auch Instanzattribute wie Metadaten, Tags, GPU-Zuweisungen, Netzwerktags und Dienstkontoeigenschaften.

MCS verwendet dann Ihre Master-VM-Instanz, um die Google Cloud-*Instanzvorlage* zu erstellen. Auf der Basis der Instanzvorlage werden dann die geklonten VDA-Instanzen erstellt, die den Maschinenkatalog umfassen. Geklonte Instanzen erben die Eigenschaften der Master-VM-Instanz (mit Ausnahme der Eigenschaften für VPC, Subnetz und nichtflüchtigen Speicher), aus der die Instanzvorlage erstellt wurde.

Nachdem Sie die Eigenschaften der Master-VM-Instanz konfiguriert haben, starten Sie die Instanz und bereiten den nichtflüchtigen Speicher für die Instanz vor.

Es wird empfohlen, manuell einen Snapshot des Speichers zu erstellen. Dies ermöglicht eine aussagekräftige Benennung zum Nachverfolgen von Versionen, bietet mehr Optionen zum Verwalten früherer Versionen des Masterimages und spart Zeit beim Erstellen des Maschinenkatalogs. Wenn Sie keinen eigenen Snapshot erstellen, erstellt MCS einen temporären Snapshot, der bei Abschluss der Bereitstellung gelöscht wird.

Maschinenkatalog erstellen

Sie können einen Maschinenkatalog auf zweierlei Art erstellen:

- Maschinenkatalog mit Web Studio erstellen
- Maschinenkatalog mit PowerShell erstellen

Maschinenkatalog mit Web Studio erstellen

> **Hinweis:**
>
> Erstellen Sie Ihre Ressourcen, bevor Sie einen Maschinenkatalog erstellen. Verwenden Sie bei der Konfiguration von Maschinenkatalogen die von Google Cloud festgelegten Namenskonventionen. Weitere Informationen finden Sie unter Richtlinien zur Bucket- und Objektbenennung.

Folgen Sie den Anweisungen unter Erstellen von Maschinenkatalogen. Die folgende Beschreibung gilt nur für Google Cloud-Kataloge.

1. Melden Sie sich bei Web Studio an und wählen Sie im linken Bereich **Maschinenkataloge**.
2. Wählen Sie in der Aktionsleiste **Maschinenkatalog erstellen**.
3. Wählen Sie auf der Seite **Betriebssystem** die Option **Multisitzungs-OS** und wählen Sie **Weiter**.
   - Citrix Virtual Apps and Desktops unterstützt auch Einzelsitzungs-OS.
4. Wählen Sie auf der Seite **Maschinenverwaltung** die Optionen **Maschinen mit Energieverwaltung** und **Citrix Maschinenerstellungsdienste** und wählen Sie **Weiter**. Bei mehreren vorhandenen Ressourcen wählen Sie eine Ressource im Menü aus.
5. Führen Sie auf der Seite **Image** diese Schritte nach Bedarf aus und klicken Sie dann auf **Weiter**.
   a) Wählen Sie einen Snapshot oder eine VM als Masterimage aus. Wenn Sie die Einzelmandantenfunktion verwenden möchten, wählen Sie ein Image, dessen Knotengruppeneigenschaft korrekt konfiguriert ist. Siehe Aktivieren der Zonenauswahl.
   b) Um eine vorhandene VM als Maschinenprofil zu verwenden, wählen Sie Maschinenprofil verwenden und anschließend die VM aus.

      > **Hinweis:**
      >
      > Derzeit übernehmen VMs in diesem Katalog die Einstellungen "ID des Datenträgerverschlüsselungssatzes", "Maschinengröße", "Speichertyp"und "Zone"vom Maschinenprofil.

   c) Wählen Sie die Mindestfunktionsebene für den Katalog. Wenn Sie die Einzelmandantenfunktion verwenden möchten, wählen Sie ein Image, dessen Knotengruppeneigenschaft korrekt konfiguriert ist.
6. Wählen Sie auf der Seite **Speichertypen** den Speichertyp für das Betriebssystem für den Maschinenkatalog aus. Für die folgenden Speicheroptionen gelten jeweils eigene Preis- und

Leistungsmerkmale. (Ein Identitätsdatenträger wird immer mit dem persistenten Standarddatenträger der Zone erstellt.)

- Persistenter Standarddatenträger
- Ausbalancierter persistenter Datenträger
- Persistenter SSD-Datenträger

Informationen zu den Optionen finden Sie unter https://cloud.google.com/compute/docs/disks/.

7. Geben Sie auf der Seite **Virtuelle Maschinen** an, wie viele VMs Sie erstellen möchten, zeigen Sie die Spezifikation der VMs an und wählen Sie **Weiter**. Wenn Sie für Maschinenkataloge Knotengruppen für einzelne Mandanten verwenden, wählen Sie **ausschließlich** die Zonen, in denen reservierte Knoten für einzelne Mandanten verfügbar sind. Siehe Aktivieren der Zonenauswahl.
8. Wählen Sie auf der Seite **Computerkonten** ein Active Directory-Konto aus und wählen Sie **Weiter**.

   - Wenn Sie **Neue Active Directory-Konten erstellen** auswählen, wählen Sie eine Domäne und geben Sie dann die Zeichenfolge ein, die das Benennungsschema für die bereitgestellten, in Active Directory erstellten VM-Computerkonten darstellt. Das Kontenbenennungsschema schreibt 1–64 Zeichen und ausschließlich ASCII-Zeichen vor, der Name darf nicht ausschließlich aus Leerzeichen bestehen und folgende Zeichen nicht enthalten:
   - Bei Auswahl von **Vorhandene Active Directory-Konten verwenden** wählen Sie **Durchsuchen**, um die vorhandenen Active Directory-Computerkonten für die ausgewählten Maschinen aufzurufen.

9. Wählen Sie auf der Seite **Domänenanmeldeinformationen** die Option **Anmeldeinformationen eingeben**. Geben Sie den Benutzernamen und das Kennwort ein, wählen Sie **Speichern** und dann **Weiter**.

   - Die eingegebene Anmeldeinformationen müssen über Berechtigungen zum Ausführen von Active Directory-Kontovorgängen verfügen.

10. Überprüfen Sie die Informationen auf der Seite **Zusammenfassung**, geben Sie einen Namen für den Katalog ein und wählen Sie **Fertigstellen**.

    > **Hinweis:**
    >
    > Ab Version 2402 müssen GCP-Katalognamen den folgenden Regeln entsprechen:
    >
    > - Beginnen Sie mit einem Kleinbuchstaben.
    > - Verwenden Sie nur Kleinbuchstaben (a-z), Ziffern und Bindestriche.
    > - Beenden Sie entweder mit einem Kleinbuchstaben oder einer Ziffer.
    >
    > Wenn Sie versuchen, vorhandene GCP-Kataloge umzubenennen, die diesen Regeln nicht

> entsprechen, werden Fehlermeldungen angezeigt, die Sie anweisen, sie gemäß den aktualisierten Regeln umzubenennen.

Die Erstellung des Maschinenkatalogs kann lange dauern. Öffnen Sie die Google Cloud-Konsole, um zu überprüfen, ob die Maschinen auf den Zielknotengruppen erstellt wurden.

Importieren manuell erstellter Google Cloud-Maschinen

Sie können *eine Verbindung zu Google Cloud herstellen* und dann *einen Katalog mit Google Cloud-Maschinen erstellen*. Anschließend können Sie Google Cloud-Maschinen manuell mit Citrix Virtual Apps and Desktops neu starten. Das Feature ermöglicht folgende Aktionen:

- Manuell erstellte Google Cloud-Maschinen mit Multisitzungs-OS in einen Citrix Virtual Apps and Desktops-Maschinenkatalog importieren.
- Manuell erstellte Google Cloud-Maschinen mit Multisitzungs-OS aus einem Citrix Virtual Apps and Desktops-Katalog entfernen.
- Energieverwaltung von Multisitzungs-OS-Maschinen in Google Cloud über vorhandene Energieverwaltungsfunktionen von Citrix Virtual Apps and Desktops. Richten Sie beispielsweise einen Neustartplan für diese Maschinen ein.

Hierfür ist es nicht erforderlich, vorhandene Bereitstellungsworkflows für Citrix Virtual Apps and Desktops zu ändern oder vorhandene Features zu entfernen. Es wird empfohlen, Maschinen mit MCS in Web Studio bereitzustellen, anstatt manuell erstellte Google Cloud-Maschinen zu importieren.

Freigegebene virtuelle private Cloud

Freigegebene VPCs umfassen ein Hostprojekt, aus dem die freigegebenen Subnetze zur Verfügung gestellt werden, sowie mindestens ein Dienstprojekt, das die Ressource verwendet. Freigegebene VPCs sind gute Optionen für größere Installationen, da sie eine zentrale Steuerung, Nutzung und Verwaltung gemeinsam genutzter Google-Cloud-Ressourcen bieten. Weitere Informationen finden Sie auf der Google-Dokumentationssite.

Mit diesem Feature unterstützt Maschinenerstellungsdienste (MCS) das Provisioning und die Verwaltung von Maschinenkatalogen, die in freigegebenen VPCs bereitgestellt werden. Diese Unterstützung entspricht funktional der derzeitigen für lokale VPCs, weist aber in zwei Bereichen Unterschiede auf:

1. Sie müssen dem Dienstkonto, das zum Erstellen der Hostverbindung verwendet wird, zusätzliche Berechtigungen erteilen. Dadurch kann MCS auf freigegebene VPC-Ressourcen zugreifen und diese nutzen.
2. Sie müssen zwei Firewallregeln (eine für den eingehenden und eine für den ausgehenden Datenverkehr) erstellen. Die Firewallregeln werden beim Imagemastering verwendet.

Neue Berechtigungen erforderlich

Beim Erstellen der Hostverbindung ist ein Google Clouddienstkonto mit bestimmten Berechtigungen erforderlich. Diese zusätzlichen Berechtigungen müssen allen Dienstkonten erteilt werden, die zum Erstellen von Hostverbindungen für die freigegebene VPC verwendet werden.

> **Tipp:**
>
> Die zusätzlichen Berechtigungen sind für Citrix Virtual Apps and Desktops nicht neu. Sie werden verwendet, um die Verwendung lokaler VPCs zu erleichtern. Bei freigegebenen VPCs ermöglichen die zusätzlichen Berechtigungen den Zugriff auf andere freigegebene VPC-Ressourcen.

Dem Dienstkonto, das der Hostverbindung zugeordnet ist, müssen bis zu vier zusätzliche Berechtigungen erteilt werden, um eine freigegebene VPC zu unterstützen:

1. **compute.firewalls.list:** Diese Berechtigung ist obligatorisch. Mit ihr kann MCS die Liste der Firewallregeln auf der freigegebenen VPC abrufen.
2. **compute.networks.list:** Diese Berechtigung ist obligatorisch. Damit kann MCS die freigegebenen VPC-Netzwerke identifizieren, die dem Dienstkonto zur Verfügung stehen.
3. **compute.subnetworks.list:** Diese Berechtigung ist je nach Verwendung der VPCs optional. Damit kann MCS die Subnetze der sichtbaren, freigegebenen VPCs identifizieren. Diese Berechtigung ist für die Verwendung lokaler VPCs erforderlich, muss aber auch im Hostprojekt für freigegebene VPCs zugewiesen werden.
4. **compute.subnetworks.use:** Diese Berechtigung ist je nach Verwendung der VPCs optional. Sie ist zur Verwendung von Subnetzressourcen in den bereitgestellten Maschinenkatalogen erforderlich. Diese Berechtigung ist für die Verwendung lokaler VPCs erforderlich, muss aber auch im Hostprojekt für freigegebene VPCs zugewiesen werden.

Berücksichtigen Sie bei der Verwendung dieser Berechtigungen, dass es, basierend auf dem Berechtigungstyp, verschiedene Ansätze zum Erstellen des Maschinenkatalogs gibt:

- Berechtigung auf Projektebene:
  - Ermöglicht Zugriff auf alle freigegebenen VPCs im Hostprojekt.
  - Erfordert, dass dem Dienstkonto die Berechtigungen 3 und 4 zugewiesen sind.
- Berechtigung auf Subnetzebene:
  - Ermöglicht den Zugriff auf einzelne Subnetze in der freigegebenen VPC.
  - Die Berechtigungen 3 und 4 gehören zur Zuweisung auf Subnetzebene und müssen daher dem Dienstkonto nicht direkt zugewiesen werden.

Wählen Sie das Konzept aus, der Ihren Anforderungen und Sicherheitsstandards entspricht.

> **Tipp:**
>
> Weitere Informationen zu den Unterschieden zwischen Berechtigungen auf Projektebene und Subnetzebene finden Sie in der Google Cloud-Dokumentation.

Firewallregeln

Bei der Vorbereitung eines Maschinenkatalogs wird ein Maschinenabbild vorbereitet, das als Masterimage-Systemdatenträger für den Katalog dient. Bei diesem Vorgang wird der Datenträger vorübergehend an eine virtuelle Maschine angefügt. Die VM muss in einer isolierten Umgebung ausgeführt werden, die jeglichen eingehenden und ausgehenden Netzwerkdatenverkehr verhindert. Dies wird durch zwei Alles-abweisen-Firewallregeln verwirklicht: eine für eingehenden und eine für ausgehenden Datenverkehr. Bei Verwendung Google Cloud-lokaler VCPs erstellt MCS diese Firewall im lokalen Netzwerk und wendet sie für das Mastering auf die Maschine an. Nach Abschluss des Masterings werden die Firewallregeln aus dem Image entfernt.

Es wird empfohlen, die Anzahl der neuen Berechtigungen, die für die Verwendung freigegebener VPCs erforderlich sind, auf ein Minimum zu beschränken. Freigegebene VPCs sind wichtige Unternehmensressourcen, für die in der Regel strenge Sicherheitsprotokolle gelten. Erstellen Sie daher im Hostprojekt zwei Firewallregeln für die freigegebenen VPC-Ressourcen: eine für eingehenden und eine für ausgehenden Datenverkehr. Weisen Sie diesen die höchste Priorität zu. Wenden Sie auf beide Regeln über den folgenden Wert ein neues Ziel-Tag an:

```
citrix-provisioning-quarantine-firewall
```

Wenn MCS einen Maschinenkatalog erstellt oder aktualisiert, sucht es nach Firewallregeln mit diesem Ziel-Tag. Es prüft die Regeln auf Richtigkeit und wendet sie auf die Maschine an, die zur Vorbereitung des Masterimages für den Katalog verwendet wird. Werden die Firewallregeln nicht gefunden oder die gefundenen Regeln haben die falsche Priorität, wird folgende Meldung (oder eine mit ähnlichem Wortlaut) angezeigt:

```
"Unable to find valid INGRESS and EGRESS quarantine firewall rules
for VPC <name> in project <project>. "Please ensure you have created
 'deny all'firewall rules with the network tag 'citrix-provisioning-
quarantine-firewall'and proper priority.""Refer to Citrix Documentation
 for details."
```

Konfigurieren der freigegebenen VPC

Führen Sie vor dem Hinzufügen der freigegebenen VPC als Hostverbindung in Web Studio die folgenden Schritte aus, um die Dienstkonten aus dem betreffenden Projekt hinzuzufügen:

1. IAM-Rolle erstellen.

2. Fügen Sie der IAM-Rolle des Hostprojekts für die freigegebene VPC das Dienstkonto hinzu, das zum Erstellen einer CVAD-Hostverbindung verwendet wird.
3. Fügen Sie der IAM-Rolle des Hostprojekts für die freigegebene VPC das Cloud Build-Dienstkonto aus dem Projekt hinzu, das Sie bereitstellen möchten.
4. Firewallregeln erstellen.

IAM-Rolle erstellen Wählen Sie die Zugriffsebene der Rolle: *Projektebene* oder (eingeschränkter) *Subnetzebene*.

Zugriff auf Projektebene für die IAM-Rolle. Weisen Sie einer IAM-Rolle auf Projektebene die folgenden Berechtigungen zu:

- compute.firewalls.list
- compute.networks.list
- compute.subnetworks.list
- compute.subnetworks.use

Führen Sie zum Erstellen einer IAM-Rolle auf Projektebene folgende Schritte aus:

1. Gehen Sie in der Google Cloud-Konsole zu **IAM & Admin > Roles**.
2. Wählen Sie **CREATE ROLE** auf der Seite **Roles**.
3. Geben Sie auf der Seite **Create Role** einen Rollennamen ein. Wählen Sie **ADD PERMISSIONS**.
    a) Fügen Sie auf der Seite **Add permissions** der Rolle Berechtigungen hinzu. Um eine Berechtigung hinzuzufügen, geben Sie deren Namen in das Feld **Filter table** ein. Wählen Sie die Berechtigung aus und wählen Sie **ADD**.
    b) Wählen Sie **CREATE**.

IAM-Rolle auf Subnetzebene. Bei dieser Rolle werden die Berechtigungen `compute.subnetworks.list` und `compute.subnetworks.use` nach Auswahl von **CREATE ROLE** ausgelassen. Für diese IAM-Zugriffsebene müssen die Berechtigungen `compute.firewalls.list` und `compute.networks.list` auf die neue Rolle angewendet werden.

Führen Sie zum Erstellen einer IAM-Rolle auf Subnetzebene folgende Schritte aus:

1. Navigieren Sie in der Google Cloud-Konsole zu **VPC network** > **Shared VPC**. Auf der Seite **Shared VPC** werden die Subnetze der freigegebenen VPC-Netzwerke des Hostprojekts angezeigt.
2. Wählen Sie auf der Seite **Shared VPC** das Subnetz aus, auf das Sie zugreifen möchten.
3. Wählen Sie oben rechts **ADD MEMBER**, um ein Dienstkonto hinzuzufügen.
4. Führen Sie auf der Seite **Add members** die folgenden Schritte aus:
    a) Geben Sie im Feld **New members** den Namen des Dienstkontos ein und wählen Sie dann im Menü das Dienstkonto aus.

b) Wählen Sie das Feld **Select a Roll** und dann **Compute Network User**.
c) Wählen Sie **SAVE**.

5. Gehen Sie in der Google Cloud-Konsole zu **IAM & Admin** > **Roles**.
6. Wählen Sie **CREATE ROLE** auf der Seite **Roles**.
7. Geben Sie auf der Seite **Create Role** einen Rollennamen ein. Wählen Sie **ADD PERMISSIONS**.

a) Fügen Sie auf der Seite **Add permissions** der Rolle Berechtigungen hinzu. Um eine Berechtigung hinzuzufügen, geben Sie deren Namen in das Feld **Filter table** ein. Wählen Sie die Berechtigung aus und wählen Sie **ADD**.
b) Wählen Sie **CREATE**.

Hinzufügen eines Dienstkontos zur IAM-Rolle des Hostprojekts Führen Sie nach dem Erstellen einer IAM-Rolle die folgenden Schritte aus, um ein Dienstkonto für das Hostprojekt hinzuzufügen:

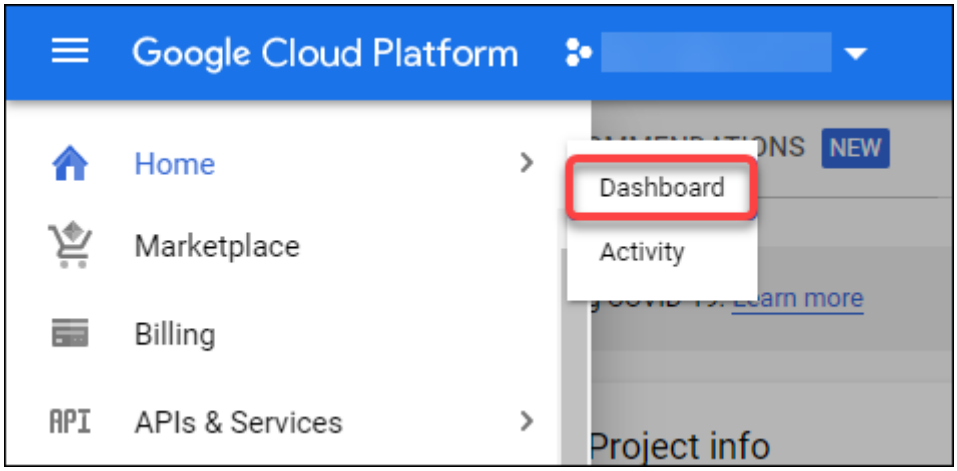
1. Gehen Sie in der Google Cloud-Konsole zum Hostprojekt und dann zu **IAM & Admin > IAM**.
2. Wählen Sie auf der Seite **IAM** die Option **ADD**, um ein Dienstkonto hinzuzufügen.
3. Führen Sie auf der Seite **Add members** folgende Schritte aus:

a) Geben Sie im Feld **New members** den Namen des Dienstkontos ein und wählen Sie dann im Menü das Dienstkonto aus.
b) Wählen Sie ein Rollenfeld, geben Sie die erstellte IAM-Rolle ein und wählen Sie dann im Menü die Rolle.
c) Wählen Sie **SAVE**.

Das Dienstkonto ist damit für das Hostprojekt konfiguriert.

Cloud Build-Dienstkonto zur freigegebenen VPC hinzufügen Jedes Google Cloud-Abonnement hat ein Dienstkonto, das denselben Namen trägt wie die Projekt-ID, gefolgt von `cloudbuild.gserviceaccount`. Beispiel: `705794712345@cloudbuild.gserviceaccount`.

Die Projekt-ID Ihres Projekts ermitteln Sie, indem Sie in der Google Cloud-Konsole **Home** und **Dashboard** auswählen:



Die ID wird im Bereich **Project Info** unter **Project Number** angezeigt.

Zum Hinzufügen des Cloud Build-Dienstkontos zur freigegebenen VPC führen Sie folgende Schritte aus:

1. Gehen Sie in der Google Cloud-Konsole zum Hostprojekt und dann zu **IAM & Admin** > **IAM**.
2. Wählen Sie **ADD** auf der Seite **Permissions**, um ein Konto hinzuzufügen.
3. Führen Sie auf der Seite **Add members** die folgenden Schritte aus:

    a) Geben Sie im Feld **New members** den Namen des Cloud Build-Kontos ein und wählen Sie dann im Menü das Dienstkonto aus.
    b) Wählen Sie das Feld **Select a role**, geben Sie `Computer Network User` ein und wählen Sie dann im Menü die Rolle.
    c) Wählen Sie **SAVE**.

Erstellen von Firewallregeln Beim Mastering kopiert MCS das ausgewählte Maschinenabbild und bereitet damit den Masterimage-Systemdatenträger für den Katalog vor. Beim Masterings fügt MCS den Datenträger an eine temporäre virtuelle Maschine an und führt dann Vorbereitungsskripts aus. Die VM muss in einer isolierten Umgebung ausgeführt werden, die jeglichen eingehenden und ausgehenden Netzwerkdatenverkehr verhindert. Um eine isolierte Umgebung zu erstellen, erfordert MCS zwei *Alles-abweisen*-Firewallregeln (eine Eingangsregel und eine Ausgangregel). Erstellen Sie daher zwei Firewallregeln im *Hostprojekt*:

1. Gehen Sie in der Google Cloud-Konsole zum Hostprojekt und dann zu **VPC network > Firewall**.
2. Wählen Sie auf der Seite **Firewall** die Option **CREATE FIREWALL RULE**.
3. Führen Sie auf der Seite **Create a firewall rule** die folgenden Schritte aus:

    - **Name**. Geben Sie einen Namen für die Regel ein.
    - **Network**. Wählen Sie das freigegebene VPC-Netzwerk aus, für das die Firewallregel für eingehenden Datenverkehr gilt.

- **Priority**. Je kleiner der Wert ist, desto höher ist die Priorität der Regel. Citrix empfiehlt einen kleinen Wert (z. B. 10).
- **Direction of traffic**. Wählen Sie **Ingress**.
- **Action on match**. Wählen Sie **Deny**.
- **Targets**. Verwenden Sie die Standardeinstellung **Specified target tags**.
- **Target tags**. Geben Sie `citrix-provisioning-quarantine-firewall` ein.
- **Source filter**. Verwenden Sie die Standardeinstellung **IP ranges**.
- **Source IP ranges**. Geben Sie einen Bereich ein, der den gesamten Datenverkehr abdeckt. Geben Sie `0.0.0.0/0` ein.
- **Protocols and ports**. Wählen Sie **Deny all**.

4. Wählen Sie **CREATE**, um die Regel zu erstellen.
5. Wiederholen Sie die Schritte 1 bis 4, um eine weitere Regel zu erstellen. Wählen Sie für **Direction of traffic** die Option **Egress**.

Hinzufügen einer Verbindung Fügen Sie eine Verbindung zu den Google Cloud-Umgebungen hinzu. Siehe Eine Verbindung hinzufügen.

Aktivieren der Zonenauswahl

Citrix Virtual Apps and Desktops unterstützt die Zonenauswahl. Bei der Zonenauswahl geben Sie die Zonen an, in denen VMs erstellt werden sollen. Mithilfe der Zonenauswahl können Administratoren die Einzelmandantenknoten in Zonen ihrer Wahl platzieren. Um die Einzelmandantenfähigkeit zu konfigurieren, müssen Sie folgende Schritte in Google Cloud ausführen:

- Reservieren eines Google Cloud-Knotens für einzelne Mandanten
- Erstellen des VDA-Masterimages

Einen Google Cloud-Sole-Mandantenknoten reservieren

Informationen zum Reservieren eines Einzelmandantenknotens finden Sie in der Dokumentation zu Google Cloud.

> **Wichtig:**
>
> Eine Knotenvorlage wird zur Bezeichnung der Leistungsmerkmale des Systems verwendet, das in der Knotengruppe reserviert ist. Zu diesen Merkmalen gehören die Anzahl der virtuellen GPUs, der dem Knoten zugewiesene Arbeitsspeicher und der für die auf dem Knoten erstellten Maschinen verwendete Maschinentyp. Weitere Informationen finden Sie in der Dokumentation zu Google Cloud.

Erstellen des VDA-Masterimages

Um Maschinen auf dem Knoten für einzelne Mandanten erfolgreich bereitzustellen, müssen Sie beim Erstellen eines Master-VM-Images zusätzliche Schritte ausführen. Maschineninstanzen in Google Cloud besitzen die Eigenschaft *node affinity labels*. Bei Instanzen, die als Masterimage für auf Knoten für einzelne Mandanten bereitgestellte Kataloge verwendet werden, muss das *Knotenaffinitätslabel* mit dem Namen der **Zielknotengruppe** übereinstimmen. Um dies zu erreichen, beachten Sie Folgendes:

- Legen Sie für neue Instanzen das Knotenaffinitätslabel bei deren Erstellung in der Google Cloud-Konsole fest. Weitere Informationen finden Sie unter Festlegen des Knotenaffinitätslabels beim Erstellen einer Instanz.
- Legen Sie für bestehende Instanzen das Knotenaffinitätslabel über die **gcloud**-Befehlszeile fest. Weitere Informationen finden Sie unter Festlegen des Knotenaffinitätslabels für eine bestehende Instanz.

> **Hinweis:**
>
> Wenn Sie die Einzelmandantenfähigkeit mit einer freigegebenen VPC verwenden möchten, lesen Sie den Abschnitt Freigegebene virtuelle private Cloud.

Festlegen des Knotenaffinitätslabels beim Erstellen einer Instanz Zum Festlegen des Knotenaffinitätslabels führen Sie folgende Schritte aus:

1. Navigieren Sie in der Google Cloud-Konsole zu **Compute Engine > VM instances**.
2. Wählen Sie auf der Seite **VM instances** die Option **Create instance**.
3. Geben Sie auf der Seite **Instance creation** die erforderlichen Informationen an und wählen Sie **management, security, disks, networking, sole tenancy**, um das Einstellungsfenster zu öffnen.
4. Wählen Sie **Browse** auf der Registerkarte **Sole tenancy**, um die verfügbaren Knotengruppen im aktuellen Projekt anzuzeigen. Die Seite **Sole-tenant node** wird mit einer Liste der verfügbaren Knotengruppen angezeigt.
5. Wählen Sie auf der Seite **Sole-tenant node** die gewünschte Knotengruppe aus der Liste aus und wählen Sie **Select**, um zur Registerkarte **Sole tenancy** zurückzukehren. Das Feld ‘‘node affinity labels’’wird mit den ausgewählten Informationen ausgefüllt. Mit dieser Einstellung wird sichergestellt, dass aus der Instanz erstellte Maschinenkataloge für die ausgewählte Knotengruppe bereitgestellt werden.
6. Wählen Sie **Create**, um die Instanz zu erstellen.

Festlegen des Knotenaffinitätslabels für eine bestehende Instanz Zum Festlegen des Knotenaffinitätslabels führen Sie folgende Schritte aus:

1. Legen Sie im Google Cloud Shell-Terminalfenster ein Knotenaffinitätslabel mit dem Befehl *gcloud compute instances* fest. Der **gcloud**-Befehl muss die folgenden Informationen enthalten:

   - **Name der VM.** Verwenden Sie beispielsweise eine bestehende VM namens `s*2019-vda-base*`.
   - **Name der Knotengruppe.** Verwenden Sie den zuvor erstellten Knotengruppennamen. Beispiel: `mh-sole-tenant-node-group-1`.
   - **Die Zone, in der sich die Instanz befindet**. Die VM kann sich beispielsweise in `*us-east-1b* zone` befinden.

   Geben Sie beispielsweise den folgenden Befehl im Terminalfenster ein:

   - `gcloud compute instances set-scheduling "s2019-vda-base"--node-group="mh-sole-tenant-node-group-1"--zone="us-east1-b"`

   Weitere Informationen zum Befehl *gcloud compute instances* finden Sie in der Google Developer Tools-Dokumentation unter https://cloud.google.com/sdk/gcloud/reference/beta/compute/instances/set-scheduling.

2. Navigieren Sie zu der Seite **VM instance details** der Instanz und prüfen Sie, ob das Feld **Node Affinities** das Label enthält.

Maschinenkatalog erstellen Nach dem Festlegen des Knotenaffinitätslabels konfigurieren Sie den Maschinenkatalog.

Vom Kunden verwaltete Verschlüsselungsschlüssel (CMEK)

Sie können vom Kunden verwaltete Verschlüsselungsschlüssel (Customer Managed Encryption Keys, CMEK) für MCS-Kataloge verwenden. Wenn Sie das Feature verwenden, weisen Sie dem Compute Engine Service-Agent die Google Cloud Key Management Service `CryptoKey Encrypter/Decrypter`-Rolle zu. Das Citrix Virtual Apps and Desktops-Konto muss über die richtigen Berechtigungen in dem Projekt verfügen, in dem der Schlüssel gespeichert ist. Weitere Informationen finden Sie unter Ressourcen mit Cloud KMS-Schlüsseln schützen.

Ihr Compute Engine Service Agent folgt folgendem Format: `service-<Project _Number>@compute-system.iam.gserviceaccount.com`. Dieses unterscheidet sich von dem standardmäßigen Compute Engine Service-Konto.

> **Hinweis:**
>
> Dieses Compute Engine Service-Konto wird möglicherweise nicht in den **IAM-Berechtigungen** der Google-Konsole angezeigt. Verwenden Sie in solchen Fällen den Befehl `gcloud`, wie unter Ressourcen mit Cloud KMS-Schlüsseln schützen beschrieben.

Berechtigungen zum Citrix Virtual Apps and Desktops-Konto zuweisen

Google Cloud KMS-Berechtigungen können auf verschiedene Art und Weise konfiguriert werden. Sie können entweder die KMS-Berechtigungen auf *Projektebene* oder auf *Ressourcenebene* bereitstellen. Weitere Informationen finden Sie unter Berechtigungen und Rollen.

Berechtigungen auf Projektebene Sie können dem Citrix Virtual Apps and Desktops-Konto Berechtigungen auf Projektebene zum Durchsuchen von Cloud KMS-Ressourcen zuweisen. Erstellen Sie dazu eine benutzerdefinierte Rolle und fügen Sie die folgenden Berechtigungen hinzu:

- `cloudkms.keyRings.list`
- `cloudkms.keyRings.get`
- `cloudkms.cryptokeys.list`
- `cloudkms.cryptokeys.get`

Weisen Sie die benutzerdefinierte Rolle Ihrem Citrix Virtual Apps and Desktops zu. Dadurch können Sie regionale Schlüssel im relevanten Projekt im Bestand durchsuchen.

Berechtigungen auf Ressourcenebene Gehen Sie für die zweite Option –Berechtigungen auf Ressourcenebene –in der Google Cloud-Konsole zu dem `cryptoKey`, den Sie für die MCS-Bereitstellung verwenden. Fügen Sie das Citrix Virtual Apps and Desktops-Konto einem Schlüsselbund oder Schlüssel hinzu, den Sie für die Katalogbereitstellung verwenden.

> **Tipp:**
>
> Mit dieser Option können Sie keine regionalen Schlüssel für Ihr Projekt im Bestand durchsuchen, da das Citrix Virtual Apps and Desktops-Konto keine Listenberechtigungen auf Projektebene für die Cloud KMS-Ressourcen hat. Sie können jedoch Kataloge mit CMEK bereitstellen, indem Sie die korrekte `cryptoKeyId` in den benutzerdefinierten Eigenschaften für `ProvScheme` angeben wie unten beschrieben.

Provisioning mit vom Kunden verwalteten Verschlüsselungsschlüsseln (CMEK) mit benutzerdefinierte Eigenschaften

Geben Sie beim Erstellen Ihres Provisioningschemas über PowerShell eine `CryptoKeyId`-Eigenschaft in `ProvScheme CustomProperties` an. Beispiel:

```
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
    <Property xsi:type="StringProperty" Name="CryptoKeyId" Value="<
       yourCryptoKeyId>" />
</CustomProperties>'
<!--NeedCopy-->
```

Die `cryptoKeyId` muss im folgenden Format angegeben werden:

`projectId:location:keyRingName:cryptoKeyName`

Wenn Sie beispielsweise den Schlüssel `my-example-key` im Schlüsselbund `my-example-key-ring` in der Region `us-east1` und Projekt-ID `my-example-project-1` verwenden möchten, sehen die benutzerdefinierten `ProvScheme`-Einstellungen in etwa so aus:

```
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
    <Property xsi:type="StringProperty" Name="CryptoKeyId" Value="my-
       example-project-1:us-east1:my-example-key-ring:my-example-key"
       />
</CustomProperties>'
<!--NeedCopy-->
```

Alle zu dem Provisioningschema gehörenden, per MCS bereitgestellten Datenträger und Images verwenden diesen kundenverwalteten Verschlüsselungsschlüssel.

> **Tipp:**
>
> Wenn Sie globale Schlüssel verwenden, muss der Kundeneigenschaftenort anstelle des Namens der **Region** (im obigen Beispiel **us-east1**) `global` sein. Beispiel: `<Property xsi:type="StringProperty"Name="CryptoKeyId"Value="my-example-project-1:global:my-example-key-ring:my-example-key"/>`.

Wechsel vom Kunden verwalteter Schlüssel

Google Cloud unterstützt keinen Wechsel von Schlüsseln für bestehende persistente Datenträger bzw. Images. Sobald eine Maschine bereitgestellt ist, ist sie an die zum Zeitpunkt ihrer Erstellung verwendete Schlüsselversion gebunden. Es kann jedoch eine neue Schlüsselversion erstellt werden, die dann

für neu bereitgestellte Maschinen bzw. Ressourcen verwendet, die erstellt werden, wenn ein Katalog mit einem neuen Masterimage aktualisiert wird.

Wichtige Überlegungen zu Schlüsselbunden Schlüsselbunde können nicht umbenannt oder gelöscht werden. Außerdem können bei ihrer Konfiguration unerwartete Gebühren anfallen. Wenn Sie einen Schlüsselbund löschen, zeigt Google Cloud eine Fehlermeldung an:

```
Sorry, you can't delete or rename keys or key rings. We were concerned about the security implications of allowing multiple keys or key versions over time to have the same resource name, so we decided to make names immutable. (And you can't delete them, because we wouldn't be able to do a true deletion--there would still have to be a tombstone tracking that this name had been used and couldn't be reused).
We're aware that this can make things untidy, but we have no immediate plans to change this.
If you want to avoid getting billed for a key or otherwise make it unavailable, you can do so by deleting all the key versions; neither keys nor key rings are billed for, just the active key versions within the keys.
<!--NeedCopy-->
```

> **Tipp:**
>
> Weitere Informationen finden Sie unter Bearbeiten oder Löschen eines Schlüsselbunds von der Konsole.

Kompatibilität mit einheitlichem Zugriff auf Bucket-Ebene

Citrix Virtual Apps and Desktops ist kompatibel mit der Richtlinie zum einheitlichen Zugriff auf Bucket-Ebene von Google Cloud. Diese Funktion erweitert die Verwendung der IAM-Richtlinie, die Berechtigungen für ein Dienstkonto erteilt, um die Bearbeitung von Ressourcen (einschließlich Storage-Buckets) zu ermöglichen. Durch einheitlichen Zugriff auf Bucket-Ebene können Sie in Citrix Virtual Apps and Desktops per Zugriffssteuerungsliste (ACL) den Zugriff auf Storage-Buckets oder darin gespeicherte Objekte zu steuern. Einen Überblick über den einheitlichen Zugriff auf Bucket-Ebene in Google Cloud finden Sie unter Einheitlicher Zugriff auf Bucket-Ebene. Informationen zur Konfiguration finden Sie unter Anfordern des einheitlichen Zugriffs auf Bucket-Ebene.

Maschinenkatalog mit PowerShell erstellen

In diesem Abschnitt wird beschrieben, wie Sie Kataloge mit PowerShell erstellen:

- Katalog mit persistentem Zurückschreibcachedatenträger erstellen
- Startleistung mit MCSIO verbessern

- Maschinenkatalog mit einem Maschinenprofil erstellen
- Maschinenkatalog mit einem Maschinenprofil als Instanzvorlage erstellen
- Katalog mit Shielded VM mit PowerShell erstellen
- Windows 11-VMs auf dem Einzelmandantenknoten erstellen

Katalog mit persistentem Zurückschreibcachedatenträger erstellen

Zum Konfigurieren eines Katalogs mit persistentem Datenträger für den Zurückschreibcache verwenden Sie den PowerShell-Parameter `New-ProvScheme CustomProperties`.

> **Tipp:**
>
> Verwenden Sie den PowerShell-Parameter hier nur für cloudbasierte Hostverbindungen. Wenn Sie Maschinen mit persistentem Zurückschreibcachedatenträger für eine On-Premises-Lösung (z. B. XenServer) bereitstellen möchten, wird PowerShell nicht benötigt, da der Datenträger automatisch persistent ist.

Dieser Parameter unterstützt die zusätzliche Eigenschaft `PersistWBC`, welche bestimmt, ob der Zurückschreibcachedatenträger bei von MCS-bereitgestellten Maschinen persistent 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.

> **Hinweis:**
>
> Dieses Verhalten gilt für Azure und GCP, bei dem der standardmäßige MCSIO-Zurückschreibcachedatenträger beim Aus- und Wiedereinschalten gelöscht und neu erstellt wird. Sie können den Datenträger als persistent konfigurieren, um das Löschen und neu Erstellen des MCSIO-Zurückschreibcachedatenträger zu vermeiden.

Wenn `PersistWBC` auf **`true`** festgelegt ist, wird der Zurückschreibcachedatenträger nicht gelöscht, wenn der Citrix Virtual Apps and Desktops-Administrator die Maschine über die Verwaltungsoberfläche herunterfährt.

Wenn `PersistWBC` auf **`false`** festgelegt ist, wird der Zurückschreibcachedatenträger gelöscht, wenn der Citrix Virtual Apps and Desktops-Administrator die Maschine über die Verwaltungsoberfläche herunterfährt.

> **Hinweis:**
>
> Wird die Eigenschaft `PersistWBC` nicht angegeben, so gilt der Standardwert **`false`** und der Zurückschreibcachedatenträger wird beim Herunterfahren der Maschine über die Verwaltungsoberfläche gelöscht.

Beispiel: Festlegen von `PersistWBC` auf **`true`** mithilfe des Parameters "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>
<!--NeedCopy-->
```

> **Hinweis:**
>
> 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.

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-->
```


Startleistung mit MCSIO verbessern

Sie können die Startleistung für in Azure oder GCP verwaltete Datenträger verbessern, wenn MCSIO aktiviert ist. Verwenden Sie die benutzerdefinierte PowerShell-Eigenschaft `PersistOSDisk` im Befehl `New-ProvScheme`, um dieses Feature zu konfigurieren: Optionen für `New-ProvScheme`:

```
<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="Resource <!--NeedCopy-->
``````<!--NeedCopy-->
<!--NeedCopy-->
````````Groups" Value="benvaldev5RG3" />
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true"
   />
</CustomProperties>
<!--NeedCopy-->
```

Um dieses Feature zu aktivieren, legen Sie die benutzerdefinierte Eigenschaft `PersistOSDisk` auf **`true`** fest. Beispiel:

```
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
   =`"PersistOsDisk`" 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-->
```

### Maschinenkatalog mit einem Maschinenprofil erstellen

Wenn Sie einen Katalog für das Provisioning von Maschinen mit MCS erstellen, können Sie ein Maschinenprofil verwenden, das die Hardwareeigenschaften einer virtuellen Maschine erfasst und auf neu bereitgestellte VMs im Katalog anwendet. Wenn der Parameter `MachineProfile` nicht verwendet wird, werden die Hardwareeigenschaften von der Masterimage-VM oder dem Snapshot erfasst. Einige Eigenschaften, die Sie explizit definieren (beispielsweise `StorageType`, `CatalogZones` und `CryptoKeyIs`) werden im Maschinenprofil ignoriert.

- Verwenden Sie den Befehl `New-ProvScheme`, um einen Katalog mit einem Maschinenprofil zu erstellen. Beispiel: `New-ProvScheme –MachineProfile "path to VM"`. Wenn Sie den Parameter `MachineProfile` nicht angeben, werden Hardwareeigenschaften von der Masterimage-VM erfasst.
- Verwenden Sie den Befehl `Set-ProvScheme`, um einen Katalog mit einem neuen Maschinenprofil zu aktualisieren. Beispiel: `Set-ProvScheme –MachineProfile "path to new VM"`. Dieser Befehl ändert das Maschinenprofil der vorhandenen VMs im Katalog nicht. Nur neu erstellte VMs, die dem Katalog hinzugefügt werden, haben das neue Maschinenprofil.
- Sie können auch das Masterimage aktualisieren, allerdings werden hierbei die Hardwareeigenschaften nicht aktualisiert. Wenn Sie die Hardwareeigenschaften aktualisieren möchten, müssen Sie das Maschinenprofil mit dem Befehl `Set-ProvScheme` aktualisieren. Die Änderungen gelten nur für die neuen Maschinen im Katalog. Um die Hardwareeigenschaften einer vorhandenen Maschine zu aktualisieren, können Sie den Befehl `Set-ProvVMUpdateTimeWindow` mit den Parametern `-StartsNow` und `-DurationInMinutes -1` verwenden.

  > **Hinweis:**
  >
  > - `StartsNow` gibt an, dass die geplante Startzeit die aktuelle Uhrzeit ist.
  > - `DurationInMinutes` mit einer negativen Zahl (z. B. -1) gibt an, dass es im Zeitfenster des Zeitplans keine Obergrenze gibt.

### Maschinenkatalog mit einem Maschinenprofil als Instanzvorlage erstellen

Sie können eine GCP-Instanzvorlage als Eingabe für das Maschinenprofil auswählen. Instanzvorlagen sind schlanke Ressourcen in GCP und daher sehr kostengünstig.

### Maschinenkatalog mit einem Maschinenprofil als Instanzvorlage erstellen

1. Öffnen Sie ein PowerShell-Fenster.
2. Führen Sie `asnp citrix*` aus, um die Citrix-spezifischen PowerShell-Module zu laden.
3. Suchen Sie mit dem folgenden Befehl eine Instanzvorlage in Ihrem GCP-Projekt:

```
cd XDHyp:\HostingUnits<HostingUnitName>\instanceTemplates.folder
<!--NeedCopy-->
```

4. Erstellen Sie mit dem Befehl NewProvScheme einen neuen Maschinenkatalog mit Maschinenprofil als Instanzvorlage:

```
New-ProvScheme -ProvisioningSchemeName <CatalogName>  -
    HostingUnitName <HostingUnitName> -IdentityPoolName <identity
    pool name> -MasterImageVM
XDHyp:\HostingUnits<HostingUnitName> \Base.vm\Base.snapshot -
    MachineProfile XDHyp:\HostingUnits<HostingUnitName>\
    instanceTemplates.folder\mytemplate.template
<!--NeedCopy-->
```

   Weitere Hinweise zum Befehl New-ProvScheme finden Sie unter https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/MachineCreation/New-ProvScheme/.

5. Beenden Sie das Erstellen des Maschinenkatalogs mithilfe von PowerShell-Befehlen. Informationen zum Erstellen eines Katalogs mit dem Remote PowerShell SDK finden Sie unter https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

### Maschinenprofil eines vorhandenen Maschinenkatalogs in eine Instanzvorlage ändern

Schritte zum Ändern des Maschinenprofils eines vorhandenen Maschinenkatalogs in eine Instanzvorlage:

1. Öffnen Sie ein PowerShell-Fenster.
2. Führen Sie `asnp citrix*` aus, um die Citrix-spezifischen PowerShell-Module zu laden.
3. Führen Sie den folgenden Befehl aus:

```
Set-ProvScheme -ProvisioningSchemeName  <CatalogName> -
    MachineProfile XDHyp:\HostingUnits<HostingUnitName>\
    instanceTemplates.folder<TemplateName>.template
<!--NeedCopy-->
```

   Weitere Informationen zum Befehl Set-ProvScheme finden Sie unter https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/MachineCreation/Set-ProvScheme/.

### Katalog mit Shielded VM mit PowerShell erstellen

Sie können einen MCS-Maschinenkatalog mit Shielded VM-Eigenschaften erstellen. Eine abgeschirmte virtuelle Maschine wird durch Sicherheitskontrollen gehärtet, die eine überprüfbare Integrität der Compute Engine-Instanzen über erweiterte Plattformsicherheitsfunktionen wie Sicherer Start, ein virtuelles Trusted Platform Module, UEFI-Firmware und Integritätsüberwachung bieten.

MCS unterstützt die Erstellung des Katalogs mithilfe des Maschinenprofil-Workflows. Wenn Sie den Maschinenprofil-Workflow verwenden, müssen Sie die Shielded VM-Eigenschaften für eine VM-Instanz aktivieren. Sie können diese VM-Instanz dann als Eingabe für das Maschinenprofil verwenden.

MCS-Maschinenkatalog mit Shielded VM mithilfe des Maschinenprofil-Workflows erstellen:

1. Aktivieren Sie die Shielded VM-Optionen für eine VM-Instanz in der Google Cloud-Konsole. Weitere Informationen finden Sie unter Kurzanleitung: Shielded VM-Optionen aktivieren.
2. Erstellen Sie mithilfe der VM-Instanz einen MCS-Maschinenkatalog mit dem Maschinenprofil-Workflow.
    a) Öffnen Sie ein PowerShell-Fenster.
    b) Führen Sie `asnp citrix*` aus, um die Citrix-spezifischen PowerShell-Module zu laden.
    c) Erstellen Sie einen Identitätspool, falls noch nicht vorhanden.
    d) Führen Sie den Befehl `New-ProvScheme` aus. Beispiel:

```
New-ProvScheme -ProvisioningSchemeName <catalog-name>
-HostingUnitName gcp-hostint-unit
-MasterImageVM XDHyp:\HostingUnits\gcp-hostint-unit\catalog-
    vda.vm
-MachineProfile XDHyp:\HostingUnits\gcp-hostint-unit\catalog-
    machine.vm
<!--NeedCopy-->
```

3. Beenden Sie die Erstellung des Maschinenkatalogs.

Maschinenkatalog mit einem neuen Maschinenprofil aktualisieren:

1. Führen Sie den Befehl `Set-ProvScheme` aus. Beispiel:

```
Set-ProvScheme -ProvisioningSchemeName <catalog-name>
-MasterImageVM XDHyp:\HostingUnits<hostin-unit>\catalog-vda.vm
-MachineProfile "DHyp:\HostingUnits<hostin-unit>\catalog-machine.
    vm
<!--NeedCopy-->
```

Führen Sie den Befehl `Set-ProvVMUpdateTimeWindow` aus, um die in `Set-ProvScheme` vorgenommene Änderung auf die vorhandenen VMs anzuwenden.

1. Führen Sie den Befehl `Set-ProvVMUpdateTimeWindow` aus. Beispiel:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -
    VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

2. Starten Sie die VMs neu.

### Windows 11-VMs auf dem Einzelmandantenknoten erstellen

Sie können Windows 11-VMs in GCP erstellen. Wenn Sie jedoch Windows 11 auf dem Masterimage installieren, müssen Sie vTPM während der Erstellung des Masterimages aktivieren. Außerdem müssen Sie vTPM auf der Maschinenprofilquelle (VM oder Instanzvorlage) aktivieren.

Die wichtigsten Schritte zum Erstellen von Windows 11-VMs auf dem Knoten für einzelne Mandanten sind:

1. Richten Sie Google Cloud-Virtualisierungsumgebungen ein. Weitere Informationen finden Sie unter Google Cloud-Umgebungen.
2. Installieren Sie einen VDA. Weitere Informationen finden Sie unter VDAs installieren.
3. Erstellen Sie eine Verbindung zu Google-Cloudumgebungen. Weitere Informationen finden Sie unter Verbindung zu Google-Cloud-Umgebungen.
4. Erstellen Sie ein Windows 11 Bring Your Own License (BYOL) -Masterimage und importieren Sie das Image in Google Cloud. Weitere Informationen finden Sie unter Windows 11 BYOL-Masterimage erstellen.
5. Erstellen Sie die Maschinenprofilquelle: Stellen Sie die VM auf dem Einzelmandantenknoten bereit und aktivieren Sie das vTPM des Quellmaschinenprofils. Weitere Informationen finden Sie unter VM auf einem Einzelmandantenknoten bereitstellen.
6. Erstellen Sie einen MCS-Maschinenkatalog mit der Windows 11-Maschinenprofilquelle, die mit vTPM aktiviert ist. Die Maschinenprofilquelle muss denselben Instanztyp haben, der im Knoten für den Einzelmandanten beschrieben ist. Weitere Informationen finden Sie unter MCS-Maschinenkatalog mit der Windows 11-Maschinenprofilquelle erstellen.

#### Windows 11 BYOL-Masterimage erstellen

Es gibt zwei Optionen, um ein Windows 11 BYOL-Masterimage zu erstellen und das Masterimage in Google Cloud zu importieren:

- Google Cloud Build Tools erstellen
- Masterimage auf einem anderen Hypervisor erstellen

**Google Cloud Build Tools erstellen**

1. Laden Sie die Windows 11-ISO-, GCP SDK-, .NET Framework- und PowerShell-Installationsdateien in den GCP-Speicher-Bucket hoch.
2. Geben Sie den Speicherort der Datei in der `.yaml`-Cloud-Build-Datei als Parameter an.
3. Führen Sie den folgenden Cloud Build über die Befehlszeile aus, um das endgültige Windows 11-Image zu erstellen. GCP bootet und erstellt das Masterimage im ausgewählten Projekt mit dem Daisy-Workflow in GCP. Das Masterimage wird in GCP importiert.

```
gcloud compute instances import INSTANCE-NAME--source-uri=gs://
   BUCKET/IMAGE-OVF-FILE.ovf --guest-os-features=UEFI_COMPATIBLE
   --byol --machine-type=MACHINE-TYPE --zone=ZONE
<!--NeedCopy-->
```

> **Hinweis:**
>
> Ersetzen Sie den gesamten Großbuchstabentext durch die tatsächlichen Ressourcendetails.

Vollständige Informationen finden Sie unter Benutzerdefinierte Windows BYOL-Images erstellen.

**Masterimage auf einem anderen Hypervisor erstellen**

1. Erstellen Sie das Windows 11-Masterimage mit einem anderen Hypervisor.
2. Exportieren Sie das Masterimage in einem OVF-Format auf der lokalen Maschine.
3. Laden Sie die OVF-Dateien über die lokale gcloud-Befehlszeilenschnittstelle in den GCP-Speicherbucket hoch.

```
gsutil cp LOCAL_IMAGE_PATH_OVF_FILES gs://BUCKET_NAME/
<!--NeedCopy-->
```

4. Führen Sie den folgenden Cloud Build über die Befehlszeile aus, um das endgültige Windows 11-Image zu erstellen. GCP bootet und erstellt das Masterimage im ausgewählten Projekt mit dem Daisy-Workflow in GCP. Das Masterimage wird in GCP importiert.

```
gcloud compute instances import INSTANCE-NAME --source-uri=gs://
   BUCKET/IMAGE-OVF-FILE.ovf --guest-os-features=UEFI_COMPATIBLE
   --byol --machine-type=MACHINE-TYPE --zone=ZONE
<!--NeedCopy-->
```

> **Hinweis:**
>
> Ersetzen Sie den gesamten Großbuchstabentext durch die tatsächlichen Ressourcendetails.

#### VM auf einem Einzelmandantenknoten bereitstellen

Verwenden Sie Knoten für einzelne Mandanten, um Ihre VMs physisch von VMs in anderen Projekten zu trennen, oder um Ihre VMs auf derselben Hosthardware zu gruppieren. Informationen zum Einzelmandantenknoten finden Sie im GCP-Dokument Sole-Tenancy Overview.

Informationen zur Bereitstellung einer VM (Maschinenprofilquelle) auf dem Einzelmandantenknoten finden Sie im GCP-Dokument Provisioning VMs on Sole-Tenant Nodes.

> **Hinweis:**
>
> - Wählen Sie denselben Instanztyp und dieselbe Region wie für die Knotengruppe aus.
> - Aktivieren Sie vTPM im Abschnitt Shielded VM. Weitere Informationen finden Sie unter Kurzanleitung: Shielded VM-Optionen aktivieren.
> - Deaktivieren Sie den Bitlocker auf der Quell-VM.

#### MCS-Maschinenkatalog mit der Windows 11-Maschinenprofilquelle erstellen

Sie können einen MCS-Maschinenkatalog erstellen, um Windows 11-VMs mit Web Studio- oder PowerShell-Befehlen zu erstellen.

> **Hinweis:**
>
> - Wählen Sie für das Masterimage den Windows 11-Snapshot oder die VM aus.
> - Wählen Sie für die Maschinenprofilquelle die Windows 11-VM als Maschinenprofil aus. Die Maschinenprofilquelle muss denselben Instanztyp haben, der im Knoten für den Einzelmandanten beschrieben ist.

Informationen zur Verwendung von Web Studio finden Sie unter Maschinenkatalog mit Web Studio erstellen.

Informationen zu PowerShell-Befehlen finden Sie unter Maschinenkatalog mit einem Maschinenprofil erstellen.

Nachdem Sie den Katalog erstellt und die VMs eingeschaltet haben, können Sie sehen, dass die Windows 11-VMs auf dem Einzelmandantenknoten in der Google Cloud-Konsole ausgeführt werden.

### Google Cloud Marketplace

Im **Google Cloud Marketplace** können Sie von Citrix angebotene Images durchsuchen und auswählen, um damit Maschinenkataloge zu erstellen. Derzeit unterstützen die Maschinenerstellungsdienste (MCS) nur den Maschinenprofilworkflow für dieses Feature.

Um über den Google Cloud Marketplace nach einem Citrix VDA-VM-Produkt zu suchen, gehen Sie zu https://console.cloud.google.com/marketplace.

Sie können ein benutzerdefiniertes Image oder ein einsatzbereites Citrix-Image im **Google Cloud Marketplace** verwenden, um das Image eines Maschinenkatalogs zu aktualisieren.

> **Hinweis:**
>
> Wenn das Maschinenprofil keine Angaben zum Speichertyp enthält, wird der Wert aus benutzerdefinierten Eigenschaften abgeleitet.

Die unterstützten Google Cloud Marketplace-Images sind:

- Windows 2019 Einzelsitzung
- Windows 2019 Multisitzung
- Ubuntu

Beispiel für das Erstellen eines Maschinenkatalogs basierend auf einem einsatzbereiten Citrix-Image:

```
New-ProvScheme -ProvisioningSchemeName GCPCatalog \
-HostingUnitName GcpHu -IdentityPoolName gcpPool -CleanOnBoot \
-MasterImageVM XDHyp:\HostingUnits\GcpHu\images.folder\citrix-daas-
   win2019-single-vda-v20220819.publicimage \
-MachineProfile XDHyp:\HostingUnits\GcpHu\Base.vm
<!--NeedCopy-->
```

### So geht es weiter

- Wenn Sie den ersten Katalog erstellen, werden Sie von Web Studio zum Erstellen einer Bereitstellungsgruppe geleitet.
- Informationen zum gesamten Konfigurationsprozess finden Sie unter Installation und Konfiguration
- Informationen zur Verwaltung von Katalogen finden Sie unter Maschinenkataloge verwalten und Google Cloud Platform-Katalog verwalten.

### Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Verbindung zu Google-Cloudumgebungen
- Maschinenkataloge erstellen

# HPE Moonshot-Maschinenkatalog erstellen

June 27, 2024

Unter Maschinenkataloge erstellen werden die Assistenten zum Erstellen eines Maschinenkatalogs beschrieben. Die folgenden Informationen beziehen sich speziell auf HPE Moonshot-Umgebungen.

> **Hinweis:**
>
> - Verbindung zu HPE Moonshot herstellen
> - Vergewissern Sie sich, dass mindestens ein HPE Moonshot-Knoten verfügbar ist, und installieren Sie VDAs auf dem Knoten.
> - Informationen zur Erstellung des ersten HPE Moonshot Cartridge-Images finden Sie im Benutzerhandbuch zur Betriebssystembereitstellung von HP.

Sie können einen HPE Moonshot-Maschinenkatalog unter Verwendung von Folgendem erstellen:

- Web Studio
- PowerShell-Befehle

## Maschinenkatalog mit Web Studio erstellen

Führen Sie im **Assistenten für die Maschinenkatalogerstellung** folgende Schritte aus:

1. Wählen Sie auf der Seite **Betriebssystem** die Option **Einzelsitzungs-OS** oder **Multisitzungs-OS**.
2. Wählen Sie auf der Seite **Maschinenverwaltung** die Option **Maschinen mit Energieverwaltung** und **Anderer Dienst oder andere Technologie**.
3. Fügen Sie auf der Seite **Virtuelle Maschinen** Maschinen und deren Active Directory-Maschinenkonten hinzu. Sie haben folgende Wahl:
   - Klicken Sie auf **Maschinen hinzufügen**, um Maschinen manuell hinzuzufügen. Das Fenster **VMs auswählen** wird angezeigt. Erweitern Sie die HPE Moonshot Chassis-Verbindung, die Sie zuvor erstellt haben, und wählen Sie die Knoten (VMs), die Sie hinzufügen möchten. Fügen Sie dann die zugehörigen Maschinenkontonamen hinzu.
   - Klicken Sie auf **CSV-Datei hinzufügen**, um Maschinen en gros hinzuzufügen. Informationen zur Verwendung von CSV-Dateien zum Hinzufügen von Maschinen finden Sie unter Verwenden von CSV-Dateien zum Massenhinzufügen von Maschinen zu einem Katalog.

Die Seiten **Geltungsbereiche** und **Zusammenfassung** enthalten keine HPE Moonshot-spezifischen Informationen.

### Maschinenkatalog mit PowerShell-Befehlen erstellen

Führen Sie die PowerShell-Befehle `New-BrokerCatalog` und `New-BrokerMachine` aus, um einen Brokerkatalog zu erstellen und Maschinen darin zu importieren.

Beispiel:

```
1 New-BrokerCatalog  -AdminAddress "MyDDC.MyDomain.local" -AdminClientIP
     "103.14.252.249" -AllocationType "Random" -IsRemotePC $False -
     MachinesArePhysical $False -MinimumFunctionalLevel "L7_20" -Name "
     BurMC" -PersistUserChanges "OnLocal" -ProvisioningType "Manual" -
     Scope @() -SessionSupport "MultiSession" -ZoneUid "e166e2cb-25dc
     -4578-bc07-bcf2a82d1463"
2 New-BrokerMachine  -AdminAddress "MyDDC.MyDomain.local" -AdminClientIP
     "103.14.252.249" -CatalogUid 3 -HostedMachineId "c10n1" -
     HypervisorConnectionUid 4 -IsReserved $False -MachineName "S
     -1-5-21-2589939477-3963209805-1860259709-1121"
3 <!--NeedCopy-->
```

### So geht es weiter

- Wenn Sie den ersten Katalog erstellen, werden Sie von Web Studio zum Erstellen einer Bereitstellungsgruppe geleitet.
- Informationen zum gesamten Konfigurationsprozess finden Sie unter Installation und Konfiguration
- Informationen zur Verwaltung von Katalogen finden Sie unter Maschinenkataloge verwalten und HPE Moonshot-Katalog verwalten

### Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Verbindung zu HPE Moonshot
- Maschinenkataloge erstellen

## Microsoft Azure-Katalog erstellen

June 28, 2024

> **Hinweis:**
>
> Seit Juli 2023 hat Microsoft Azure Active Directory (Azure AD) in Microsoft Entra ID umbenannt. In diesem Dokument bezieht sich jeder Verweis auf Azure Active Directory, Azure AD oder AAD jetzt

> auf Microsoft Entra ID.

Unter Maschinenkataloge erstellen werden die Assistenten zum Erstellen eines Maschinenkatalogs beschrieben. Die folgenden Informationen beziehen sich speziell auf Microsoft Azure Resource Manager-Cloudumgebungen.

> **Hinweis:**
>
> Bevor Sie einen Microsoft Azure-Katalog erstellen, müssen Sie eine Verbindung zu Microsoft Azure hergestellt haben. Siehe Verbindung zu Microsoft Azure.

### Maschinenkatalog erstellen

Sie können einen Maschinenkatalog auf zweierlei Art erstellen:

- Maschinenkatalog unter Verwendung eines Azure Resource Manager-Images in Web Studio erstellen
- Maschinenkatalog mit PowerShell erstellen

#### Maschinenkatalog unter Verwendung eines Azure Resource Manager-Images in Web Studio erstellen

Ein Image kann ein Datenträger, ein Snapshot oder eine Imageversion einer Imagedefinition in Azure Compute Gallery sein, das zum Erstellen der VMs in einem Maschinenkatalog verwendet wird. Erstellen Sie vor dem Erstellen des Maschinenkatalogs ein Image in Azure Resource Manager. Allgemeine Informationen über Images finden Sie im Artikel Erstellen von Maschinenkatalogen.

> **Hinweis:**
>
> Die Unterstützung für die Verwendung eines Masterimages aus einer anderen Region als der in der Hostverbindung konfigurierten Region ist veraltet. Verwenden Sie Azure Compute Gallery, um das Masterimage in die gewünschte Region zu replizieren.

Während der Imagevorbereitung wird eine Vorbereitungs-VM basierend auf der ursprünglichen VM erstellt. Diese Vorbereitungs-VM ist vom Netzwerk getrennt. Zum Trennen des Netzwerks von der Vorbereitungs-VM wird eine Netzwerksicherheitsgruppe erstellt, um den gesamten eingehenden und ausgehenden Datenverkehr zu blockieren. Die Netzwerksicherheitsgruppe wird automatisch einmal pro Katalog erstellt. Der Name der Netzwerksicherheitsgruppe lautet `Citrix-Deny-All-a3pgu-GUID`, wobei die GUID nach dem Zufallsprinzip generiert wird. Beispiel: `Citrix-Deny-All-a3pgu-3f161981-28e2-4223-b797-88b04d336dd1`.

Assistent für die Maschinenkatalogerstellung:

- Die Seiten **Maschinentyp** und **Maschinenverwaltung** enthalten keine Azure-spezifischen Informationen. Folgen Sie den Anleitungen im Artikel Maschinenkataloge erstellen.
- Wählen Sie auf der Seite **Image** ein Image aus, das Sie als Vorlage für die Erstellung von Maschinen in diesem Katalog verwenden möchten.

  Wenn Sie **Masterimage** als zu verwendenden Imagetyp auswählen, klicken Sie auf **Image auswählen** und gehen Sie wie folgt vor, um bei Bedarf ein Masterimage auszuwählen:

  1. (Gilt nur für Verbindungen mit innerhalb oder zwischen Mandanten freigegebenen Images) Wählen Sie das Abonnement, in dem sich das Image befindet.
  2. Wählen Sie eine Ressourcengruppe.
  3. Gehen Sie zur Azure-VHD, zur Azure Compute Gallery oder zur Azure-Imageversion. Fügen Sie bei Bedarf einen Hinweis für das ausgewählte Image hinzu.

  Beachten Sie bei der Imageauswahl Folgendes:

  - Vergewissern Sie sich, dass ein Citrix VDA auf dem Image installiert ist.
  - Wenn Sie eine virtuelle Festplatte auswählen, die an eine VM angeschlossen ist, müssen Sie die VM herunterfahren, bevor Sie mit dem nächsten Schritt fortfahren.

  > **Hinweis:**
  >
  > - Das Abonnement, das der Verbindung (Host) entspricht, die die Maschinen im Katalog erstellt hat, ist mit einem grünen Punkt gekennzeichnet. Bei den anderen Abonnements handelt es sich um diejenigen, die die Azure Compute Gallery mit diesem Abonnement teilen. In diesen Abonnements werden nur geteilte Kataloge angezeigt. Informationen zur Konfiguration freigegebener Abonnements finden Sie unter Images innerhalb eines Mandanten freigeben (abonnementübergreifend) und Images mandantenübergreifend freigeben.
  > - Die Verwendung eines Maschinenprofils mit vertrauenswürdigem Start als **Sicherheitstyp** ist obligatorisch, wenn Sie ein Image oder einen Snapshot auswählen, für das bzw. den der vertrauenswürdige Start aktiviert ist. Sie können dann SecureBoot und vTPM aktivieren oder deaktivieren, indem Sie die zugehörigen Werte im Maschinenprofil angeben. Der vertrauenswürdige Start wird für Shared Image Gallery nicht unterstützt. Informationen zu vertrauenswürdigen Starts in Azure finden Sie unter https://docs.microsoft.com/en-us/azure/virtual-machines/trusted-launch.
  > - Sie können ein Provisioningschema mit einem kurzlebigen Betriebssystemdatenträger unter Windows mit vertrauenswürdigem Start erstellen. Wenn Sie ein Image mit vertrauenswürdigem Start auswählen, müssen Sie ein Maschinenprofil mit vertrauenswürdigem Start auswählen, das mit vTPM aktiviert ist. Informationen zum Erstellen von Maschinenkatalogen mit kurzlebigem Betriebssystemdatenträger finden Sie unter Erstellen von Maschinen mit kurzlebigem Betriebssystemdaten-

> träger.
> - Während der Imagereplikation können Sie das Image als Masterimage auswählen und das Setup abschließen. Die Katalogerstellung kann jedoch länger dauern, während das Image repliziert wird. MCS erfordert, dass die Replikation innerhalb einer Stunde ab Katalogerstellung abgeschlossen ist. Tritt bei der Replikation ein Timeout auf, schlägt die Katalogerstellung fehl. Sie können den Replikationsstatus in Azure überprüfen. Versuchen Sie es erneut, wenn die Replikation noch aussteht oder nach dem Abschluss der Replikation.
> - Wenn Sie ein Masterimage für Maschinenkataloge in Azure auswählen, bestimmt MCS den Betriebssystemtyp basierend auf dem von Ihnen ausgewählten Masterimage und Maschinenprofil. Wenn MCS den Betriebssystemtyp nicht bestimmen kann, wählen Sie den Betriebssystemtyp aus, der dem Masterimage entspricht.
> - Sie können einen VM-Katalog der zweiten Generation mithilfe eines Images der zweiten Generation bereitstellen, um die Startzeitleistung zu verbessern. Das Erstellen eines Maschinenkatalogs der zweiten Generation mit einem Image der ersten Generation wird nicht unterstützt. Das Erstellen eines Maschinenkatalogs der ersten Generation mit einem Image der zweiten Generation wird ebenfalls nicht unterstützt. Außerdem werden ältere Images ohne Generationsangabe als Image der ersten Generation behandelt.

Wenn Sie **Vorbereitetes Image** als zu verwendenden Imagetyp auswählen, klicken Sie auf **Image auswählen** und wählen Sie bei Bedarf ein vorbereitetes Image aus.

Um eine erfolgreiche VM-Erstellung sicherzustellen, vergewissern Sie sich, dass auf dem Image Citrix VDA 2311 oder höher installiert ist MCSIO auf dem VDA vorhanden ist.

Sobald Sie ein Image ausgewählt haben, wird das Kontrollkästchen **Maschinenprofil verwenden (für Azure Active Directory erforderlich)** automatisch aktiviert. Klicken Sie auf **Wählen Sie ein Maschinenprofil**, um eine VM- oder ARM-Vorlagenspezifikation aus einer Liste mit Ressourcengruppen auszuwählen. Virtuelle Maschinen im Katalog können folgende Konfigurationen vom ausgewählten Maschinenprofil übernehmen:

Validieren Sie die ARM-Vorlagenspezifikation, um sicherzustellen, dass sie als Maschinenprofil zum Erstellen eines Maschinenkatalogs verwendet werden kann. Es gibt zwei Möglichkeiten zur Validierung der ARM-Vorlagenspezifikation:

- Klicken Sie nach Auswahl der ARM-Vorlagenspezifikation aus der Liste der Ressourcengruppen auf **Weiter**. Wenn die ARM-Vorlagenspezifikation Fehler enthält, werden Fehlermeldungen angezeigt,
- Führen Sie einen der folgenden PowerShell-Befehle aus:
  * `Test-ProvInventoryItem -HostingUnitName <string> -InventoryPath <string>`

```
* Test-ProvInventoryItem -HostingUnitUid <Guid> -InventoryPath
  <string>
```

Beispiele für Konfigurationen, die VMs von einem Maschinenprofil übernehmen können:

- Beschleunigtes Netzwerk
- Startdiagnose
- Caching des Hostdatenträgers (bei OS- und MCSIO-Datenträgern)
- Maschinengröße (sofern nicht anders angegeben)
- Für VM platzierte Tags

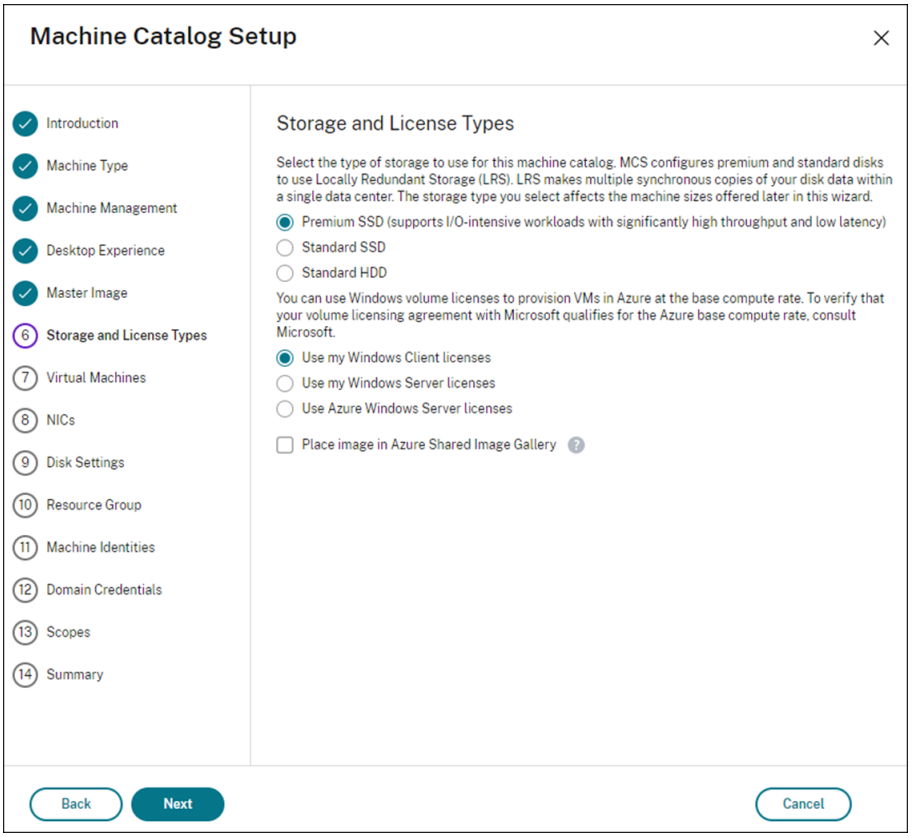
Nachdem Sie den Katalog erstellt haben, können Sie die Konfigurationen anzeigen, die das Image vom Maschinenprofil erbt. Wählen Sie auf dem Knoten **Maschinenkataloge** den Katalog aus, um die Details im unteren Bereich anzuzeigen. Klicken Sie dann auf die Registerkarte **Vorlageneigenschaften**, um die Eigenschaften des Maschinenprofils anzuzeigen. Im Abschnitt **Tags** werden bis zu drei Tags angezeigt. Zum Anzeigen aller auf der VM platzierten Tags klicken Sie auf **Alle anzeigen**.

Um VMs mit Maschinenerstellungsdiensten (MCS) auf einem dedizierten Azure-Host bereitzustellen, aktivieren Sie das Kontrollkästchen **Dedizierte Hostgruppe verwenden** und wählen dann eine Hostgruppe aus der Liste aus. Eine Hostgruppe ist eine Ressource, die eine Sammlung dedizierter Hosts darstellt. Ein dedizierter Host ist ein Dienst, der physische Server bereitstellt, die eine oder mehrere virtuelle Maschinen hosten. Ihr Server ist für Ihr Azure-Abonnement reserviert und wird nicht mit anderen Abonnenten geteilt. Bei Verwendung eines dedizierten Hosts stellt Azure sicher, dass nur Ihre VMs auf diesem Host ausgeführt werden. Dieses Feature eignet sich für Szenarios, in denen Sie regulatorische oder interne Sicherheitsanforderungen erfüllen müssen. Weitere Informationen zu Hostgruppen und Überlegungen zu ihrer Verwendung finden Sie unter Dedizierte Azure-Hosts.

> **Wichtig:**
>
> - Es werden nur Hostgruppen mit aktivierter automatischer Azure-Platzierung angezeigt.
> - Durch Verwendung einer Hostgruppe wird die Seite **Virtuelle Maschinen** geändert, die später im Assistenten angezeigt wird. Auf dieser Seite werden nur die Maschinengrößen angezeigt, die in der ausgewählten Hostgruppe enthalten sind. Außerdem sind Verfügbarkeitszonen automatisch ausgewählt und nicht wählbar.

- Die Seite **Speicher- und Lizenztypen** wird nur angezeigt, wenn Sie ein Azure Resource Manager-Image verwenden.

Seite 


Für den Maschinenkatalog können Sie die folgenden Speichertypen verwenden:

- **Premium-SSD.** Bietet Datenträgerspeicherung mit hoher Leistung und niedriger Latenz für VMs mit E/A-intensiven Workloads.
- **Standard-SSD.** Kostengünstige Speicheroption, die für Workloads geeignet ist, die eine gleichmäßige Leistung bei niedrigeren IOPS-Raten erfordern.
- **Standard-HDD.** Zuverlässiger, kostengünstiger Datenträgerspeicher, der für VMs mit latenzunempfindlichen Workloads geeignet ist.
- **Kurzlebiger Azure-Betriebsystemdatenträger**. Kostengünstige Speicheroption mit Wiederverwendung des lokalen VM-Datenträgers zum Hosten des Betriebssystemdatenträgers. Alternativ können Sie mit PowerShell Maschinen mit kurzlebigen Betriebsystemdatenträgern erstellen. Weitere Informationen finden Sie unter Kurzlebige Azure-Datenträger. Beachten Sie bei der Verwendung kurzlebiger Betriebssystemdatenträger Folgendes:
  - Kurzlebige Azure-Betriebssystemdatenträger und MCS-E/A können nicht gleichzeitig aktiviert werden.
  - Zum Aktualisieren von Maschinen, die kurzlebige Betriebssystemdatenträger verwenden, müssen Sie ein Image auswählen, dessen Größe die des Cachedatenträgers bzw. des temporären Datenträgers der VM nicht übersteigt.
  - Sie können die später im Assistenten angebotene Option **VM und Systemdatenträger**

**während Energiezyklen beibehalten** nicht verwenden.

> **Hinweis:**
>
> Der Identitätsdatenträger wird unabhängig vom gewählten Speichertyp immer mit Standard-SSD erstellt.

Der gewählte Speichertyp bestimmt, welche Maschinengrößen auf der Seite **Virtuelle Maschinen** des Assistenten angeboten werden. MCS konfiguriert Premium- und Standarddatenträger für die Verwendung von lokal redundantem Speicher (LRS). LRS erstellt mehrere synchrone Kopien Ihrer Daten in einem Datencenter. Bei kurzlebigen Azure-Betriebssystemdatenträgern wird das Betriebssystem auf dem lokalen VM-Datenträger gespeichert. 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 Windows- oder Linux-Lizenzen verwendet werden sollen.

- Windows-Lizenzen: Mit Windows-Lizenzen und Windows-Images (Azure- oder benutzerdefinierte Images) können Sie Windows-VMs in Azure zu geringeren Kosten ausführen. Es gibt zwei Arten von Lizenzen:
  - **Windows Server-Lizenz**. Ermöglicht die Verwendung Ihrer Windows Server- oder Azure Windows Server-Lizenzen und somit die Nutzung des Azure-Hybridvorteils. Einzelheiten finden Sie unter https://azure.microsoft.com/en-us/pricing/hybrid-benefit/. Der Azure-Hybridvorteil senkt die Kosten des Ausführens von VMs in Azure auf die Grundgebühr für Computekapazität, da keine Gebühren für zusätzliche Windows Server-Lizenzen aus dem Azure-Katalog erhoben werden.
  - **Windows-Clientlizenz**. Ermöglicht die Verwendung Ihrer Windows 10- und Windows 11-Lizenzen in Azure und somit die Ausführung von Windows 10- und Windows 11-VMs in Azure ohne Erfordernis zusätzlicher Lizenzen. Weitere Informationen finden Sie unter Clientzugriffslizenzen und Verwaltungslizenzen.

Sie können mit folgendem PowerShell-Befehl überprüfen, ob eine VM den Lizenzierungsvorteil nutzt: `Get-AzVM -ResourceGroup MyResourceGroup -Name MyVM`.

- Bei Windows Server-Lizenzen muss der Lizenztyp **Windows_Server** sein. Weitere Anweisungen finden Sie unter https://docs.microsoft.com/en-us/azure/virtual-machines/windows/hybrid-use-benefit-licensing/.

- Bei Windows-Clientlizenzen muss der Lizenztyp **Windows_Client** sein. Weitere Anweisungen finden Sie unter https://docs.microsoft.com/en-us/azure/virtual-machines/windows/windows-desktop-multitenant-hosting-deployment/.

Alternativ können Sie zur Überprüfung das PowerShell-SDK `Get-Provscheme` verwenden. Beispiel: `Get-Provscheme -ProvisioningSchemeName "My Azure Catalog"`. Weitere Informationen zu diesem Cmdlet finden Sie unter https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Get-ProvScheme/.

- Linux-Lizenzen: Bei Verwendung eigener Linux-Lizenzen (Bring Your Own Subscription oder BYOS) müssen Sie für die Software nicht zahlen. Die BYOS-Gebühr umfasst nur die Hardware für die Rechenleistung. Es gibt zwei Arten von Lizenzen:
  * **RHEL_BYOS**: Um den Typ RHEL_BYOS zu verwenden, aktivieren Sie Red Hat Cloud Access in Ihrem Azure-Abonnement.
  * **SLES_BYOS**: Die BYOS-Versionen von SLES beinhalten Unterstützung von SUSE.

  Sie können den LicenseType-Wert unter `New-ProvScheme` und `Set-ProvScheme` auf Linux-Optionen setzen.

  Beispiel für das Festlegen von LicenseType auf RHEL_BYOS unter `New-ProvScheme`:

```
1 New-ProvScheme -CleanOnBoot -ProvisioningSchemeName "
    azureCatalog" -RunAsynchronously -Scope @() -SecurityGroup
    @() -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="StandardSSD_LRS" /><Property xsi:type="
    StringProperty" Name="ResourceGroups" Value="hu-dev-mcs"
    /><Property xsi:type="StringProperty" Name="OsType" Value="
    Linux" /><Property xsi:type="StringProperty" Name="
    LicenseType" Value="RHEL_BYOS" /></CustomProperties>'
2 <!--NeedCopy-->
```

  Beispiel für das Festlegen von LicenseType auf SLES_BYOS unter `Set-ProvScheme`:

```
1 Set-ProvScheme -ProvisioningSchemeName "azureCatalog" -
    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="StandardSSD_LRS" /><Property xsi:type="
    StringProperty" Name="ResourceGroups" Value="hu-dev-mcs"
    /><Property xsi:type="StringProperty" Name="OsType" Value="
    Linux" /><Property xsi:type="StringProperty" Name="
    LicenseType" Value="SLES_BYOS" /></CustomProperties>'
2 <!--NeedCopy-->
```

> **Hinweis:**
>
> Wenn der Wert `LicenseType` leer ist, werden als Standardwert die Azure Windows-Serverlizenz oder Azure Linux-Lizenz verwendet, abhängig vom OsType-Wert.

Beispiel für einen leeren Wert für LicenseType:

```
Set-ProvScheme -ProvisioningSchemeName "azureCatalog" -
    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="StandardSSD_LRS" /><Property xsi:type="
    StringProperty" Name="ResourceGroups" Value="hu-dev-mcs"
    /><Property xsi:type="StringProperty" Name="OsType" Value="
    Linux" /></CustomProperties>'
<!--NeedCopy-->
```

Lesen Sie die folgenden Dokumente, um mehr über Lizenztypen und ihre Vorteile zu erfahren:

- https://docs.microsoft.com/en-us/dotnet/api/microsoft.azure.management.compute.models.virtualmachine.licensetype?view=azure-dotnet
- https://docs.microsoft.com/en-us/azure/virtual-machines/linux/azure-hybrid-benefit-linux

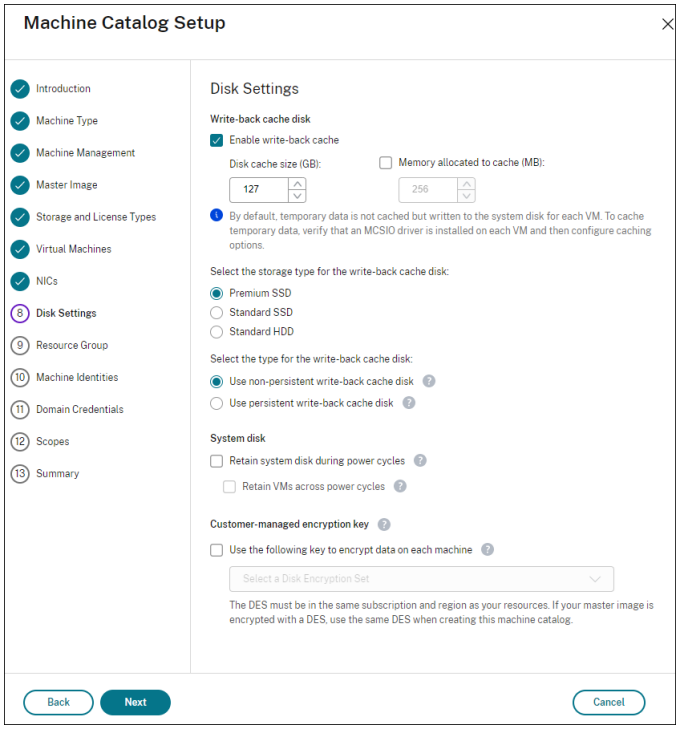
Azure Compute Gallery (früher Azure Shared Image Gallery) ist ein Repository zum Verwalten und Freigeben von Images. Damit können Sie Images in Ihrer gesamten Organisation verfügbar machen. Wir empfehlen Ihnen, beim Erstellen großer nicht-persistenter Maschinenkataloge ein Image in SIG zu speichern, da sich VDA-Betriebssystemdatenträger dadurch schneller zurücksetzen lassen. Nachdem Sie **Vorbereitetes Image in der Azure Compute Gallery platzieren** ausgewählt haben, wird der Abschnitt **Azure Compute Gallery-Einstellungen** angezeigt, in dem Sie weitere Azure Compute Gallery-Einstellungen angeben können:

- **Verhältnis von virtuellen Maschinen zu Imagereplikaten**. Hier können Sie das Verhältnis von virtuellen Maschinen zu Imagereplikaten angeben, die Azure beibehalten soll. Standardmäßig speichert Azure ein Imagereplikat pro 40 nicht-persistente Maschinen. Bei persistenten Maschinen ist diese Zahl voreingestellt auf 1000.
- **Maximale Replikate**. Hier können Sie die maximale Anzahl von Image-Replikaten angeben, die Azure speichern soll. Der Standardwert ist 10.

- Geben Sie auf der Seite **VMs** an, wie viele VMs Sie erstellen möchten. Sie müssen mindestens eine VM angeben und eine Maschinengröße auswählen. Nach der Katalogerstellung können Sie die Maschinengröße durch Bearbeiten des Katalogs ändern.

- Die Seite **Netzwerkkarten** enthält keine Azure-spezifischen Informationen. Folgen Sie den Anleitungen im Artikel Maschinenkataloge erstellen.
- Wählen Sie auf der Seite **Datenträgereinstellungen**, ob der Zurückschreibcache aktiviert werden soll. Wenn die MCS-Speicheroptimierung aktiviert ist, können Sie beim Erstellen eines Katalogs folgende Einstellungen konfigurieren. Diese Einstellungen gelten für Azure- und für GCP-Umgebungen.




Nach dem Aktivieren des Zurückschreibcache können Sie Folgendes tun:

- Konfigurieren Sie die Größe des Datenträgers und des RAM, die zum Zwischenspeichern temporärer Daten verwendet werden. Weitere Informationen finden Sie unter Konfigurieren eines Cache für temporäre Daten.
- Wählen des Speichertyps für den Datenträger für den Zurückschreibcache. Die folgenden Speichertypen stehen für den Zurückschreibcache-Datenträger zur Verfügung:
  - Premium-SSD
  - Standard-SSD
  - Standard-HDD
- Wählen eines persistenten Datenträgers für den Zurückschreibcache für die bereitgestellten VMs (bei Bedarf). Wählen Sie **Zurückschreibcache aktivieren**, um die Optionen verfügbar zu machen. Die Standardeinstellung ist **Nicht-persistenten Datenträger für Zurückschreibcache verwenden**.
- Wählen Sie einen Datenträgertyp für den Zurückschreibcache aus.

  - **Nicht-persistenten Datenträger für Zurückschreibcache verwenden**. Wenn diese Option ausgewählt ist, wird der Datenträger für den Zurückschreibcache während Energiezyklen gelöscht. Alle darauf umgeleitete Daten gehen verloren. Wenn auf dem temporären Datenträger der VM ausreichend Speicherplatz vorhanden ist, wird er als Host für den Zurückschreibcachedatenträger verwendet, da dies Ihre Kosten reduziert. Nach der Katalogerstellung können Sie überprüfen, ob die bereitgestellten Maschinen den temporären Datenträger verwenden. Klicken Sie dazu auf den Katalog und überprüfen Sie die Informationen auf der Registerkarte **Vorlageneigenschaften**. Bei Verwendung des temporären Datenträgers wird für **Nicht-persistenter Datenträger für Zurückschreibcache** der Wert **Ja (mit dem temporären Datenträger der VM)** angezeigt. Wenn er nicht verwendet wird, wird für **Nicht-persistenter Datenträger für Zurückschreibcache** der Wert **Nein (nicht mit dem temporären Datenträger der VM)** angezeigt.
  - **Persistenter Datenträger für Zurückschreibcache.** Wenn diese Option ausgewählt ist, wird der Zurückschreibcache-Datenträger für die bereitgestellten VMs beibehalten. Die Aktivierung dieser Option erhöht die Speicherkosten.

- Wählen Sie aus, ob VMs und Systemdatenträger für VDAs bei Energiezyklen beibehalten werden sollen.

  **VM und Systemdatenträger während Neustarts beibehalten**. Verfügbar, wenn Sie **Zurückschreibcache aktivieren** ausgewählt haben. Standardmäßig werden VMs und die Systemdatenträger beim Herunterfahren gelöscht und beim Starten neu erstellt. Wenn Sie die VM-Neustartzeiten reduzieren möchten, wählen Sie diese Option. Allerdings erhöht die Aktivierung dieser Option auch die Speicherkosten.

- Wählen Sie aus, ob Sie **Einsparung von Speicherkosten** aktivieren möchten. Wenn diese Option aktiviert ist, wird der Speicherdatenträger beim Herunterfahren der VM auf Standard-HDD herabgestuft, um Speicherkosten zu senken. Beim Neustart wechselt die VM wieder zu den ursprünglichen Einstellungen. Die Option lässt sich auf Speicher- und Zurückschreibcache-Datenträger anwenden. Alternativ können Sie auch PowerShell verwenden. Siehe Speichertyp beim Herunterfahren einer VM zu einer niedrigeren Ebene ändern.

  > **Hinweis:**
  >
  > Bei Microsoft gelten Einschränkungen für die Änderung des Speichertyps beim Herunterfahren einer VM. Es ist auch möglich, dass Microsoft künftig Änderungen des Speichertyps blockiert. Weitere Informationen finden Sie in diesem Microsoft-Artikel.

- Wählen Sie aus, ob Daten auf den im Katalog bereitgestellten Maschinen verschlüsselt werden sollen. Die serverseitige Verschlüsselung mit einem vom Kunden verwalteten Schlüssel ermöglicht die Verwaltung der Verschlüsselung auf der Ebene verwalteter Datenträger

und das Schützen von Daten auf den Maschinen im Katalog. Weitere Informationen finden Sie unter Azure-serverseitige Verschlüsselung.

- Wählen Sie auf der Seite **Ressourcengruppe** aus, ob Sie neue Ressourcengruppen erstellen oder vorhandene verwenden.
  - Wenn Sie Ressourcengruppen erstellen möchten, wählen Sie **Weiter**.
  - Wenn Sie vorhandene Ressourcengruppen verwenden möchten, wählen Sie Gruppen in der Liste **Zum Bereitstellen verfügbare Ressourcengruppen** aus. **Nicht vergessen:** Wählen Sie genügend Gruppen aus, um die Maschinen aufzunehmen, die Sie im Katalog erstellen. Wenn sie nicht ausreichen, werden Sie in einer Meldung darauf hingewiesen. 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.

- Wählen Sie auf der Seite **Maschinenidentitäten** einen Identitätstyp und konfigurieren Sie Identitäten für Maschinen in dem Katalog. Wenn Sie die VMs als **In Azure Active Directory eingebunden** festlegen, können Sie sie zu einer Azure AD-Sicherheitsgruppe hinzufügen. Verfahren:

  1. Wählen Sie im Feld **Identitätstyp** die Option **In Azure Active Directory eingebunden**. Die Option **Azure AD-Sicherheitsgruppe (optional)** wird angezeigt.
  2. Klicken Sie auf **Azure AD-Sicherheitsgruppe: Neu erstellen**.
  3. Geben Sie einen Gruppennamen ein und klicken Sie auf **Erstellen**.
  4. Folgen Sie den angezeigten Anweisungen, um sich bei Azure anzumelden.
     Wenn der Gruppenname in Azure nicht vorliegt, erscheint ein grünes Symbol. Andernfalls erscheint eine Fehlermeldung, in der Sie aufgefordert werden, einen neuen Namen einzugeben.
  5. Geben Sie das Benennungsschema für Maschinenkonten für die VMs ein.

  Nach der Katalogerstellung greift Citrix Virtual Apps and Desktops für Sie auf Azure zu und erstellt die Sicherheitsgruppe und eine dynamische Mitgliedschaftsregel für die Gruppe. Basierend auf der Regel werden virtuelle Maschinen mit dem in diesem Katalog angegebenen Benennungsschema automatisch zur Sicherheitsgruppe hinzugefügt.

  Um dem Katalog virtuelle Maschinen mit einem anderen Benennungsschema hinzuzufügen, müssen Sie sich bei Azure anmelden. Citrix Virtual Apps and Desktops kann dann auf Azure zugreifen und eine dynamische Mitgliedschaftsregel erstellen, die auf dem neuen Benennungsschema basiert.

  Beim Löschen des Katalogs ist für das Löschen der Sicherheitsgruppe aus Azure ebenfalls eine Anmeldung bei Azure erforderlich.

- Die Seiten **Domänenanmeldeinformationen** und **Zusammenfassung** enthalten keine Azure-spezifischen Informationen. Folgen Sie den Anleitungen im Artikel Maschinenkataloge erstellen.

Schließen Sie den Assistenten ab.

### Bedingungen für die Verwendung eines temporären Azure-Datenträgers als Datenträger für den Zurückschreibcache

Sie können den temporären Azure-Datenträger nur dann als Datenträger für den Zurückschreibcache verwenden, wenn alle der folgenden Bedingungen erfüllt sind:

- Der Datenträger für den Zurückschreibcache darf nicht persistent sein, da der temporäre Azure-Datenträger nicht für persistente Daten geeignet ist.
- Die gewählte Azure-VM-Größe muss einen temporären Datenträger einschließen.
- Der kurzlebige Betriebsystemdatenträger muss nicht aktiviert sein.
- Stimmen Sie zu, dass die Datenträgerdatei für den Zurückschreibcache auf dem temporären Azure-Datenträger platziert wird.
- Der temporäre Azure-Datenträger muss größer sein als der Gesamtwert für (Größe des Datenträgers des Zurückschreibecache + reservierter Speicherplatz für Auslagerungsdatei + 1 GB Pufferspeicher).

### Szenarios mit nicht persistentem Datenträger für den Zurückschreibcache

Die folgende Tabelle enthält drei Szenarios, in denen beim Erstellen des Maschinenkatalogs der temporäre Datenträger für den Zurückschreibcache (WBC) verwendet wird.

| Szenario | Ergebnis |
|---|---|
| Alle Bedingungen zur Verwendung des temporären Datenträgers für den Zurückschreibcache sind erfüllt. | Die WBC-Datei `mcsdif.vhdx` wird auf dem temporären Datenträger abgelegt. |
| Der temporäre Datenträger hat nicht genügend Speicherplatz für den Zurückschreibcache. | Der VHD-Datenträger `MCSWCDisk` wird erstellt und die WBC-Datei `mcsdif.vhdx` wird auf diesem Datenträger abgelegt. |
| Der temporäre Datenträger hat genügend Speicherplatz für den Zurückschreibcache, `UseTempDiskForWBC` ist jedoch auf **False** gesetzt. | Der VHD-Datenträger `MCSWCDisk` wird erstellt und die WBC-Datei `mcsdif.vhdx` wird auf diesem Datenträger abgelegt. |

### Azure-Vorlagenspezifikation erstellen

Sie können eine Azure-Vorlagenspezifikation im Azure-Portal erstellen und sie in Web Studio und in den PowerShell-Befehlen verwenden, um einen MCS-Maschinenkatalog zu erstellen oder zu aktualisieren.

Azure-Vorlagenspezifikation für eine vorhandene VM erstellen:

1. Gehen Sie zum Azure-Portal. Wählen Sie eine Ressourcengruppe und dann die VM und die Netzwerkschnittstelle aus. Klicken Sie oben im Menü **...** auf **Export template**.
2. Deaktivieren Sie das Kontrollkästchen **Include parameters**, wenn Sie eine Vorlagenspezifikation für die Katalogbereitstellung erstellen möchten.
3. Klicken Sie auf **Add to library**, um die Vorlagenspezifikation später zu ändern.
4. Geben Sie auf der Seite **Importing template** die erforderlichen Informationen wie **Name**, **Subscription**, **Subscription**, **Location** und **Version** ein. Klicken Sie auf **Next: Edit Template**.
5. Sie benötigen außerdem eine Netzwerkschnittstelle als unabhängige Ressource, wenn Sie Kataloge bereitstellen möchten. Daher müssen Sie alle `dependsOn`-Elemente in der Vorlagenspezifikation entfernen. Beispiel:

```
"dependsOn": [
"[resourceId('Microsoft.Network/networkInterfaces', 'tnic937')]"
],
<!--NeedCopy-->
```

6. Wählen Sie **Review + Create** und erstellen Sie die Vorlagenspezifikation.
7. Überprüfen Sie auf der Seite **Template Specs** die gerade erstellte Vorlagenspezifikation. Klicken Sie auf die Vorlagenspezifikation. Klicken Sie im linken Bereich auf **Versions**.
8. Sie können eine neue Version erstellen, indem Sie auf **Create new version** klicken. Geben Sie eine neue Versionsnummer an, nehmen Sie Änderungen an der aktuellen Vorlagenspezifikation vor und klicken Sie auf **Review + Create**, um die neue Version der Vorlagenspezifikation zu erstellen.

Mit den folgenden PowerShell-Befehlen können Sie Informationen zur Vorlagenspezifikation und Vorlagenversion abrufen:

- Um Informationen über die Vorlagenspezifikation zu erhalten, führen Sie folgenden Befehl aus:

```
get-item XDHyp:\HostingUnits\East\machineprofile.folder\abc.
   resourcegroup\bggTemplateSpec.templatespec
<!--NeedCopy-->
```

- Um Informationen über die Version der Vorlagenspezifikation zu erhalten, führen Sie folgenden Befehl aus:

```
get-item XDHyp:\HostingUnits\East\machineprofile.folder\abc.
    resourcegroup\bggTemplateSpec.templatespec\bgg1.0.
    templatespecversion
<!--NeedCopy-->
```

### Vorlagenspezifikation beim Erstellen oder Aktualisieren eines Katalogs verwenden

Sie können einen MCS-Maschinenkatalog erstellen oder aktualisieren, indem Sie eine Vorlagenspezifikation als Eingabe für das Maschinenprofil verwenden. Hierfür können Sie Web Studio oder PowerShell-Befehle verwenden.

- Verwendung von Web Studio: Siehe Maschinenkatalog unter Verwendung eines Azure Resource Manager-Images in Web Studio erstellen.
- Verwendung von PowerShell: Siehe Vorlagenspezifikation beim Erstellen oder Aktualisieren eines Katalogs mit PowerShell verwenden.

### Azure-serverseitige Verschlüsselung

Citrix Virtual Apps and Desktops unterstützt vom Kunden verwaltete Schlüssel für verwaltete Azure-Datenträger über Azure Key Vault. Mit dieser Unterstützung können Sie Ihre Unternehmens- und Compliance-Anforderungen verwalten, indem Sie die verwalteten Datenträger des Maschinenkatalogs mit Ihrem eigenen Schlüssel verschlüsseln. Weitere Informationen finden Sie unter Serverseitige Verschlüsselung von Azure Disk Storage.

Bei Verwendung dieses Features für verwaltete Datenträger gilt Folgendes:

- Um den Schlüssel zu ändern, mit dem ein Datenträger verschlüsselt ist, ändern Sie den aktuellen Schlüssel im `DiskEncryptionSet`. Alle dem `DiskEncryptionSet` zugeordneten Ressourcen werden dann mit dem neuen Schlüssel verschlüsselt.
- Wenn Sie den Schlüssel deaktivieren oder löschen, werden alle VMs mit Datenträgern, die den Schlüssel verwenden, automatisch heruntergefahren. Nach dem Herunterfahren können die VMs erst wieder verwendet werden, wenn Sie den Schlüssel wieder aktivieren oder einen neuen Schlüssel zuweisen. Kataloge, die den Schlüssel verwenden, können nicht aktiviert werden und Sie können solchen Katalogen keine VMs hinzufügen.

#### Wichtige Überlegungen bei der Verwendung vom Kunden verwalteter Schlüssel

Beachten Sie die folgenden Punkte bei der Verwendung dieses Features:

- Alle zu von Kunden verwalteten Schlüsseln gehörenden Ressourcen (Azure Key Vaults, Datenträgerverschlüsselungssätze, VMs, Datenträger und Snapshots) müssen demselben Abonnement und derselben Region angehören.
- Ein einmal aktivierter kundenverwalteter Schlüssel kann nicht mehr deaktiviert werden. Wenn Sie einen kundenverwalteten Schlüssel deaktivieren oder entfernen möchten, kopieren Sie alle Daten auf einen anderen verwalteten Datenträger, für den der Schlüssel nicht verwendet wird.
- Datenträger, die aus verschlüsselten benutzerdefinierten Images mit serverseitiger Verschlüsselung und einem kundenverwalteten Schlüssel erstellt wurden, müssen mit demselben kundenverwalteten Schlüssel verschlüsselt werden. Diese Datenträger müssen im selben Abonnement sein.
- Snapshots von Datenträgern, die mit serverseitiger Verschlüsselung und einem kundenverwalteten Schlüssel verschlüsselt wurden, müssen mit demselben kundenverwalteten Schlüssel verschlüsselt werden.
- Datenträger, Snapshots und Images, die mit kundenverwalteten Schlüsseln verschlüsselt wurden, können nicht in anderen Ressourcengruppen oder Abonnements verschoben werden.
- Verwaltete Datenträger, die mit Azure Disk Encryption verschlüsselt sind oder es zuvor einmal waren, können nicht mit kundenverwalteten Schlüsseln verschlüsselt werden.
- Auf der Microsoft-Website finden Sie Informationen zu Limits für Datenträgerverschlüsselungssätze pro Region.

> **Hinweis:**
>
> Weitere Informationen zum Konfigurieren der Azure-serverseitigen Verschlüsselung finden Sie unter Schnellstart: Key Vault-Erstellung mit dem Azure-Portal .

### Vom Kunden verwalteter Schlüssel für Azure

Beim Erstellen eines Maschinenkatalogs können Sie wählen, ob Daten auf den im Katalog bereitzustellenden Maschinen verschlüsselt werden sollen. Die serverseitige Verschlüsselung mit einem vom Kunden verwalteten Schlüssel ermöglicht die Verwaltung der Verschlüsselung auf der Ebene verwalteter Datenträger und das Schützen von Daten auf den Maschinen im Katalog. Ein Datenträgerverschlüsselungssatz (DES) repräsentiert einen vom Kunden verwalteten Schlüssel. Um das Feature zu nutzen, müssen Sie zuerst einen DES in Azure erstellen. Ein DES hat folgendes Format:

- `/subscriptions/12345678-1234-1234-1234-123456789012/resourceGroups/Sample-RG/providers/Microsoft.Compute/diskEncryptionSets/SampleEncryption`

Wählen Sie einen DES aus der Liste aus. Der ausgewählte DES muss sich im selben Abonnement und in derselben Region wie Ihre Ressourcen befinden. Wenn Ihr Image mit einem DES verschlüsselt ist, verwenden Sie beim Erstellen des Maschinenkatalogs denselben DES. Sie können den DES nicht mehr ändern, wenn Sie den Katalog erstellt haben.

Wenn Sie einen Katalog mit einem Schlüssel erstellen und später den entsprechenden DES in Azure deaktivieren, können Sie die Maschinen im Katalog nicht mehr einschalten und diesem keine Maschinen mehr hinzufügen.

Weitere Informationen finden Sie unter Creating a machine catalog using customer-managed key.

### Azure-Datenträgerverschlüsselung auf dem Host

Sie können einen MCS-Maschinenkatalog mit Verschlüsselung auf dem Host erstellen. Derzeit unterstützen die Maschinenerstellungsdienste (MCS) nur den Maschinenprofilworkflow für dieses Feature. Sie können eine VM oder eine Vorlagenspezifikation als Eingabe für ein Maschinenprofil verwenden.

Bei diesem Verschlüsselungsverfahren werden Daten nicht über den Azure-Speicher verschlüsselt. Die Daten werden auf dem Hostserver verschlüsselt und dann verschlüsselt durch den Azure-Speicherserver geleitet. Es kommt also zu einer End-to-End-Verschlüsselung der Daten.

**Einschränkungen:**

Die Azure-Datenträgerverschlüsselung auf dem Host:

- wird nicht für alle Azure-Maschinengrößen unterstützt.
- ist nicht kompatibel mit der Azure-Datenträgerverschlüsselung.

Erstellen eines Maschinenkatalogs mit Verschlüsselung auf dem Host:

1. Prüfen Sie, ob die Verschlüsselung auf dem Host für Ihr Abonnement aktiviert ist. Weitere Informationen hierzu finden Sie unter https://learn.microsoft.com/en-us/rest/api/resources/features/get?tabs=HTTP/. Wenn das Feature nicht aktiviert ist, müssen Sie es für das Abonnement aktivieren. Informationen zur Aktivierung des Features für Ihr Abonnement finden Sie unter https://learn.microsoft.com/en-us/azure/virtual-machines/disks-enable-host-based-encryption-portal?tabs=azure-powershell#prerequisites/.
2. Prüfen Sie, ob die Verschlüsselung auf dem Host für die vorliegende Azure-VM-Größe unterstützt wird. Führen Sie dazu in einem PowerShell-Fenster einen der folgenden Befehle aus:

```
PS XDHyp:\Connections<your connection>\east us.region\
   serviceoffering.folder>
<!--NeedCopy-->
```

```
PS XDHyp:\HostingUnits<your hosting unit>\serviceoffering.folder>
<!--NeedCopy-->
```

3. Erstellen Sie eine VM oder Vorlagenspezifikation als Eingabe für das Maschinenprofil, im Azure-Portal mit aktivierter Verschlüsselung auf dem Host.

   - Wenn Sie eine VM erstellen möchten, wählen Sie eine VM-Größe, die die Verschlüsselung auf dem Host unterstützt. Nach dem Erstellen der VM ist die VM-Eigenschaft **Encryption at host** aktiviert.
   - Wenn Sie eine Vorlagenspezifikation verwenden möchten, weisen Sie dem Parameter `Encryption at Host` den Wert **true** unter `securityProfile` zu.

4. Erstellen Sie einen MCS-Maschinenkatalog mit Maschinenprofilworkflow, indem Sie eine VM oder Vorlagenspezifikation auswählen.

   - Datenträger/Betriebssystemdatenträger: Die Verschlüsselung erfolgt über einen kundenseitig verwalteten Schlüssel und einen plattformseitig verwalteten Schlüssel.
   - Kurzlebiger Betriebssystemdatenträger: Die Verschlüsselung erfolgt nur über einen plattformseitig verwalteten Schlüssel.
   - Cache-Datenträger: Die Verschlüsselung erfolgt über einen kundenseitig verwalteten Schlüssel und einen plattformseitig verwalteten Schlüssel.

   Sie können den Maschinenkatalog mithilfe von Web Studio oder über PowerShell-Befehle erstellen.

#### Informationen zur Verschlüsselung am Host aus Maschinenprofil abrufen

Sie können Informationen zur Verschlüsselung am Host aus einem Maschinenprofil abrufen, wenn Sie den PowerShell-Befehl mit dem Parameter `AdditionalData` ausführen. Ist der Parameter `EncryptionAtHost` **True**, dann ist die Verschlüsselung am Host für das Maschinenprofil aktiviert.

Beispiel: Wenn die Maschinenprofileingabe eine VM ist, führen Sie den folgenden Befehl aus:

```
1 (get-item XDHyp:\HostingUnits\myAzureNetwork\machineprofile.folder\abc.
     resourcegroup\def.vm).AdditionalData
2 <!--NeedCopy-->
```

Beispiel: Wenn die Maschinenprofileingabe eine Vorlagenspezifikation ist, führen Sie den folgenden Befehl aus:

```
1 (get-item XDHyp:\HostingUnits\myAzureNetwork\machineprofile.folder\abc.
     resourcegroup\def_templatespec.templatespec\EncryptionAtHost.
     templatespecversion).AdditionalData
2 <!--NeedCopy-->
```

### Doppelte Verschlüsselung auf verwalteten Datenträgern

Sie können einen Maschinenkatalog mit doppelter Verschlüsselung erstellen. Bei mit diesem Feature erstellten Katalogen werden alle Datenträger serverseitig mit plattformseitig und kundenseitig verwalteten Schlüsseln verschlüsselt. Sie besitzen und verwalten den Azure Key Vault, den Verschlüsselungsschlüssel und die Datenträgerverschlüsselungssätze (DES).

Die doppelte Verschlüsselung besteht aus der plattformseitigen Verschlüsselung (Standard) und der vom Kunden verwalteten Verschlüsselung. Kunden, die ein hohes Sicherheitsniveau erfordern und Risiken bezüglich des Verschlüsselungsalgorithmus, der Implementierung oder kompromittierter Schlüssel befürchten, können die doppelte Verschlüsselung wählen. Persistente Datenträger für OS und Daten, Snapshots und Images werden sämtlich im Ruhezustand doppelt verschlüsselt.

> **Hinweis:**
>
> - Sie können einen Maschinenkatalog mit Web Studio und mit PowerShell-Befehlen erstellen und aktualisieren. Informationen zu PowerShell-Befehlen finden Sie unter Maschinenkatalog mit doppelter Verschlüsselung erstellen.
> - Sie können einen nicht auf Maschinenprofilen basierenden Workflow oder einen auf Maschinenprofilen basierenden Workflow verwenden, um einen Maschinenkatalog mit doppelter Verschlüsselung zu erstellen oder zu aktualisieren.
> - Wenn Sie einen nicht auf Maschinenprofilen basierenden Workflow verwenden, um einen Maschinenkatalog zu erstellen, können Sie die gespeicherte `DiskEncryptionSetId` wiederverwenden.
> - Wenn Sie ein Maschinenprofil verwenden, können Sie eine VM- oder Vorlagenspezifikation als Eingabe für das Maschinenprofil verwenden.

**Einschränkungen:**

- Die doppelte Verschlüsselung wird für Ultra Disk- und Premium SSD v2-Datenträgern nicht unterstützt.
- Die doppelte Verschlüsselung wird für nicht verwaltete Datenträger nicht unterstützt.
- Wenn Sie den mit einem Katalog verknüpften DiskEncryptionSet-Schlüssel deaktivieren, werden die VMs des Katalogs deaktiviert.
- Alle zu von Kunden verwalteten Schlüsseln gehörenden Ressourcen (Azure Key Vaults, Datenträgerverschlüsselungssätze, VMs, Datenträger und Snapshots) müssen demselben Abonnement und derselben Region angehören.
- Sie können maximal 50 Datenträgerverschlüsselungssätze pro Region und Abonnement erstellen.
- Sie können einen Maschinenkatalog, der bereits eine `DiskEncryptionSetId` hat, nicht mit einer anderen `DiskEncryptionSetId` aktualisieren.

## Azure-Ressourcengruppen

Azure Provisioning-Ressourcengruppen sind eine Methode des Provisionings von VMs, über die Benutzern Anwendungen und Desktops bereitgestellt werden. Wenn Sie einen MCS-Maschinenkatalog erstellen, können Sie vorhandene, leere Azure-Ressourcengruppen hinzufügen oder neue erstellen. Informationen zu Azure-Ressourcengruppen finden Sie in der Dokumentation von Microsoft.

### Verwendung von Azure-Ressourcengruppen

Es gibt keine Beschränkung für die Anzahl der virtuellen Maschinen, verwalteten Datenträger, Snapshots und Images pro Azure-Ressourcengruppe. (Die Beschränkung auf 240 VMs pro 800 verwaltete Datenträger pro Azure-Ressourcengruppe wurde entfernt.)

- Wenn Sie zum Erstellen eines Maschinenkatalogs einen Dienstprinzipal mit vollem Gültigkeitsbereich verwenden, erstellen die Maschinenerstellungsdienste nur eine Azure-Ressourcengruppe und verwenden nur diese Gruppe für den Katalog.
- Wenn Sie zum Erstellen eines Maschinenkatalogs einen Dienstprinzipal mit eingeschränktem Gültigkeitsbereich verwenden, müssen Sie eine leere, vorab erstellte Azure-Ressourcengruppe für den Katalog angeben.

## Kurzlebige Azure-Datenträger

Ein kurzlebiger Azure-Datenträger ermöglicht die Umnutzung des Cachedatenträgers oder temporären Datenträgers zum Speichern des Betriebssystemdatenträgers für eine virtuelle Azure-Maschine. Dies ist nützlich für Azure-Umgebungen, die anstelle von Standard-HDD-Datenträgern leistungsstärkere SSD-Datenträger erfordern. Informationen zum Erstellen eines Katalogs mit einem kurzlebigen Azure-Datenträger finden Sie unter Katalog mit kurzlebigem Azure-Datenträger erstellen.

> **Hinweis:**
>
> Persistente Kataloge unterstützen keine kurzlebigen Betriebssystemdatenträger.

Kurzlebige Betriebssystemdatenträger erfordern ein Provisioningschema mit verwalteten Datenträgern und Shared Image Gallery.

### Speichern einer temporären kurzlebigen OS-Datenträgers

Sie können einen kurzlebigen OS-Datenträger auf dem Temp- bzw. Ressourcendatenträger der VM speichern. So können Sie einen kurzlebigen OS-Datenträger mit VMs verwenden, die über keinen oder

nur unzureichenden Cache verfügen. Solche VMs verfügen über einen Temp- bzw. Ressourcendatenträger zum Speichern eines kurzlebigen OS-Datenträgers (z. B. `Ddv4`).

Beachten Sie Folgendes:

- Kurzlebige Datenträger werden entweder auf dem VM-Cachedatenträger oder auf dem temporären bzw. Ressourcendatenträger der VM gespeichert. Die Cachedatenträger ist dem temporären Datenträger vorzuziehen, es sei denn, der Cachedatenträger ist zu klein für den Inhalt des Betriebsystemdatenträgers.
- Entsteht bei Updates ein neues Image, das größer als der Cachedatenträger und kleiner als der Temp-Datenträger ist, wird der kurzlebige OS-Datenträger durch den Temp-Datenträger der VM ersetzt.

#### Kurzlebige Azure-Betriebssystemdatenträger und MCS-Speicheroptimierung (MCS-E/A)

Kurzlebige Azure-Betriebssystemdatenträger und MCS-E/A können nicht gleichzeitig aktiviert werden.

Wichtige Punkte:

- Sie können keinen Maschinenkatalog mit gleichzeitig aktiviertem kurzlebigem Betriebssystemdatenträger und MCS-E/A erstellen.
- Die PowerShell-Parameter (`UseWriteBackCache` und `UseEphemeralOsDisk`) schlagen mit entsprechender Fehlermeldung fehl, wenn Sie sie in `New-ProvScheme` oder `Set-ProvScheme` auf **true** festlegen.
- Bei bestehenden Maschinenkatalogen, für die bei der Erstellung beide Features aktiviert wurden, ist weiterhin Folgendes möglich:
  - Aktualisieren des Maschinenkatalogs
  - Hinzufügen oder Löschen von VMs
  - Löschen des Maschinenkatalogs

### Azure Compute Gallery

Verwenden Sie Azure Compute Gallery (früher Azure Shared Image Gallery) als Repository mit veröffentlichten Images für per MCS bereitgestellte Maschinen in Azure. Sie können ein veröffentlichtes Image in der Image Gallery speichern, um die Erstellung und Hydration von Betriebssystemdatenträgern zu beschleunigen und die OS- und Anwendungsstartzeiten nicht persistenter VMs zu verbessern. Die Shared Image Gallery enthält die folgenden drei Elemente:

- *Gallery*: Hier werden Images gespeichert. MCS erstellt je eine Gallery für jeden Maschinenkatalog.

- *Imagedefinition*: Diese Definition enthält Informationen zum veröffentlichten Image (Betriebssystemtyp/-zustand, Azure-Region). MCS erstellt eine Imagedefinition für jedes Image, das für den Katalog erstellt wurde.
- *Imageversion:* Jedes Image in einer Shared Image Gallery kann mehrere Versionen haben, und jede Version kann mehrere Replikate in verschiedenen Regionen haben. Jedes Replikat ist eine vollständige Kopie des veröffentlichten Images.

> **Hinweis:**
>
> Die Shared Image Gallery-Funktion ist nur mit verwalteten Datenträgern kompatibel. Sie ist nicht für Legacy-Maschinenkataloge verfügbar.

Weitere Informationen finden Sie unter Übersicht über Azure Compute Gallery.

Informationen zum Erstellen oder Aktualisieren eines Maschinenkatalogs mithilfe eines Azure Compute Gallery-Images und PowerShell finden Sie unter Maschinenkatalog mit einem Azure Compute Gallery-Image erstellen oder aktualisieren.

### Vertrauliche Azure-VMs

Azure Confidential Computing-VMs stellen sicher, dass Ihr virtueller Desktop im Arbeitsspeicher verschlüsselt und bei der Verwendung geschützt ist.

Sie können MCS verwenden, um einen Katalog mit vertraulichen Azure-VMs zu erstellen. Sie müssen den Maschinenprofil-basierten Workflow verwenden, um einen solchen Katalog zu erstellen. Sie können sowohl die VM- als auch die ARM-Vorlagenspezifikation als Eingabe für das Maschinenprofil verwenden.

#### Wichtige Überlegungen zu vertraulichen VMs

Im Hinblick auf unterstützte VM-Größen und die Erstellung von Maschinenkatalogen mit vertraulichen VMs gilt es, Folgendes zu beachten:

- Unterstützte VM-Größen:
  - DCasv5-Serie
  - DCadsv5-Serie
  - ECasv5-Serie
  - ECadsv5-Serie
- Erstellen von Maschinenkatalogen mit vertraulichen VMs.
  - Sie können mithilfe von Web Studio- und PowerShell-Befehlen einen Maschinenkatalog mit vertraulichen Azure-VMs erstellen.

- Sie müssen einen maschinenprofilbasierten Workflow verwenden, um einen Maschinenkatalog mit vertraulichen Azure-VMs zu erstellen. Sie können eine VM oder eine Vorlagenspezifikation als Maschinenprofileingabe verwenden.
- Für das Masterimage und das als Eingabe verwendete Maschinenprofil muss derselbe Sicherheitstyp aktiviert werden. Es gibt folgende Sicherheitstypen:
  * **VMGuestStateOnly**: Vertrauliche VM, bei der nur der VM-Gastzustand verschlüsselt ist
  * **DiskWithVMGuestState**: Vertrauliche VM, bei der sowohl der Betriebssystemdatenträger als auch der VM-Gastzustand mit einem plattformverwalteten oder einem vom Kunden verwalteten Schlüssel verschlüsselt sind. Es können normale und auch kurzlebige Betriebssystemdatenträger verschlüsselt werden.
- Über den Parameter "AdditionalData"können Sie Informationen zu vertraulichen VMs verschiedener Ressourcentypen, etwa verwaltete Datenträger, Snapshots, Azure Compute Gallery-Image, VM und ARM-Vorlagenspezifikation abrufen. Beispiel:

  ```
  PS C:\Users\username> (get-item XDHyp:\HostingUnits\mynetwork
     \image.folder\username-dev-testing-rg.resourcegroup\
     username-dev-tsvda.vm).AdditionalData
  <!--NeedCopy-->
  ```

  Es gibt folgende zusätzlichen Daten:

  * DiskSecurityType
  * ConfidentialVMDiskEncryptionSetId
  * DiskSecurityProfiles

  Führen Sie folgenden Befehl aus, um die Confidential Compute-Eigenschaft für eine Maschinengröße abzurufen: `(Get-Item -path "XDHyp:\Connections\my-connection-name\East US.region\serviceoffering.folder\abc.serviceoffering").AdditionalData`

  Das "additional data"-Feld ist `ConfidentialComputingType`.
- Sie können den Sicherheitstyp eines Masterimages oder eines Maschinenprofils nicht von "vertraulich"in "nicht vertraulich"oder umgekehrt ändern.
- Für jede falsche Konfiguration erhalten Sie eine entsprechende Fehlermeldung.

#### Masterimages und Maschinenprofile vorbereiten

Bevor Sie einen Satz vertraulicher VMs erstellen, gehen Sie wie folgt vor, um ein Masterimage und ein Maschinenprofil für sie vorzubereiten:

1. Erstellen Sie im Azure-Portal eine vertrauliche VM mit bestimmten Einstellungen wie:

- **Sicherheitstyp**: Vertrauliche virtuelle Maschinen
- **Vertrauliche Betriebssystem-Datenträgerverschlüsselung**: Aktiviert.
- **Schlüsselverwaltung**: Vertrauliche Datenträgerverschlüsselung mit einem plattformverwalteten Schlüssel
  Weitere Informationen zum Erstellen vertraulicher VMs finden Sie in diesem Microsoft-Artikel.

2. Bereiten Sie das Masterimage auf der erstellten VM vor. Installieren Sie die erforderlichen Anwendungen und den VDA auf der erstellten VM.

   > **Hinweis:**
   >
   > Das Erstellen vertraulicher VMs mit VHD wird nicht unterstützt. Verwenden Sie stattdessen Azure Compute Gallery, verwaltete Datenträger oder Snapshots für diesen Zweck.

3. Erstellen Sie das Maschinenprofil auf eine der folgenden Arten:

   - Verwenden Sie die in Schritt 1 erstellte vorhandene VM, wenn sie die erforderlichen Maschineneigenschaften besitzt.
   - Wenn Sie sich für eine ARM-Vorlagenspezifikation als Maschinenprofil entscheiden, erstellen Sie die Vorlagenspezifikation wie erforderlich. Konfigurieren Sie insbesondere Parameter, die Ihre Anforderungen für vertrauliche VMs erfüllen, wie *SecurityEncryptionType* und *diskEncryptionSet* (für vom Kunden verwaltete Schlüssel). Weitere Informationen finden Sie unter Azure-Vorlagenspezifikation erstellen.

     > **Hinweis:**
     >
     > - Stellen Sie sicher, dass das Masterimage und das Maschinenprofil denselben Sicherheitsschlüsseltyp haben.
     > - Um vertrauliche virtuelle Maschinen zu erstellen, die eine vertrauliche Betriebssystem-Datenträgerverschlüsselung mit einem vom Kunden verwalteten Schlüssel erfordern, stellen Sie sicher, dass die IDs des Datenträgerverschlüsselungssatzes im Masterimage und im Maschinenprofil identisch sind.

#### Vertrauliche VMs mit Web Studio- oder PowerShell-Befehlen erstellen

Um eine Reihe vertraulicher VMs zu erstellen, erstellen Sie einen Maschinenkatalog mit einem Masterimage und einem Maschinenprofil, das von der gewünschten vertraulichen VM abgeleitet wurde.

Um den Katalog mit Web Studio zu erstellen, folgen Sie den unter Maschinenkataloge erstellen beschriebenen Schritten. Beachten Sie die folgenden Überlegungen:

- Wählen Sie auf der Seite **Image** ein Masterimage und ein Maschinenprofil aus, das Sie für die Erstellung der vertraulichen VM vorbereitet haben. Die Auswahl des Maschinenprofils ist obligatorisch und es stehen nur Profile zur Auswahl, die den gleichen Sicherheitsverschlüsselungstyp wie das ausgewählte Masterimage haben.
- Auf der Seite **Virtuelle Maschinen** werden nur Maschinengrößen zur Auswahl angezeigt, die vertrauliche VMs unterstützen.
- Auf der Seite **Datenträgereinstellungen** können Sie den Datenträgerverschlüsselungssatz nicht angeben, da er vom ausgewählten Maschinenprofil übernommen wurde.

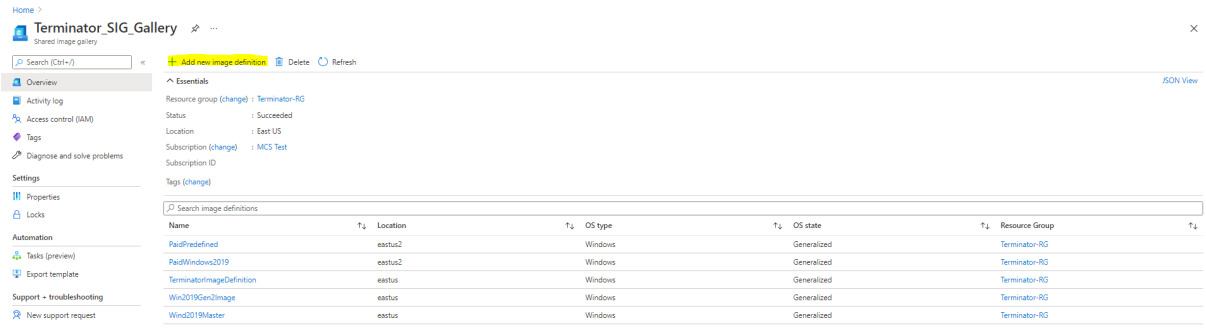
### Azure Marketplace

Citrix Virtual Apps and Desktops unterstützt die Verwendung eines Masterimages mit Abonnementinformationen zum Erstellen von Maschinenkatalogen in Azure. Weitere Informationen finden Sie unter Microsoft Azure Marketplace.

> **Tipp:**
>
> Manchen Images im Azure-Marketplace (z. B. Standard-Windows Server-Image) sind keine Abonnementinformationen angefügt. Das Citrix Virtual Apps and Desktops-Feature ist für kostenpflichtige Images vorgesehen.

#### Vergewissern Sie sich, dass das in der Shared Image Gallery erstellte Image Azure-Abonnementinformationen enthält

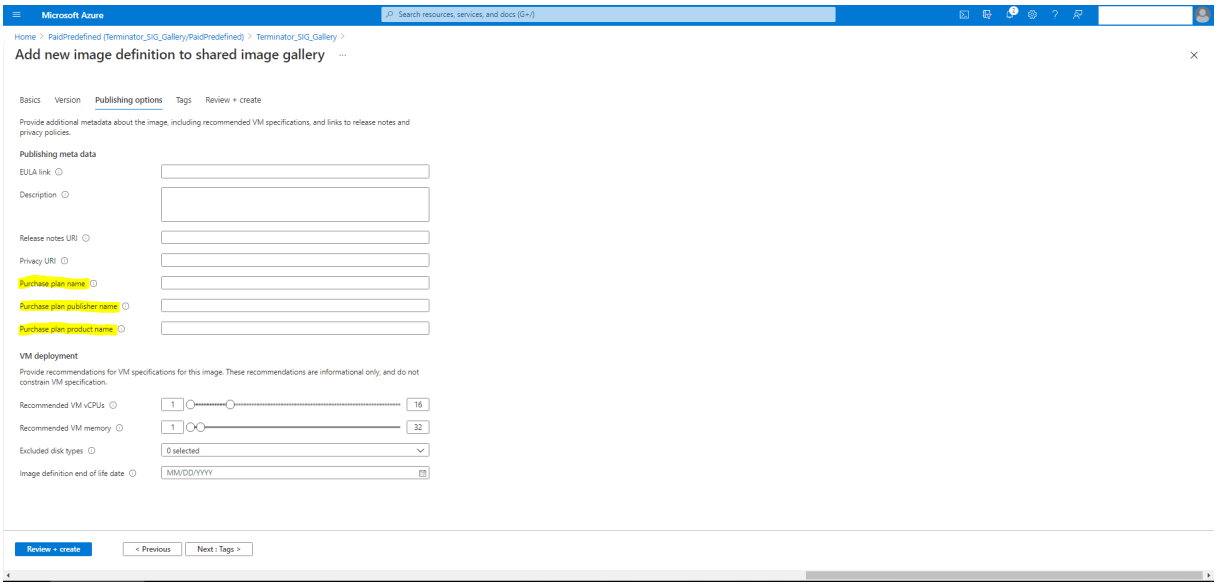
Gehen Sie wie in diesem Abschnitt beschrieben vor, um Images in der Shared Image Gallery in Web Studio anzuzeigen. Diese Images können für ein Masterimage verwendet werden. Um das Image in einer Shared Image Gallery abzulegen, erstellen Sie in der Gallery eine Imagedefinition.



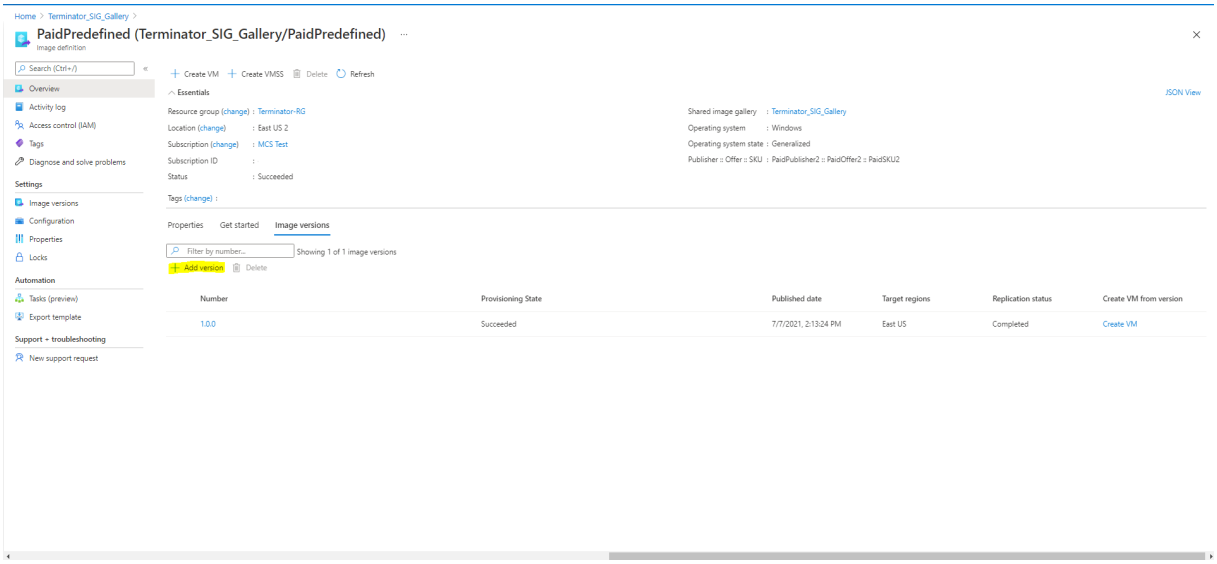

 

Überprüfen Sie auf der Seite **Veröffentlichungsoptionen** die Informationen zum Abonnement.

Die Informationsfelder sind zunächst leer. Füllen Sie diese Felder mit den Abonnementinformationen für das Image aus. Werden die Informationen nicht angegeben, kann der Maschinenkatalogprozess fehlschlagen.

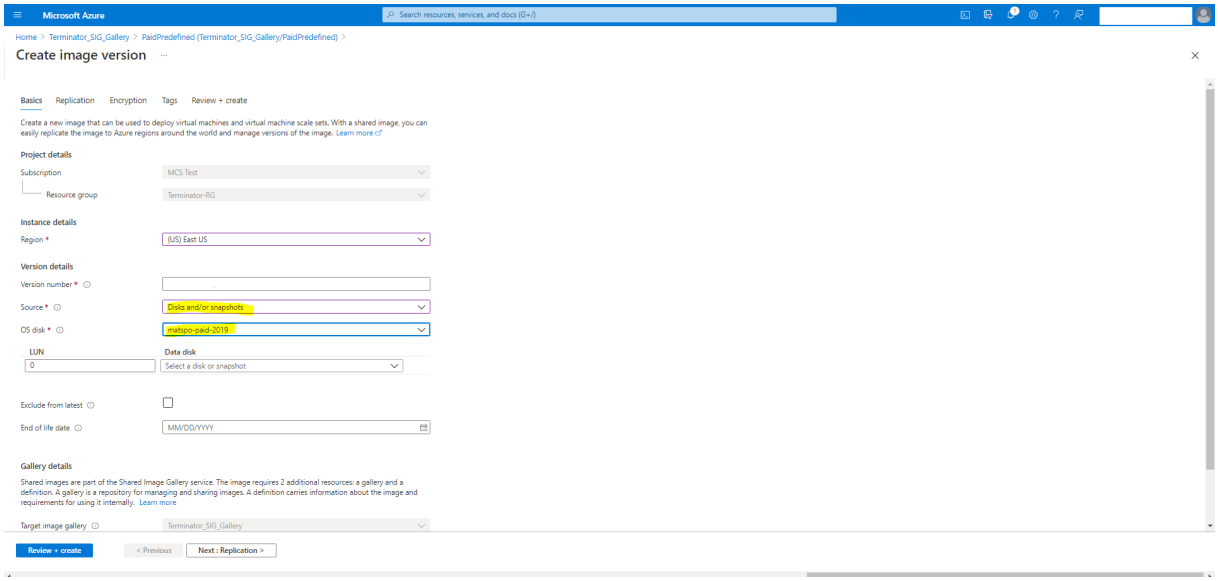



Nach dem Prüfen der Abonnementinformationen erstellen Sie eine Imageversion in der Definition. Diese wird als Masterimage verwendet. Klicken Sie auf **Add Version**:




Wählen Sie im Abschnitt **Version details** den Image-Snapshot oder verwalteten Datenträger als Quelle aus:




## Maschinenkatalog mit PowerShell erstellen

In diesem Abschnitt wird beschrieben, wie Sie Kataloge mit PowerShell erstellen:

- Katalog mit nicht-persistentem Zurückschreibcachedatenträger erstellen
- Katalog mit persistentem Zurückschreibcachedatenträger erstellen
- Startleistung mit MCSIO verbessern
- Vorlagenspezifikation beim Erstellen oder Aktualisieren eines Katalogs mit PowerShell verwenden
- Maschinenkataloge mit vertrauenswürdigem Start
- Eigenschaftswerte für Maschinenprofile verwenden
- Maschinenkatalog mit einem vom Kunden verwalteten Verschlüsselungsschlüssel erstellen
- Maschinenkatalog mit doppelter Verschlüsselung erstellen
- Katalog mit kurzlebigem Azure-Datenträger erstellen
- Dedizierte Azure-Hosts
- Maschinenkatalog mit einem Azure Compute Gallery-Image erstellen oder aktualisieren
- Shared Image Gallery konfigurieren
- Provisioning von Maschinen in spezifischen Verfügbarkeitszonen
- Speichertypen
- Speicherort der Auslagerungsdatei
- Einstellung für die Auslagerungsdatei aktualisieren
- Katalog mit Azure Spot-VMs erstellen
- Backup-VM-Größen konfigurieren
- Tags in allen Ressourcen kopieren
- Provisioning von Katalog-VMs mit installiertem Azure Monitor Agent

### Katalog mit nicht-persistentem Zurückschreibcachedatenträger erstellen

Zum Konfigurieren eines Katalogs mit nicht-persistentem Datenträger für den Zurückschreibcache verwenden Sie den PowerShell-Parameter `New-ProvScheme CustomProperties`. Die benutzerdefinierte Eigenschaft `UseTempDiskForWBC` legt fest, ob der temporäre Azure-Speicher zum Speichern der Zurückschreibcachedatei verwendet werden soll. Sie muss beim Ausführen von `New-ProvScheme` auf "true"gesetzt sein, wenn Sie den temporären Datenträger als Datenträger für den Zurückschreibcache verwenden möchten. Wenn die Eigenschaft nicht festgelegt ist, wird die Standardeinstellung **False** für den Parameter verwendet.

Beispiel der Verwendung des Parameters `CustomProperties` zur Einstellung von `UseTempDiskForWBC` auf **true**:

```
-CustomProperties '<CustomProperties xmlns=" http://schemas.citrix.com
   /2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org/2001/
   XMLSchema-instance"> `
<Property xsi:type="StringProperty" Name="PersistWBC" Value="false"/> `
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false
   "/> `
<Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
   Premium_LRS"/> `
<Property xsi:type="StringProperty" Name="WBCDiskStorageType" Value="
   Premium_LRS"/> `
<Property xsi:type="StringProperty" Name="LicenseType" Value="
   Windows_Client"/> `
<Property xsi:type="StringProperty" Name="UseTempDiskForWBC" Value="
   true"/> `
</CustomProperties>'
<!--NeedCopy-->
```

> **Hinweis:**
>
> Nachdem Sie für den Maschinenkatalog den lokalen temporären Azure-Speicher als Datenträger für den Zurückschreibecache festgelegt haben, können Sie die Einstellung später nicht in VHD ändern.

### Katalog mit persistentem Zurückschreibcachedatenträger erstellen

Zum Konfigurieren eines Katalogs mit persistentem Datenträger für den Zurückschreibcache verwenden Sie den PowerShell-Parameter `New-ProvScheme CustomProperties`. Dieser Parameter unterstützt die zusätzliche Eigenschaft `PersistWBC`, welche bestimmt, ob der Zurückschreibcachedatenträger bei von MCS-bereitgestellten Maschinen persistent 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.

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 Sie 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 Web Studio herunterfährt.

Wird `PersistWBC` auf **false** festgelegt, wird der Zurückschreibcachedatenträger gelöscht, wenn der Citrix Virtual Apps and Desktops-Administrator die Maschine mit Web Studio herunterfährt.

> **Hinweis:**
>
> Wird die Eigenschaft `PersistWBC` nicht angegeben, so gilt der Standardwert **false** und der Zurückschreibcachedatenträger wird bei Herunterfahren der Maschine mit Web 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.

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-->
```

### Startleistung mit MCSIO verbessern

Sie können die Startleistung für in Azure oder GCP verwaltete Datenträger verbessern, wenn MCSIO aktiviert ist. Verwenden Sie die benutzerdefinierte PowerShell-Eigenschaft `PersistOSDisk` im Befehl `New-ProvScheme`, um dieses Feature zu konfigurieren: Optionen für `New-ProvScheme`:

```
<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="Resource <!--NeedCopy-->
```

```
``````<!--NeedCopy-->
<!--NeedCopy-->
````````Groups" Value="benvaldev5RG3" />
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true"
    />
</CustomProperties>
<!--NeedCopy-->
```

Um dieses Feature zu aktivieren, legen Sie die benutzerdefinierte Eigenschaft `PersistOSDisk` auf **`true`** fest. Beispiel:

```
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
    =`"PersistOsDisk`" 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-->
```

### Vorlagenspezifikation beim Erstellen oder Aktualisieren eines Katalogs mit PowerShell verwenden

Sie können einen MCS-Maschinenkatalog erstellen oder aktualisieren, indem Sie eine Vorlagenspezifikation als Eingabe für das Maschinenprofil verwenden. Hierfür können Sie Web Studio oder PowerShell-Befehle verwenden.

Verwendung von Web Studio: Siehe Maschinenkatalog unter Verwendung eines Azure Resource Manager-Images in Web Studio erstellen.

Mit PowerShell:

1. Öffnen Sie das **PowerShell**-Fenster.
2. Führen Sie `asnp citrix*` aus.
3. Erstellen oder aktualisieren Sie einen Katalog.

   - Gehen Sie zum Erstellen eines Katalogs wie folgt vor:

     a) Verwenden Sie den Befehl `New-ProvScheme` mit einer Vorlagenspezifikation als Eingabe für das Maschinenprofil. Beispiel:

     ```
     New-ProvScheme -MasterImageVM "XDHyp:/HostingUnits/azure/
         image.folder/fgthj.resourcegroup/nab-ws-
         vda_OsDisk_1_xxxxxxxxxxa.manageddisk"
     MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.
         folder/fgthj.resourcegroup/test.templatespec/V1.
         templatespecversion"
     -ProvisioningSchemeName <String>
     -HostingUnitName <String>
     -IdentityPoolName <String>
     [-ServiceOffering <String>][-CustomProperties <String>
     [-LoggingId <Guid>]
     [-BearerToken <String>][-AdminAddress <String>]
     [<CommonParameters>]
     <!--NeedCopy-->
     ```

     b) Beenden Sie die Erstellung des Maschinenkatalogs.

   - Verwenden Sie zum Aktualisieren eines Katalogs den Befehl `Set-ProvScheme` mit einer Vorlagenspezifikation als Eingabe für das Maschinenprofil. Beispiel:

     ```
     Set-ProvScheme -MasterImageVm 'XDHyp://Connections/Azure/East
         Us.region/vm.folder/MasterDisk.vm'
     MachineProfile 'XDHyp:/HostingUnits/azure/machineprofile.
         folder/fgthj.resourcegroup/testing.templatespec/V1.
         templatespecversion'
     [-ProvisioningSchemeName] <String>
     [-CustomProperties <String>][-ServiceOffering <String>] [-
         PassThru]
     [-LoggingId <Guid>] [-BearerToken <String>][-AdminAddress <
         String>] [<CommonParameters>]
     <!--NeedCopy-->
     ```

### Maschinenkataloge mit vertrauenswürdigem Start

Zur problemlosen Erstellung eines Maschinenkatalogs mit vertrauenswürdigem Start verwenden Sie:

- Ein Maschinenprofil mit vertrauenswürdigem Start
- Eine VM-Größe, die vertrauenswürdigen Start unterstützt
- Eine Windows-VM-Version, die vertrauenswürdigen Start unterstützt. Derzeit unterstützen Windows 10, Windows 11, Windows Server 2016, 2019 und 2022 den vertrauenswürdigen Start.

> **Wichtig:**
>
> MCS unterstützt die Erstellung eines neuen Katalogs mit VMs, für die vertrauenswürdiger Start aktiviert ist. Um einen vorhandenen persistenten Katalog und vorhandene VMs zu aktualisieren, müssen Sie jedoch das Azure-Portal verwenden. Sie können den vertrauenswürdigen Start eines nicht persistenten Katalogs nicht aktualisieren. Weitere Informationen finden Sie im Microsoft-Dokument Enable Trusted launch on existing Azure VMs.

Führen Sie den folgenden Befehl aus, um den Bestand des Citrix Virtual Apps and Desktops-Angebots anzuzeigen und zu ermitteln, ob die VM-Größe den vertrauenswürdigen Start unterstützt:

1. Öffnen Sie ein PowerShell-Fenster.
2. Führen Sie **asnp citrix*** aus, um die Citrix-spezifischen PowerShell-Module zu laden.
3. Führen Sie den folgenden Befehl aus:

```
$s = (ls XDHyp:\HostingUnits<name of hosting unit>\serviceoffering
    .folder"<VM size>.serviceoffering)
<!--NeedCopy-->
```

4. Führen Sie `$s | select -ExpandProperty Additionaldata` aus.
5. Prüfen Sie den Wert des Attributs `SupportsTrustedLaunch`.
   - Wenn `SupportsTrustedLaunch` **True** ist, unterstützt die VM-Größe den vertrauenswürdigen Start.
   - Wenn `SupportsTrustedLaunch` **False**ist, unterstützt die VM-Größe den vertrauenswürdigen Start nicht.

Bei Azure-PowerShell können Sie den folgenden Befehl verwenden, um die VM-Größen zu ermitteln, die den vertrauenswürdigen Start unterstützen:

```
(Get-AzComputeResourceSku | where {
 $_.Locations.Contains($region) -and ($_.Name -eq "<VM size>")  }
 )[0].Capabilities
<!--NeedCopy-->
```

Die folgenden Beispiele veranschaulichen, welche von dem Azure PowerShell-Befehl zurückgegebenen VMs den vertrauenswürdigen Start unterstützen.

- *Beispiel 1*: Wenn die Azure-VM nur Generation 1 unterstützt, unterstützt die VM keinen vertrauenswürdigen Start. Daher wird `TrustedLaunchDisabled` nicht angezeigt, wenn Sie den Azure PowerShell-Befehl ausgeführt haben.
- *Beispiel 2*: Wenn die Azure-VM nur Generation 2 unterstützt und der Wert von `TrustedLaunchDisabled` **True** ist, unterstützt die Generation 2-VM-Größe den vertrauenswürdigen Start nicht.

- *Beispiel 3*: Wenn die Azure-VM nur Generation 2 unterstützt und `TrustedLaunchDisabled` nicht angezeigt wird, wenn Sie den PowerShell-Befehl ausgeführt haben, unterstützt die Generation 2-VM-Größe den vertrauenswürdigen Start.

Weitere Informationen zum vertrauenswürdigen Start für virtuelle Azure-Maschinen finden Sie in dem Microsoft-Dokument Vertrauenswürdiger Start für Azure-VMs.

#### Maschinenkatalog mit vertrauenswürdigem Start erstellen

1. Erstellen Sie ein Masterimage, für das vertrauenswürdiger Start aktiviert ist. Weitere Informationen finden Sie in der Microsoft-Dokumentation Unterstützte Images für VMs mit vertrauenswürdigem Start.
2. Erstellen Sie eine VM oder Vorlagenspezifikation mit Sicherheitstyp als **virtuelle Maschinen mit vertrauenswürdigem Start**. Weitere Informationen zum Erstellen einer VM oder Vorlagenspezifikation finden Sie im Microsoft-Dokument Bereitstellen eines virtuellen Computers mit vertrauenswürdigem Start.
3. Erstellen Sie einen Maschinenkatalog mit den Befehlen von Web Studio oder PowerShell.
   - Wenn Sie Web Studio verwenden möchten, lesen Sie Maschinenkatalog unter Verwendung eines Azure Resource Manager-Images in Web Studio erstellen.
   - Wenn Sie PowerShell-Befehle verwenden möchten, verwenden Sie den Befehl `New-ProvScheme` mit der VM oder Vorlagenspezifikation als Maschinenprofileingabe. Eine vollständige Liste der Befehle zum Erstellen eines Katalogs finden Sie unter Erstellen eines Katalogs.

     Beispiel für `New-ProvScheme` mit VM als Maschinenprofileingabe:

     ```
     New-ProvScheme -CleanOnBoot -HostingUnitName "name" -
        IdentityPoolName "name" -InitialBatchSizeHint 1
     -MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/fgthj.
        resourcegroup/nab-ws-vda_OsDisk_1_xxxxxxxxxxa.manageddisk"
     -MachineProfile "XDHyp:\HostingUnits<adnet>\machineprofile.
        folder<def.resourcegroup><machine profile vm.vm>"
     -ProvisioningSchemeName <String>
     -HostingUnitName <String>
     -IdentityPoolName <String>
     [-ServiceOffering <String>][-CustomProperties <String>]
     [<CommonParameters>]
     <!--NeedCopy-->
     ```

     Beispiel für `New-ProvScheme` mit Vorlagenspezifikation als Maschinenprofileingabe:

     ```
     New-ProvScheme -CleanOnBoot -HostingUnitName "name" -
        IdentityPoolName "name" -InitialBatchSizeHint 1
     ```

```
2   -MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/fgthj.
        resourcegroup/nab-ws-vda_OsDisk_1_xxxxxxxxxxa.manageddisk"
3   MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.
        folder/fgthj.resourcegroup/test.templatespec/V1.
        templatespecversion"
4   -ProvisioningSchemeName <String>
5   -HostingUnitName <String>
6   -IdentityPoolName <String>
7   [-ServiceOffering <String>][-CustomProperties <String>]
8   [<CommonParameters>]
9   <!--NeedCopy-->
```

#### Fehler beim Erstellen von Maschinenkatalogen mit vertrauenswürdigem Start

Beim Erstellen eines Maschinenkatalogs mit vertrauenswürdigem Start treten in den folgenden Szenarien Fehler auf:

| Szenario | Fehler |
| --- | --- |
| Sie wählen beim Erstellen eines nicht verwalteten Katalogs ein Maschinenprofil aus. | `MachineProfileNotSupportedForUnmanagedCata` |
| Sie wählen beim Erstellen eines Katalogs mit einem nicht verwalteten Datenträger als Masterimage ein Maschinenprofil, das den vertrauenswürdigen Start unterstützt. | `SecurityTypeNotSupportedForUnmanagedDisk` |
| Sie wählen beim Erstellen eines verwalteten Katalogs mit einer Masterimagequelle, deren Sicherheitstyp “vertrauenswürdiger Start”ist, kein Maschinenprofil aus. | `MachineProfileNotFoundForTrustedLaunchMaste` |
| Sie wählen ein Maschinenprofil aus, dessen Sicherheitstyp sich von dem des Masterimages unterscheidet. | `SecurityTypeConflictBetweenMasterImageAndMa` |
| Sie wählen eine VM-Größe, die den vertrauenswürdigen Start nicht unterstützt, verwenden aber beim Erstellen eines Katalogs ein Masterimage, das den vertrauenswürdigen Start unterstützt. | `MachineSizeNotSupportTrustedLaunch` |

### Eigenschaftswerte für Maschinenprofile verwenden

Der Maschinenkatalog verwendet die folgenden Eigenschaften, die in den benutzerdefinierten Eigenschaften definiert sind:

- Verfügbarkeitszone
- ID der dedizierten Hostgruppe
- ID des Datenträgerverschlüsselungssatzes
- Betriebssystemtyp
- Lizenztyp
- Speichertyp

Wenn diese benutzerdefinierten Eigenschaften nicht explizit definiert sind, werden die Eigenschaftswerte über die ARM-Vorlagenspezifikation oder VM festgelegt, je nachdem, was als Maschinenprofil verwendet wird. Wenn `ServiceOffering` nicht angegeben ist, wird der Wert über das Maschinenprofil festgelegt.

> **Hinweis:**
>
> Wenn einige der Eigenschaften im Maschinenprofil fehlen und nicht in den benutzerdefinierten Eigenschaften definiert sind, werden die Standardwerte der Eigenschaften angewendet, soweit zutreffend.

Im folgenden Abschnitt werden einige Szenarios für `New-ProvScheme` und `Set-ProvScheme` beschrieben, wenn für `CustomProperties` entweder alle Eigenschaften definiert sind oder Werte aus dem MachineProfile abgeleitet werden.

- New-ProvScheme-Szenarios
  - Im MachineProfile sind alle Eigenschaften definiert und CustomProperties sind nicht definiert. Beispiel:

    ```
    New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
    \machineprofile.folder\azure.resourcegroup\mpA.vm"
    ```

    Die folgenden Werte werden als benutzerdefinierte Eigenschaften für den Katalog festgelegt:

    ```
    1  Get-ProvScheme | select CustomProperties
    2  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
           machinecreation" xmlns:xsi="http://www.w3.org/2001/
           XMLSchema-instance">
    3  <Property xsi:type="StringProperty" Name="StorageAccountType"
            Value="<mpA-value>"/>
    4  <Property xsi:type="StringProperty" Name="OSType" Value="<mpA
           -value>"/>
    5  <Property xsi:type="StringProperty" Name="LicenseType" Value=
           "<mpA-value>"/>
    6  <Property xsi:type="StringProperty" Name="DiskEncryptionSetId
           " Value="<mpA-value>"/>
    7  <Property xsi:type="StringProperty" Name="
           DedicatedHostGroupId" Value="<mpA-value>"/>
    8  <Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
           value>"/>
    ```

```
</CustomProperties>
<!--NeedCopy-->
```

- Im MachineProfile sind einige Eigenschaften definiert und CustomProperties sind nicht definiert. Beispiel: Im MachineProfile sind nur LicenseType und OsType festgelegt.

  ```
  New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
  \machineprofile.folder\azure.resourcegroup\mpA.vm"
  ```

  Die folgenden Werte werden als benutzerdefinierte Eigenschaften für den Katalog festgelegt:

  ```
  Get-ProvScheme | select CustomProperties
  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
     machinecreation" xmlns:xsi="http://www.w3.org/2001/
     XMLSchema-instance">
  <Property xsi:type="StringProperty" Name="OSType" Value="<mpA
     -value>"/>
  <Property xsi:type="StringProperty" Name="LicenseType" Value=
     "<mpA-value>"/>
  </CustomProperties>
  <!--NeedCopy-->
  ```

- Sowohl im MachineProfile als auch in CustomProperties sind alle Eigenschaften definiert. Beispiel:

  ```
  New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
  \machineprofile.folder\azure.resourcegroup\mpA.vm"-CustomProperties
   $CustomPropertiesA
  ```

  Benutzerdefinierte Eigenschaften haben Priorität. Die folgenden Werte werden als benutzerdefinierte Eigenschaften für den Katalog festgelegt:

  ```
  Get-ProvScheme | select 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="<CustomPropertiesA-value>"/>
  <Property xsi:type="StringProperty" Name="OSType" Value="<
     CustomPropertiesA-value>"/>
  <Property xsi:type="StringProperty" Name="LicenseType" Value=
     "<CustomPropertiesA-value>"/>
  <Property xsi:type="StringProperty" Name="DiskEncryptionSetId
     " Value="<CustomPropertiesA-value>"/>
  <Property xsi:type="StringProperty" Name="
     DedicatedHostGroupId" Value="<CustomPropertiesA-value>"/>
  <Property xsi:type="StringProperty" Name="Zones" Value="<
     CustomPropertiesA-value>"/>
  </CustomProperties>
  <!--NeedCopy-->
  ```

- Einige Eigenschaften sind im MachineProfile definiert und einige Eigenschaften sind in CustomProperties definiert. Beispiel:
  - CustomProperties definieren LicenseType und StorageAccountType
  - MachineProfile definiert LicenseType, OsType und Zonen

```
New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
\machineprofile.folder\azure.resourcegroup\mpA.vm"-CustomProperties
 $CustomPropertiesA
```

Die folgenden Werte werden als benutzerdefinierte Eigenschaften für den Katalog festgelegt:

```
Get-ProvScheme | select 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="<CustomPropertiesA-value>"/>
<Property xsi:type="StringProperty" Name="OSType" Value="<mpA
   -value>"/>
<Property xsi:type="StringProperty" Name="LicenseType" Value=
   "<CustomPropertiesA-value>"/>
<Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
   value>"/>
</CustomProperties>
<!--NeedCopy-->
```

- Einige Eigenschaften sind im MachineProfile definiert und einige Eigenschaften sind in CustomProperties definiert. Darüber hinaus ist ServiceOffering nicht definiert. Beispiel:
  - CustomProperties definieren StorageType
  - MachineProfile definiert LicenseType

```
New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
   \machineprofile.folder\azure.resourcegroup\mp.vm"
-ServiceOffering "XDHyp:\HostingUnits\azureunit\
   serviceoffering.folder<explicit-machine-size>.
   serviceoffering"
<!--NeedCopy-->
```

Die folgenden Werte werden als benutzerdefinierte Eigenschaften für den Katalog festgelegt:

```
Get-ProvScheme | select ServiceOffering
serviceoffering.folder<explicit-machine-size>.serviceoffering

Get-ProvScheme | select 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="explicit-storage-type"/>
<Property xsi:type="StringProperty" Name="LicenseType" Value=
   "value-from-machineprofile"/>
</CustomProperties>
<!--NeedCopy-->
```

- Wenn der OsType weder in CustomProperties noch im MachineProfile definiert ist, gilt Folgendes:
  - Der Wert wird aus dem Masterimage gelesen.
  - Ist das Masterimage ein nicht verwalteter Datenträger, ist der OsType auf Windows eingestellt. Beispiel:

```
New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
\machineprofile.folder\azure.resourcegroup\mpA.vm"-MasterImageVM
 "XDHyp:\HostingUnits\azureunit\image.folder\linux-master-
image.manageddisk"
```

Der Wert aus dem Masterimage wird in die benutzerdefinierten Eigenschaften geschrieben, in diesem Fall Linux.

```
Get-ProvScheme | select CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance">
<Property xsi:type="StringProperty" Name="OSType" Value="
   Linux"/>
</CustomProperties>
<!--NeedCopy-->
```

- Set-ProvScheme-Szenarios
  - Ein vorhandener Katalog mit:
    - CustomProperties für `StorageAccountType` und OsType
    - MachineProfile `mpA.vm`, das Zonen definiert
  - Updates:
    - MachineProfile mpB.vm, das StorageAccountType definiert
    - Ein neuer Satz von benutzerdefinierten Eigenschaften $CustomPropertiesB, der LicenseType und OsType definiert

```
Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
\machineprofile.folder\azure.resourcegroup\mpB.vm"-CustomProperties
 $CustomPropertiesB
```

Die folgenden Werte werden als benutzerdefinierte Eigenschaften für den Katalog festgelegt:

```
Get-ProvScheme | select 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="<mpB-value>"/>
<Property xsi:type="StringProperty" Name="OSType" Value="<
   CustomPropertiesB-value>"/>
<Property xsi:type="StringProperty" Name="LicenseType" Value=
   "<CustomPropertiesB-value>"/>
    </CustomProperties>
<!--NeedCopy-->
```

- Ein vorhandener Katalog mit:
  - CustomProperties für `StorageAccountType` und OsType
  - MachineProfile `mpA.vm`, das StorageAccountType und LicenseType definiert
- Updates:
  - Ein neuer Satz von benutzerdefinierten Eigenschaften $CustomPropertiesB, der StorageAccountType und OsType definiert.

  ```
  Set-ProvScheme -CustomProperties $CustomPropertiesB
  ```

  Die folgenden Werte werden als benutzerdefinierte Eigenschaften für den Katalog festgelegt:

```
Get-ProvScheme | select 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="<CustomPropertiesB-value>"/>
<Property xsi:type="StringProperty" Name="OSType" Value="<
   CustomPropertiesB-value>"/>
<Property xsi:type="StringProperty" Name="LicenseType" Value=
   "<mp-A-value>"/>
</CustomProperties>
<!--NeedCopy-->
```

- Ein vorhandener Katalog mit:
  - CustomProperties für `StorageAccountType` und OsType
  - MachineProfile `mpA.vm`, das Zonen definiert
- Updates:
  - Ein MachineProfile mpB.vm, das StorageAccountType und LicenseType definiert
  - `ServiceOffering` ist nicht angegeben

```
Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
\machineprofile.folder\azure.resourcegroup\mpB.vm"
```

Die folgenden Werte werden als benutzerdefinierte Eigenschaften für den Katalog festgelegt:

```
Get-ProvScheme | select ServiceOffering
serviceoffering.folder<value-from-machineprofile>.
   serviceoffering

Get-ProvScheme | select 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="<mpB-value>"/>
<Property xsi:type="StringProperty" Name="OSType" Value="<
   prior-CustomProperties-value>"/>
<Property xsi:type="StringProperty" Name="LicenseType" Value=
   "<mpB-value>"/>
</CustomProperties>
<!--NeedCopy-->
```

### Provisioning von Katalog-VMs mit installiertem Azure Monitor Agent

Azure Monitoring ist ein Dienst, mit dem Sie Telemetriedaten aus Ihren Azure-und On-Premises-Umgebungen erfassen, analysieren und umsetzen können.

Azure Monitor Agent (AMA) sammelt Überwachungsdaten aus Rechenressourcen wie virtuellen Maschinen und übermittelt die Daten an Azure Monitor. Derzeit unterstützt der Dienst das Erfassen von Ereignisprotokollen sowie Syslog- und Leistungsmetriken, die dann an die Datenquellen Azure Monitor Metrics und Azure Monitor Logs gesendet werden.

Die Überwachung wird durch eindeutige Identifizierung der VMs in den Überwachungsdaten ermöglicht. Hierfür können Sie die VMs eines MCS-Maschinenkatalogs mit AMA als installierter Erweiterung bereitstellen.

#### Anforderungen

- Berechtigungen: Vergewissern Sie sich, dass Sie über die unter Erforderliche Azure-Berechtigungen angegebenen Azure-Mindestberechtigungen und über die folgenden Berechtigungen zur Verwendung von Azure Monitor verfügen:
  - `Microsoft.Compute/virtualMachines/extensions/read`
  - `Microsoft.Compute/virtualMachines/extensions/write`
  - `Microsoft.Insights/DataCollectionRuleAssociations/Read`

```
    - Microsoft.Insights/dataCollectionRuleAssociations/write
    - Microsoft.Insights/DataCollectionRules/Read
```

- Datensammlungsregel: Richten Sie eine Datensammlungsregel im Azure-Portal ein. Informationen zum Einrichten einer Datensammlungsregel finden Sie unter Create a data collection rule. Datensammlungsregeln sind plattformspezifisch (Windows oder Linux). Vergewissern Sie sich, dass Sie eine Datensammlungsregel gemäß der erforderlichen Plattform erstellen.
  AMA verwendet Datensammlungsregeln zum Verwalten der Zuordnung zwischen Ressourcen (wie VMs) und Datenquellen (wie Azure Monitor Metrics und Azure Monitor Logs).
- Standard-Workspace: Erstellen Sie einen Workspace im Azure-Portal. Informationen zum Erstellen eines Workspace finden Sie unter Create a Log Analytics workspace. Wenn Sie Protokolle und Daten sammeln, werden die Informationen in einem Workspace gespeichert. Ein Workspace hat eine eindeutige Workspace-ID und Ressourcen-ID. Der Workspace-Name muss für eine bestimmte Ressourcengruppe eindeutig sein. Nachdem Sie einen Workspace erstellt haben, konfigurieren Sie Datenquellen und Lösungen, um ihre Daten im Workspace zu speichern.
- Überwachungserweiterungen in Positivliste: Die Erweiterungen `AzureMonitorWindowsAgent` und `AzureMonitorLinuxAgent` sind von Citrix definierte Erweiterungen auf der Positivliste. Zur Anzeige der Erweiterungen auf der Positivliste verwenden Sie den PoSH-Befehl `Get-ProvMetadataConfiguration`.
- Masterimage: Microsoft empfiehlt, Erweiterungen von einer vorhandenen Maschine zu entfernen, bevor eine neue Maschine damit erstellt wird. Wenn die Erweiterungen nicht entfernt werden, kann dies zu unerwartetem Verhalten durch verbliebene Dateien führen. Weitere Informationen finden Sie unter If the VM is recreated from an existing VM.

Erstellen von Katalog-VMs mit aktiviertem AMA:

1. Richten Sie eine Maschinenprofilvorlage ein.
   - Wenn Sie eine VM als Maschinenprofilvorlage verwenden:
     a) Erstellen Sie eine VM im Azure-Portal.
     b) Schalten Sie die VM ein.
     c) Fügen Sie die VM der Datensammlungsregel unter **Ressourcen** hinzu. Dadurch wird der Agent auf der Vorlagen-VM installiert.

     > **Hinweis:**
     >
     > Wenn Sie einen Linux-Katalog erstellen müssen, richten Sie eine Linux-Maschine ein.

   - Wenn Sie eine Vorlagenspezifikation als Maschinenprofilvorlage verwenden möchten:
     a) Richten Sie eine Vorlagenspezifikation ein.

b) Fügen Sie der generierten Vorlagenspezifikation die folgende Erweiterungs- und Datensammlungsregelzuordnung hinzu:

```
{

"type": "Microsoft.Compute/virtualMachines/extensions",
"apiVersion": "2022-03-01",
"name": "<vm-name>/AzureMonitorWindowsAgent",
"dependsOn": [
    "Microsoft.Compute/virtualMachines/<vm-name>"
],
"location": "<azure-region>",
"properties": {

    "publisher": "Microsoft.Azure.Monitor",
    "type": "AzureMonitorWindowsAgent",
    "typeHandlerVersion": "1.0",
    "autoUpgradeMinorVersion": true,
    "enableAutomaticUpgrade": true
 }

 }
 ,
 {

    "type": "Microsoft.Insights/
       dataCollectionRuleAssociations",
    "apiVersion": "2021-11-01",
    "name": "<associatio-name>",
    "scope": "Microsoft.Compute/virtualMachines/<vm-name>",
    "dependsOn": [
     "Microsoft.Compute/virtualMachines/<vm-name>",
    "Microsoft.Compute/virtualMachines/<vm-name>/extensions
       /AzureMonitorWindowsAgent"
    ],
    "properties": {

       "description": "Association of data collection rule.
           Deleting this association will break the data
          collection for this Arc server.",
     "dataCollectionRuleId": "/subscriptions/<azure-
        subscription>/resourcegroups/<azure-resource-group
        >/providers/microsoft.insights/datacollectionrules
        /<azure-data-collection-rule>"
      }

     }

<!--NeedCopy-->
```

2. Erstellen oder aktualisieren Sie einen vorhandenen MCS-Maschinenkatalog.

   - Zum Erstellen eines neuen MCS-Katalogs:

a) Wählen Sie die VM oder Vorlagenspezifikation als Maschinenprofil in Web Studio aus.
b) Fahren Sie mit den nächsten Schritten zur Katalogerstellung fort.

- Zum Aktualisieren eines vorhandenen MCS-Katalogs verwenden Sie die folgenden PoSH-Befehle:
  - Um die aktualisierte Maschinenprofilvorlage für neue VMs bereitzustellen, führen Sie den folgenden Befehl aus:

```
Set-ProvScheme -ProvisioningSchemeName "name"
-MachineProfile "XDHyp:\HostingUnits\Unit1\machineprofile.
    folder\abc.resourcegroup\ab-machine-profile.vm"
<!--NeedCopy-->
```

  - Zum Aktualisieren vorhandener VMs mit der aktualisierten Maschinenprofilvorlage:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-
    catalog -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

3. Schalten Sie Katalog-VMs ein.
4. Überprüfen Sie im Azure-Portal, und ob die Überwachungserweiterung auf der VM installiert ist und ob die VM unter den Ressourcen der Datensammlungsregel angezeigt wird. Nach einigen Minuten werden die Überwachungsdaten auf dem Azure Monitor angezeigt.

#### Problembehandlung

Informationen zur Problembehandlung für Azure Monitor Agent finden Sie hier:

- https://learn.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-troubleshoot-windows-vm/
- https://learn.microsoft.com/en-us/azure/azure-resource-manager/troubleshooting/create-troubleshooting-template/

### Maschinenkatalog mit einem vom Kunden verwalteten Verschlüsselungsschlüssel erstellen

Schritte zum Erstellen eines Maschinenkatalogs mit einem vom Kunden verwalteten Verschlüsselungsschlüssel:

1. Öffnen Sie ein PowerShell-Fenster.
2. Führen Sie `asnp citrix*` aus, um die Citrix-spezifischen PowerShell-Module zu laden.
3. Geben Sie `cd xdhyp:/` ein.

4. Geben Sie `cd .\HostingUnits\(your hosting unit)` ein.
5. Geben Sie `cd diskencryptionset.folder` ein.
6. Geben Sie `dir` ein, um die Liste der Datenträgerverschlüsselungssätze abzurufen.
7. Kopieren Sie die ID eines Datenträgerverschlüsselungssets.
8. Erstellen Sie die Zeichenfolge einer benutzerdefinierten Eigenschaft, die die ID des Datenträgerverschlüsselungssets enthält. Beispiel:

```
$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=`"persistWBC`" Value=`"
    False`" />
<Property xsi:type=`"StringProperty`" Name=`"PersistOsDisk`" Value
    =`"false`" />
<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
    Value=`"true`" />
<Property xsi:type=`"StringProperty`" Name=`"DiskEncryptionSetId`"
     Value=`"/subscriptions/0xxx4xxx-xxb-4bxx-xxxx-xxxxxxxx/
    resourceGroups/abc/providers/Microsoft.Compute/
    diskEncryptionSets/abc-des`"/>
</CustomProperties>
<!--NeedCopy-->
```

9. Erstellen Sie einen Identitätspool, falls noch nicht vorhanden. Beispiel:

```
New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms## -
    Domain def.local -NamingSchemeType Numeric
<!--NeedCopy-->
```

10. Führen Sie den Befehl New-ProvScheme aus. Beispiel:

```
New-ProvScheme -CleanOnBoot -HostingUnitName "name" -
    IdentityPoolName "name" -InitialBatchSizeHint 1
-MasterImageVM "XDHyp:\HostingUnits\azure-res2\image.folder\def.
    resourcegroup\def.snapshot"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\azure-res2\virtualprivatecloud.folder\
     def.resourcegroup\def-vnet.virtualprivatecloud\subnet1.network
     " }

-ProvisioningSchemeName "name"
-ServiceOffering "XDHyp:\HostingUnits\azure-res2\serviceoffering.
    folder\Standard_DS2_v2.serviceoffering"
-MachineProfile "XDHyp:\HostingUnits<adnet>\machineprofile.folder<
    def.resourcegroup><machine profile vm.vm>"
-CustomProperties $customProperties
<!--NeedCopy-->
```

11. Beenden Sie die Erstellung des Maschinenkatalogs.

### Maschinenkatalog mit doppelter Verschlüsselung erstellen

Sie können einen Maschinenkatalog mit Web Studio und mit PowerShell-Befehlen erstellen und aktualisieren.

Schritte zum Erstellen eines Maschinenkatalogs mit doppelter Verschlüsselung:

1. Erstellen Sie einen Azure Key Vault und DES mit plattformseitig und kundenseitig verwalteten Schlüsseln. Informationen zum Erstellen eines Azure Key Vault und eines DES finden Sie unter Verwenden des Azure-Portals zum Aktivieren der doppelten Verschlüsselung von ruhenden Daten auf verwalteten Datenträgern.
2. Um die in Ihrer Hostingeinheit verfügbaren DiskEncryptionSets anzuzeigen, gehen Sie wie folgt vor:

   a) Öffnen Sie ein **PowerShell**-Fenster.
   b) Führen Sie die folgenden PowerShell-Befehle aus:

      i. `asnp citrix*`
      ii. `cd xdhyp:`
      iii. `cd HostingUnits`
      iv. `cd YourHostingUnitName` (z. B. azure-east)
      v. `cd diskencryptionset.folder`
      vi. `dir`

   Sie können eine ID des `DiskEncryptionSet` verwenden, um einen Katalog unter Verwendung benutzerdefinierter Eigenschaften zu erstellen oder zu aktualisieren.
3. Wenn Sie einen Maschinenprofilworkflow verwenden möchten, erstellen Sie eine VM- oder Vorlagenspezifikation als Eingabe für das Maschinenprofil.

   - Wenn Sie eine VM als Maschinenprofileingabe verwenden möchten:
     a) Erstellen Sie eine VM im Azure-Portal.
     b) Gehen Sie zu **Datenträger > Schlüsselverwaltung**, um die VM direkt mit einem `DiskEncryptionSetID` zu verschlüsseln.
   - Wenn Sie eine Vorlagenspezifikation als Maschinenprofileingabe verwenden möchten:
     a) Fügen Sie in der Vorlage unter `properties>storageProfile>osDisk>managedDisk` den Parameter `diskEncryptionSet` hinzu und fügen Sie die ID des DES für die doppelte Verschlüsselung hinzu.
4. Erstellen Sie den Maschinenkatalog.

- Wenn Sie Web Studio verwenden, führen Sie zusätzlich zu den Schritten unter Maschinenkataloge erstellen einen der folgenden Schritte aus.
  - Wenn Sie keinen auf Maschinenprofilen basierenden Workflow verwenden, wählen Sie auf der Seite **Datenträgereinstellungen** die Option **Verwenden Sie den folgenden Schlüssel, um Daten auf jeder Maschine zu verschlüsseln**. Wählen Sie dann den DES für die doppelte Verschlüsselung aus der Dropdownliste aus. Fahren Sie mit der Erstellung des Katalogs fort.
  - Wenn Sie den Maschinenprofil-Workflow verwenden, wählen Sie auf der Seite **Image** ein Masterimage und ein Maschinenprofil aus. Vergewissern Sie sich, dass die Eigenschaften des Maschinenprofils eine DES-ID enthalten.

  Alle im Katalog erstellten Maschinen werden mit dem Schlüssel doppelt verschlüsselt, der dem von Ihnen ausgewählten DES zugeordnet ist.
- Wenn Sie PowerShell-Befehle verwenden, führen Sie einen der folgenden Schritte aus:
  - Wenn Sie keinen auf Maschinenprofilen basierenden Workflow verwenden, fügen Sie dem Befehl `New-ProvScheme` die benutzerdefinierte Eigenschaft `DiskEncryptionSetId` hinzu. Beispiel:

```
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="
   DiskEncryptionSetId" Value="/subscriptions/12345678-
   xxxx-1234-1234-123456789012/resourceGroups/Sample-RG/
   providers/Microsoft.Compute/diskEncryptionSets/
   SampleEncryptionSet" />
</CustomProperties>'
-HostingUnitName "Redacted"
-IdentityPoolName "Redacted"
-InitialBatchSizeHint 1
-MasterImageVM "Redacted"
-NetworkMapping @{
"0"="Redacted" }

-ProvisioningSchemeName "Redacted"
-ServiceOffering "Redacted"
<!--NeedCopy-->
```

  - Wenn Sie einen Maschinenprofil-basierten Workflow verwenden, verwenden Sie eine Maschinenprofileingabe im Befehl `New-ProvScheme`. Beispiel:

```
New-ProvScheme -CleanOnBoot
```

```
-HostingUnitName azure-east
-IdentityPoolName aio-ip
-InitialBatchSizeHint 1
-MasterImageVM XDHyp:\HostingUnits\azure-east\image.folder
   \abc.resourcegroup\fgb-vda-snapshot.snapshot
-NetworkMapping @{
"0"="XDHyp:\HostingUnits\azure-east\virtualprivatecloud.
   folder\apa-resourceGroup.resourcegroup\apa-
   resourceGroup-vnet.virtualprivatecloud\default.network"
    }

-ProvisioningSchemeName aio-test
-MachineProfile XDHyp:\HostingUnits\azure-east\
   machineprofile.folder\abc.resourcegroup\abx-mp.
   templatespec\1.0.0.templatespecversion
<!--NeedCopy-->
```

5. Schließen Sie die Katalogerstellung mit dem Remote PowerShell SDK ab. Informationen zum Erstellen eines Katalogs mit dem Remote PowerShell SDK finden Sie unter https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/. Alle im Katalog erstellten Maschinen werden mit dem Schlüssel doppelt verschlüsselt, der dem von Ihnen ausgewählten DES zugeordnet ist.

#### Unverschlüsselten Katalog zur Verwendung der doppelten Verschlüsselung konvertieren

Sie können den Verschlüsselungstyp eines Maschinenkatalogs nur aktualisieren (mithilfe benutzerdefinierter Eigenschaften oder eines Maschinenprofils), wenn der Katalog zuvor unverschlüsselt war.

- Wenn Sie keinen auf Maschinenprofilen basierenden Workflow verwenden, fügen Sie dem Befehl `Set-ProvScheme` die benutzerdefinierte Eigenschaft DiskEncryptionSetId hinzu. Beispiel:

```
Set-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"
-CustomProperties '<CustomProperties xmlns="http://schemas.citrix
   .com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org
   /2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
   Value="/subscriptions/12345678-xxxx-1234-1234-123456789012/
   resourceGroups/Sample-RG/providers/Microsoft.Compute/
   diskEncryptionSets/SampleEncryptionSet" />
</CustomProperties>'
<!--NeedCopy-->
```

- Wenn Sie einen Maschinenprofil-basierten Workflow verwenden, verwenden Sie eine Maschinenprofileingabe im Befehl `Set-ProvScheme`. Beispiel:

```
Set-ProvScheme -ProvisioningSchemeName mxiao-test -MachineProfile
    XDHyp:\HostingUnits\azure-east\machineprofile.folder\aelx.
   resourcegroup\elx-mp.templatespec\1.0.0.templatespecversion
<!--NeedCopy-->
```

Alle neuen VMs, die Sie dem Katalog hinzufügen, werden nun mit dem Schlüssel doppelt verschlüsselt, der dem von Ihnen ausgewählten DES zugeordnet ist.

#### Überprüfen, ob ein Katalog doppelt verschlüsselt ist

- In Web Studio:
  1. Gehen Sie zu **Maschinenkataloge**.
  2. Wählen Sie den Katalog aus, den Sie überprüfen möchten. Klicken Sie am unteren Bildschirmrand auf die Registerkarte **Vorlageneigenschaften**.
  3. Überprüfen Sie unter **Azure-Details** die DES-ID in **Datenträgerverschlüsselungssatz**. Ist die DES-ID des Katalogs leer, ist der Katalog nicht verschlüsselt.
  4. Vergewissern Sie sich im Azure-Portal, dass es sich bei dem Verschlüsselungstyp des der DES-ID zugeordneten DES um plattformseitig und kundenseitig verwaltete Schlüssel handelt.
- Mit PowerShell:
  1. Öffnen Sie das **PowerShell**-Fenster.
  2. Führen Sie `asnp citrix*` aus, um die Citrix-spezifischen PowerShell-Module zu laden.
  3. Verwenden Sie `Get-ProvScheme`, um die Informationen des Maschinenkatalogs abzurufen. Beispiel:

     ```
     Get-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"
     <!--NeedCopy-->
     ```

  4. Rufen Sie die benutzerdefinierte DES-ID-Eigenschaft des Maschinenkatalogs ab. Beispiel:

     ```
     <Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
         Value="/subscriptions
        /12345678-1234-1234-1234-123456789012/resourceGroups/Sample
        -RG/providers/Microsoft.Compute/diskEncryptionSets/
        SampleEncryptionSet" />
     <!--NeedCopy-->
     ```

  5. Vergewissern Sie sich im Azure-Portal, dass es sich bei dem Verschlüsselungstyp des der DES-ID zugeordneten DES um plattformseitig und kundenseitig verwaltete Schlüssel handelt.

### Katalog mit kurzlebigem Azure-Datenträger erstellen

Zur Verwendung kurzlebiger Datenträger müssen Sie die benutzerdefinierte Eigenschaft `UseEphemeralOsDisk` bei der Ausführung von `New-ProvScheme` auf **true** festlegen.

> **Hinweis:**
>
> Wenn die benutzerdefinierte Eigenschaft `UseEphemeralOsDisk` auf **false** festgelegt oder kein Wert angegeben wird, verwenden alle bereitgestellten VDAs weiterhin einen bereitgestellten Betriebssystemdatenträger.

Nachfolgend finden Sie Beispiele benutzerdefinierter Eigenschaften zur Verwendung im Provisioningschema:

```
"CustomProperties": [
            {

                "Name": "UseManagedDisks",
                "Value": "true"
             }
,
            {

                "Name": "StorageType",
                "Value": "Standard_LRS"
             }
,
            {

                "Name": "UseSharedImageGallery",
                "Value": "true"
             }
,
            {

                "Name": "SharedImageGalleryReplicaRatio",
                "Value": "40"
             }
,
            {

                "Name": "SharedImageGalleryReplicaMaximum",
                "Value": "10"
             }
,
            {

                "Name": "LicenseType",
                "Value": "Windows_Server"
             }
,
```

```
38              {
39
40                  "Name": "UseEphemeralOsDisk",
41                  "Value": "true"
42               }
43
44          ],
45  <!--NeedCopy-->
```

### Kurzlebigen Datenträger für einen Katalog konfigurieren

Verwenden Sie zum Konfigurieren eines kurzlebigen Azure-Betriebssystemdatenträgers den Parameter `UseEphemeralOsDisk` in `Set-ProvScheme`. Setzen Sie den Wert des Parameters `UseEphemeralOsDisk` auf **true**.

> **Hinweis:**
>
> Um dieses Feature zu nutzen, müssen Sie auch die Parameter `UseManagedDisks` und `UseSharedImageGallery` aktivieren.

Beispiel:

```
1  Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties <
       CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
       machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
       instance">
2  <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
        />
3  <Property xsi:type="StringProperty" Name="UseSharedImageGallery" Value=
       "true" />
4  <Property xsi:type="StringProperty" Name="UseEphemeralOsDisk" Value="
       true" />
5  </CustomProperties>'
6  <!--NeedCopy-->
```

### Wichtige Überlegungen für kurzlebige Datenträger

Berücksichtigen Sie die folgenden Einschränkungen, wenn Sie das Provisioning kurzlebiger Betriebssystemdatenträger mit `New-ProvScheme` durchführen:

- Die für den Katalog verwendete VM-Größe muss kurzlebige Betriebssystemdatenträger unterstützen.
- Der einer VM-Größe zugeordnete Cachedatenträger oder temporäre Datenträger muss größer oder genauso groß sein wie der Betriebssystemdatenträger.
- Der temporäre Datenträger muss größer als der Cachedatenträger sein.

Berücksichtigen Sie diese Punkte auch bei folgenden Aufgaben:

- Erstellen des Provisioningschemas.
- Ändern des Provisioningschemas.
- Aktualisieren des Images.

### Dedizierte Azure-Hosts

Sie können mit MCS das Provisioning von VMs auf dedizierten Azure-Hosts ausführen. Vor dem Provisioning von VMs auf dedizierten Azure-Hosts führen Sie folgende Schritte aus:

- Erstellen Sie eine Hostgruppe.
- Erstellen Sie Hosts in der Hostgruppe.
- Vergewissern Sie sich, dass genügend Hostkapazität für die Erstellung von Katalogen und virtuellen Maschinen reserviert ist.

Sie können einen Katalog mit Maschinen erstellen, deren Host-Tenancy über das folgende PowerShell-Skript definiert wird:

```
1 New-ProvScheme <otherParameters> -CustomProperties '<CustomProperties
     xmlns="http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi
     ="http://www.w3.org/2001/XMLSchema-instance">
2  <Property xsi:type="StringProperty" Name="HostGroupId" Value="
      myResourceGroup/myHostGroup" />
3  ...other Custom Properties...
4  </CustomProperties>
5 <!--NeedCopy-->
```

Wenn Sie mit MCS virtuelle Maschinen auf dedizierten Azure-Hosts bereitstellen, berücksichtigen Sie Folgendes:

- Ein *dedizierter Host* ist eine Katalogeigenschaft und kann nach der Katalogerstellung nicht mehr geändert werden. Dedizieren für Mandanten wird derzeit in Azure nicht unterstützt.
- Bei Verwendung des Parameters `HostGroupId` ist eine vorkonfigurierte Azure-Hostgruppe in der Region der Hostingeinheit erforderlich.
- Die automatische Platzierung in Azure ist erforderlich. Das Feature beantragt das Onboarding des mit der Hostgruppe verknüpften Abonnements. Weitere Informationen finden Sie unter VM Scale Set on Azure Dedicated Hosts - Public Preview. Wenn die automatische Platzierung nicht aktiviert ist, tritt in MCS bei der Katalogerstellung ein Fehler auf.

### Maschinenkatalog mit einem Azure Compute Gallery-Image erstellen oder aktualisieren

Als Image zum Erstellen eines Maschinenkatalogs können Sie Images auswählen, die Sie in der Azure Compute Gallery erstellt haben.

Damit diese Images angezeigt werden, müssen Sie folgende Schritte ausführen:

1. Konfigurieren Sie eine Citrix Virtual Apps and Desktops-Site.
2. Stellen Sie eine Verbindung mit Azure Resource Manager her.
3. Erstellen Sie im Azure-Portal eine Ressourcengruppe. Weitere Informationen finden Sie unter Erstellen einer Azure Compute Gallery-Instanz über das Portal.
4. Erstellen Sie in der Ressourcengruppe eine Azure Compute Gallery.
5. Erstellen Sie in der Azure Compute Gallery eine Imagedefinition.
6. Erstellen Sie in der Imagedefinition eine Imageversion.

Verwenden Sie folgende PowerShell-Befehle, um einen Maschinenkatalog mit einem Image aus der Azure Compute Gallery zu erstellen oder zu aktualisieren:

1. Öffnen Sie ein PowerShell-Fenster.
2. Führen Sie `asnp citrix*` aus, um die Citrix-spezifischen PowerShell-Module zu laden.
3. Wählen Sie eine Ressourcengruppe und listen Sie dann alle Kataloge in der Ressourcengruppe auf.

```
Get-ChildItem -LiteralPath @("XDHyp:\HostingUnits\testresource\
    image.folder\sharedImageGalleryTest.resourcegroup")
<!--NeedCopy-->
```

4. Wählen Sie einen Katalog und listen Sie dann alle Imagedefinitionen des Katalogs auf.

```
Get-ChildItem -LiteralPath @("XDHyp:\HostingUnits\testresource\
    image.folder\sharedImageGalleryTest.resourcegroup\
    sharedImageGallery.sharedimagegallery")
<!--NeedCopy-->
```

5. Wählen Sie eine Imagedefinition und listen Sie dann alle Imageversionen der Imagedefinition auf.

```
Get-ChildItem -LiteralPath @("XDHyp:\HostingUnits\testresource\
    image.folder\sharedImageGalleryTest.resourcegroup\
    sharedImageGallery.sharedimagegallery\sigtestimage.
    imagedefinition")
<!--NeedCopy-->
```

6. Zum Erstellen und Aktualisieren eines MCS-Katalogs verwenden Sie die folgenden Elemente:

    - Ressourcengruppe

- Katalog
- Katalogimagedefinition
- Katalogimageversion

Informationen zum Erstellen eines Katalogs mit dem Remote PowerShell SDK finden Sie unter https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

### Shared Image Gallery konfigurieren

Mit dem Befehl `New-ProvScheme` erstellen Sie ein Provisioningschema mit Unterstützung für Shared Image Gallery. Verwenden Sie den Befehl `Set-ProvScheme`, um dieses Feature für ein Provisioningschema zu aktivieren bzw. deaktivieren und um die Replikatquote und die Anzahl maximaler Replikate zu ändern.

Zu Unterstützung der Shared Image Gallery-Funktion wurden Provisioningschemata um drei benutzerdefinierte Eigenschaften erweitert:

`UseSharedImageGallery`

- Legt fest, ob die Shared Image Gallery zum Speichern der veröffentlichten Images verwendet wird. Bei Auswahl von **True** wird das Image als Shared Image Gallery-Image gespeichert. Andernfalls wird es als Snapshot gespeichert.
- Gültige Werte sind **True** und **False**.
- Der Standardwert bei nicht definierter Eigenschaft ist **False**.

`SharedImageGalleryReplicaRatio`

- Definiert das Verhältnis von Maschinen zu Replikaten der Galerie-Imageversion.
- Gültige Werte sind ganze Zahlen größer als 0.
- Bei nicht definierter Eigenschaft werden Standardwerte verwendet. Der Standardwert für persistente Betriebssystemdatenträger beträgt 1000 und der Standardwert für nicht-persistente Betriebssystemdatenträger beträgt 40.

`SharedImageGalleryReplicaMaximum`

- Definiert die Anzahl maximaler Replikate für jede Galerie-Imageversion.
- Gültige Werte sind ganze Zahlen größer als 0.
- Der Standardwert bei nicht definierter Eigenschaft ist 10.
- Azure unterstützt derzeit bis zu 10 Replikate pro Galerie-Imageversion. Wenn diese Eigenschaft auf einen Wert festgelegt ist, der den Azure-Höchstwert übersteigt, versucht MCS, den angegebenen Wert zu verwenden. Azure generiert einen Fehler, der von MCS protokolliert wird, und die aktuelle Replikatanzahl wird unverändert beibehalten.

> **Tipp:**
>
> Wenn Sie die Shared Image Gallery zum Speichern eines veröffentlichten Images für Kataloge verwenden, die mit MCS bereitgestellt werden, legt MCS die Anzahl der Galerie-Imageversionsreplikate basierend auf der Anzahl der Maschinen im Katalog, der Replikatquote und der Anzahl maximaler Replikate fest. Zur Berechnung der Replikatanzahl wird die Maschinenanzahl im Katalog durch die Replikatquote dividiert (und auf den nächsten Ganzzahlwert aufgerundet) und dann gemäß der Anzahl maximaler Replikate begrenzt. Ein Beispiel: Bei eine Replikatquote von 20 und einem Höchstwert von 5 wird für 0–20 Maschinen ein Replikat erstellt, für 21–40 Maschinen 2 Replikate, für 41–60 Maschinen 3 Replikate, für 61–80 Maschinen 4 Replikate und für 81 Maschinen (und mehr) 5 Replikate.

#### Anwendungsfall: Aktualisieren der Shared Image Gallery-Replikatquote und der Anzahl maximaler Replikate

Der vorhandene Maschinenkatalog verwendet Shared Image Gallery. Verwenden Sie den Befehl `Set-ProvScheme`, um die benutzerdefinierten Eigenschaften für alle vorhandenen Maschinen im Katalog und alle zukünftigen Maschinen zu aktualisieren:

```
1 Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties '
     <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
     machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
     instance"> <Property xsi:type="StringProperty" Name="StorageType"
     Value="Standard_LRS"/> <Property xsi:type="StringProperty" Name="
     UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
     Name="UseSharedImageGallery" Value="True"/> <Property xsi:type="
     IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/> <
     Property xsi:type="IntProperty" Name="
     SharedImageGalleryReplicaMaximum" Value="20"/></CustomProperties>'
2 <!--NeedCopy-->
```

#### Anwendungsfall: Konvertieren eines Snapshot-Katalogs in einen Shared Image Gallery-Katalog

Führen Sie für diesen Anwendungsfall folgende Schritte aus:

1. Führen Sie `Set-ProvScheme` aus, wobei der Flag `UseSharedImageGallery` auf **True** gesetzt ist. Fügen Sie optional die Eigenschaften `SharedImageGalleryReplicaRatio` und `SharedImageGalleryReplicaMaximum` hinzu.
2. Aktualisieren Sie den Katalog.
3. Starten Sie die Maschinen neu, um ein Update zu erzwingen.

Beispiel:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties '
    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance"> <Property xsi:type="StringProperty" Name="StorageType"
    Value="Standard_LRS"/> <Property xsi:type="StringProperty" Name="
    UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
    Name="UseSharedImageGallery" Value="True"/> <Property xsi:type="
    IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/> <
    Property xsi:type="IntProperty" Name="
    SharedImageGalleryReplicaMaximum" Value="20"/></CustomProperties>'
<!--NeedCopy-->
```

> **Tipp:**
>
> Die Parameter `SharedImageGalleryReplicaRatio` und `SharedImageGalleryReplicaMaximum` sind nicht erforderlich. Nachdem der Befehl `Set-ProvScheme` abgeschlossen ist, wurde das Shared Image Gallery-Image noch nicht erstellt. Sobald der Katalog für die Verwendung der Galerie konfiguriert ist, speichert das nächste Katalogupdate das veröffentlichte Image in der Galerie. Der Befehl zum Katalogupdate erstellt die Galerie, das Galerie-Image und die Imageversion. Durch den Neustart der Maschinen werden sie aktualisiert, und es wird gegebenenfalls die Replikatanzahl aktualisiert. Alle vorhandenen nicht-persistenten Maschinen werden dann mit dem Shared Image Gallery-Image zurückgesetzt, und alle neu bereitgestellten Maschinen werden mit diesem Image erstellt. Der alte Snapshot wird innerhalb weniger Stunden automatisch bereinigt.

#### Anwendungsfall: Konvertieren eines Shared Image Gallery-Katalogs in einen Snapshot-Katalog

Führen Sie für diesen Anwendungsfall folgende Schritte aus:

1. Führen Sie `Set-ProvScheme` aus, wobei der Flag `UseSharedImageGallery` auf **False** gesetzt oder nicht definiert ist.
2. Aktualisieren Sie den Katalog.
3. Starten Sie die Maschinen neu, um ein Update zu erzwingen.

Beispiel:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties '
    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance"> <Property xsi:type="StringProperty" Name="StorageType"
    Value="Standard_LRS"/> <Property xsi:type="StringProperty" Name="
    UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
    Name="UseSharedImageGallery" Value="False"/></CustomProperties>'
<!--NeedCopy-->
```

> **Tipp:**
>
> Im Gegensatz zum Update von einem Snapshot-Katalog auf einen Shared Image Gallery-Katalog sind die benutzerdefinierten Daten für jede Maschine noch nicht auf die neuen benutzerdefinierten Eigenschaften aktualisiert. Führen Sie den folgenden Befehl aus, um die ursprünglichen benutzerdefinierten Shared Image Gallery-Eigenschaften anzuzeigen: `Get-ProvVm -ProvisioningSchemeName catalog-name`. Nach Abschluss des Befehls `Set-ProvScheme` ist der Imagesnapshot noch nicht erstellt. Sobald konfiguriert ist, dass der Katalog nicht mehr die Galerie verwendet, speichert das nächste Katalogupdate das veröffentlichte Image als Snapshot. Alle vorhandenen nicht-persistenten Maschinen werden dann mit dem Snapshot zurückgesetzt, und alle neu bereitgestellten Maschinen werden aus dem Snapshot erstellt. Durch Neustart werden die Maschinen aktualisiert. Die benutzerdefinierten Maschinendaten werden dabei aktualisiert und zeigen an, dass `UseSharedImageGallery` auf **False** gesetzt ist. Die alten Shared Image Gallery-Assets (Galerie, Image und Version) werden automatisch innerhalb weniger Stunden bereinigt.

### Provisioning von Maschinen in spezifischen Verfügbarkeitszonen

Sie können das Provisioning von Maschinen auch in spezifischen Verfügbarkeitszonen in Azure-Umgebungen ausführen. Das ist mit PowerShell möglich.

> **Hinweis:**
>
> Wenn keine Zonen angegeben werden, lässt MCS Azure die Maschinen innerhalb der Region platzieren. Werden mehrere Zonen angegeben, verteilt MCS die Maschinen nach dem Zufallsprinzip in den Zonen.

#### Verfügbarkeitszonen über PowerShell konfigurieren

Mit `Get-Item` in PowerShell können Sie die Elemente des Angebots anzeigen. Um beispielsweise das *Serviceangebot Eastern US* `Standard_B1ls` anzuzeigen:

```
1 $serviceOffering = Get-Item -path "XDHyp:\Connections\my-connection-
     name\East US.region\serviceoffering.folder\Standard_B1ls.
     serviceoffering"
2 <!--NeedCopy-->
```

Zum Anzeigen der Zonen verwenden Sie den Parameter `AdditionalData`:

```
$serviceOffering.AdditionalData
```

Werden keine Verfügbarkeitszone angegeben, bleibt die Art und Weise, wie Maschinen bereitgestellt werden, unverändert.

Um Verfügbarkeitszonen über PowerShell zu konfigurieren, verwenden Sie die benutzerdefinierte Eigenschaft **Zones** von `New-ProvScheme`. Die Eigenschaft **Zones** definiert eine Liste von Verfügbarkeitszonen für das Provisioning von Maschinen. Diese Zonen können eine oder mehrere Verfügbarkeitszonen enthalten. Beispiel: `<Property xsi:type="StringProperty"Name="Zones"Value="1, 3"/>` für die Zonen 1 und 3.

Verwenden Sie den Befehl `Set-ProvScheme`, um die Zonen für ein Provisioningschema zu aktualisieren.

Wird eine ungültige Zone angegeben, wird das Provisioningschema nicht aktualisiert und eine Fehlermeldung mit Anweisungen zur Korrektur des ungültigen Befehls angezeigt.

> **Tipp:**
>
> Wenn Sie eine ungültige benutzerdefinierte Eigenschaft angeben, wird das Provisioningschema nicht aktualisiert und eine Fehlermeldung angezeigt.

## Speichertypen

Wählen Sie Speichertypen für virtuelle Maschinen in Azure-Umgebungen, die MCS verwenden. Für Ziel-VMs unterstützt MCS Folgendes:

- OS-Datenträger: SSD Premium, SSD oder HDD
- Zurückschreibcache-Datenträger: SSD Premium, SSD oder HDD

Berücksichtigen Sie bei Verwendung dieser Speichertypen Folgendes:

- Ihre VM muss den ausgewählten Speichertyp unterstützen.
- Wenn Ihre Konfiguration einen kurzlebigen Azure-Datenträger enthält, wird keine Option für die Einstellung des Zurückschreibcache-Datenträgers angeboten.

> **Tipp:**
>
> `StorageType` ist für einen Betriebssystemspeichertyp und mit Speicherkonto konfiguriert. `WBCDiskStorageType` ist für den Zurückschreibcache konfiguriert. Für einen normalen Katalog ist `StorageType` erforderlich. Wenn `WBCDiskStorageType` nicht konfiguriert ist, wird `StorageType` als Standard für `WBCDiskStorageType` verwendet.

Wenn WBCDiskStorageType nicht konfiguriert ist, wird StorageType als Standard für WBCDiskStorageType verwendet.

### Speichertypen konfigurieren

Verwenden Sie den Parameter `StorageType` in `New-ProvScheme`, um Speichertypen für VMs zu konfigurieren. Stellen Sie den Wert des Parameters `StorageType` auf einen der unterstützten Spe-

ichertypen ein.

Im Folgenden finden Sie einen Beispielsatz für den Parameter `CustomProperties` in einem Provisioningschema:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -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="StorageType" Value="
    Premium_LRS" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="
    Windows_Client" />
</CustomProperties>'
<!--NeedCopy-->
```

#### Zonenredundanten Speicher aktivieren

Sie können bei der Katalogerstellung einen zonenredundanten Speicher (ZRS) auswählen. Ihre Azure Managed Disk wird dann synchron über mehrere Verfügbarkeitszonen repliziert, sodass Sie Ihre Daten bei einem Ausfall in einer Zone mithilfe der Redundanz in den übrigen Zonen wiederherstellen können.

In den benutzerdefinierten Speichertypeigenschaften können Sie **Premium_ZRS** und **Standard-SSD_ZRS** angeben. Der ZRS-Speicher kann mithilfe vorhandener benutzerdefinierter Eigenschaften oder über die Vorlage **MachineProfile** festgelegt werden. Der ZRS wird auch für den Befehl `Set-ProvVMUpdateTimeWindow` mit den Parametern `-StartsNow` und `-DurationInMinutes -1` unterstützt und Sie können vorhandene Maschinen von LRS in ZRS ändern.

**Einschränkungen:**

- Nur für verwaltete Datenträger unterstützt
- Nur mit Premium- und Standard-SSDs unterstützt
- Keine Unterstützung mit `StorageTypeAtShutdown`
- Nur in bestimmten Regionen verfügbar.
- Beim Erstellen großer Mengen an ZRS-Datenträgern sinkt die Leistung von Azure. Fahren Sie die Maschinen daher beim ersten Einschalten gestaffelt hoch (weniger als 300 Maschinen gleichzeitig).

**Zonenredundanten Speicher als Datenträgerspeichertyp festlegen** Sie können einen zonenredundanten Speicher bei der Katalogerstellung auswählen oder den Speichertyp in einem vorhandenen Katalog aktualisieren.

**Zonenredundanten Speicher mithilfe von PowerShell-Befehlen auswählen** Wenn Sie einen neuen Katalog in Azure mit dem PowerShell-Befehl `New-ProvScheme` erstellen, verwenden Sie für `StorageAccountType` den Wert `Standard_ZRS`.
Beispiel:

```
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
    StandardSSD_ZRS" />
<!--NeedCopy-->
```

Nach Auswahl dieses Werts prüft eine dynamische API, ob er ordnungsgemäß verwendet werden kann. Folgende Ausnahmen können auftreten, wenn ZRS für Ihren Katalog nicht zulässig ist:

- **StorageTypeAtShutdownNotSupportedForZrsDisks**: Die benutzerdefinierte Eigenschaft "StorageTypeAtShutdown"kann nicht mit ZRS verwendet werden.
- **StorageAccountTypeNotSupportedInRegion**: Diese Ausnahme tritt auf, wenn Sie versuchen, ZRS in einer nicht unterstützten Azure-Region zu verwenden.
- **ZrsRequiresManagedDisks**: Sie können zonenredundanten Speicher nur mit verwalteten Datenträgern verwenden.

Sie können den Datenträgerspeichertyp mit den folgenden benutzerdefinierten Eigenschaften festlegen:

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`

> **Hinweis:**
>
> Bei der Katalogerstellung wird der Betriebssystemdatenträger `StorageType` des Maschinenprofils verwendet, wenn die benutzerdefinierten Eigenschaften nicht festgelegt sind.

## Diagnoseeinstellungen auf VMs und NICs aus einem Maschinenprofil erfassen

Sie können Diagnoseeinstellungen auf VMs und NICs aus einem Maschinenprofil erfassen, während Sie einen Maschinenkatalog erstellen, einen vorhandenen Maschinenkatalog aktualisieren und vorhandene VMs aktualisieren.

Sie können eine VM- oder Vorlagenspezifikation als Maschinenprofilquelle erstellen.

### Wichtige Schritte

1. Richten Sie die erforderlichen IDs in Azure ein. Sie müssen diese IDs in der Vorlagenspezifikation angeben.

- Speicherkonto
- Protokollanalysen-Workspace
- Event Hub-Namespace mit den Standardtarifpreisen

2. Erstellen Sie eine Maschinenprofilquelle.
3. Erstellen Sie einen neuen Maschinenkatalog, aktualisieren Sie einen vorhandenen Katalog oder aktualisieren Sie vorhandene VMs.

#### Erforderliche IDs in Azure einrichten

Richten Sie eine der folgenden Optionen in Azure ein:

- Speicherkonto
- Protokollanalysen-Workspace
- Event Hub-Namespace mit den Standardtarifpreisen

**Speicherkonto einrichten** Erstellen Sie ein Standardspeicherkonto in Azure. Geben Sie in der Vorlagenspezifikation die vollständige Resourcen-ID für das Speicherkonto als `storageAccountId` an.

Sobald VMs so eingerichtet sind, dass sie Daten im Speicherkonto protokollieren, finden Sie die Daten unter dem Container `insights-metrics-pt1m`.

**Workspace für Protokollanalysen einrichten** Erstellen Sie einen Workspace für Protokollanalysen. Geben Sie in der Vorlagenspezifikation die vollständige Ressourcen-ID für den Protokollanalysen-Workspace als workspaceId an.

Sobald VMs so eingerichtet sind, dass sie Daten im Workspace protokollieren, können Daten unter “Protokolle”in Azure abgefragt werden. Sie können den folgenden Befehl in Azure unter “Protokolle” ausführen, um die Anzahl aller von einer Ressource protokollierten Metriken anzuzeigen:

‘AzureMetrics
| summarize Count=count() by ResourceId# Microsoft Azure-Katalog erstellen

> **Hinweis:**
>
> Seit Juli 2023 hat Microsoft Azure Active Directory (Azure AD) in Microsoft Entra ID umbenannt. In diesem Dokument bezieht sich jeder Verweis auf Azure Active Directory, Azure AD oder AAD jetzt auf Microsoft Entra ID.

Unter Maschinenkataloge erstellen werden die Assistenten zum Erstellen eines Maschinenkatalogs beschrieben. Die folgenden Informationen beziehen sich speziell auf Microsoft Azure Resource Manager-Cloudumgebungen.

> **Hinweis:**
>
> Bevor Sie einen Microsoft Azure-Katalog erstellen, müssen Sie eine Verbindung zu Microsoft Azure hergestellt haben. Siehe Verbindung zu Microsoft Azure.

### Maschinenkatalog erstellen

Sie können einen Maschinenkatalog auf zweierlei Art erstellen:

- Maschinenkatalog unter Verwendung eines Azure Resource Manager-Images in Web Studio erstellen
- Maschinenkatalog mit PowerShell erstellen

#### Maschinenkatalog unter Verwendung eines Azure Resource Manager-Images in Web Studio erstellen

Ein Image kann ein Datenträger, ein Snapshot oder eine Imageversion einer Imagedefinition in Azure Compute Gallery sein, das zum Erstellen der VMs in einem Maschinenkatalog verwendet wird. Erstellen Sie vor dem Erstellen des Maschinenkatalogs ein Image in Azure Resource Manager. Allgemeine Informationen über Images finden Sie im Artikel Erstellen von Maschinenkatalogen.

> **Hinweis:**
>
> Die Unterstützung für die Verwendung eines Masterimages aus einer anderen Region als der in der Hostverbindung konfigurierten Region ist veraltet. Verwenden Sie Azure Compute Gallery, um das Masterimage in die gewünschte Region zu replizieren.

Während der Imagevorbereitung wird eine Vorbereitungs-VM basierend auf der ursprünglichen VM erstellt. Diese Vorbereitungs-VM ist vom Netzwerk getrennt. Zum Trennen des Netzwerks von der Vorbereitungs-VM wird eine Netzwerksicherheitsgruppe erstellt, um den gesamten eingehenden und ausgehenden Datenverkehr zu blockieren. Die Netzwerksicherheitsgruppe wird automatisch einmal pro Katalog erstellt. Der Name der Netzwerksicherheitsgruppe lautet <!JEKYLL@5300@0>, wobei die GUID nach dem Zufallsprinzip generiert wird. Beispiel: <!JEKYLL@5300@1>.

Assistent für die Maschinenkatalogerstellung:

- Die Seiten **Maschinentyp** und **Maschinenverwaltung** enthalten keine Azure-spezifischen Informationen. Folgen Sie den Anleitungen im Artikel Maschinenkataloge erstellen.
- Wählen Sie auf der Seite **Image** ein Image aus, das Sie als Vorlage für die Erstellung von Maschinen in diesem Katalog verwenden möchten.

  Wenn Sie **Masterimage** als zu verwendenden Imagetyp auswählen, klicken Sie auf **Image auswählen** und gehen Sie wie folgt vor, um bei Bedarf ein Masterimage auszuwählen:

1. (Gilt nur für Verbindungen mit innerhalb oder zwischen Mandanten freigegebenen Images) Wählen Sie das Abonnement, in dem sich das Image befindet.
2. Wählen Sie eine Ressourcengruppe.
3. Gehen Sie zur Azure-VHD, zur Azure Compute Gallery oder zur Azure-Imageversion. Fügen Sie bei Bedarf einen Hinweis für das ausgewählte Image hinzu.

Beachten Sie bei der Imageauswahl Folgendes:

- Vergewissern Sie sich, dass ein Citrix VDA auf dem Image installiert ist.
- Wenn Sie eine virtuelle Festplatte auswählen, die an eine VM angeschlossen ist, müssen Sie die VM herunterfahren, bevor Sie mit dem nächsten Schritt fortfahren.

> **Hinweis:**
>
> - Das Abonnement, das der Verbindung (Host) entspricht, die die Maschinen im Katalog erstellt hat, ist mit einem grünen Punkt gekennzeichnet. Bei den anderen Abonnements handelt es sich um diejenigen, die die Azure Compute Gallery mit diesem Abonnement teilen. In diesen Abonnements werden nur geteilte Kataloge angezeigt. Informationen zur Konfiguration freigegebener Abonnements finden Sie unter Images innerhalb eines Mandanten freigeben (abonnementübergreifend) und Images mandantenübergreifend freigeben.
> - Die Verwendung eines Maschinenprofils mit vertrauenswürdigem Start als **Sicherheitstyp** ist obligatorisch, wenn Sie ein Image oder einen Snapshot auswählen, für das bzw. den der vertrauenswürdige Start aktiviert ist. Sie können dann SecureBoot und vTPM aktivieren oder deaktivieren, indem Sie die zugehörigen Werte im Maschinenprofil angeben. Der vertrauenswürdige Start wird für Shared Image Gallery nicht unterstützt. Informationen zu vertrauenswürdigen Starts in Azure finden Sie unter https://docs.microsoft.com/en-us/azure/virtual-machines/trusted-launch.
> - Sie können ein Provisioningschema mit einem kurzlebigen Betriebssystemdatenträger unter Windows mit vertrauenswürdigem Start erstellen. Wenn Sie ein Image mit vertrauenswürdigem Start auswählen, müssen Sie ein Maschinenprofil mit vertrauenswürdigem Start auswählen, das mit vTPM aktiviert ist. Informationen zum Erstellen von Maschinenkatalogen mit kurzlebigem Betriebssystemdatenträger finden Sie unter Erstellen von Maschinen mit kurzlebigem Betriebssystemdatenträger.
> - Während der Imagereplikation können Sie das Image als Masterimage auswählen und das Setup abschließen. Die Katalogerstellung kann jedoch länger dauern, während das Image repliziert wird. MCS erfordert, dass die Replikation innerhalb einer Stunde ab Katalogerstellung abgeschlossen ist. Tritt bei der Replikation ein Timeout auf, schlägt die Katalogerstellung fehl. Sie können den Replikationsstatus in Azure überprüfen. Versuchen Sie es erneut, wenn die Replikation noch aussteht oder

> nach dem Abschluss der Replikation.
> - Wenn Sie ein Masterimage für Maschinenkataloge in Azure auswählen, bestimmt MCS den Betriebssystemtyp basierend auf dem von Ihnen ausgewählten Masterimage und Maschinenprofil. Wenn MCS den Betriebssystemtyp nicht bestimmen kann, wählen Sie den Betriebssystemtyp aus, der dem Masterimage entspricht.
> - Sie können einen VM-Katalog der zweiten Generation mithilfe eines Images der zweiten Generation bereitstellen, um die Startzeitleistung zu verbessern. Das Erstellen eines Maschinenkatalogs der zweiten Generation mit einem Image der ersten Generation wird nicht unterstützt. Das Erstellen eines Maschinenkatalogs der ersten Generation mit einem Image der zweiten Generation wird ebenfalls nicht unterstützt. Außerdem werden ältere Images ohne Generationsangabe als Image der ersten Generation behandelt.

Wenn Sie **Vorbereitetes Image** als zu verwendenden Imagetyp auswählen, klicken Sie auf **Image auswählen** und wählen Sie bei Bedarf ein vorbereitetes Image aus.

Um eine erfolgreiche VM-Erstellung sicherzustellen, vergewissern Sie sich, dass auf dem Image Citrix VDA 2311 oder höher installiert ist MCSIO auf dem VDA vorhanden ist.

Sobald Sie ein Image ausgewählt haben, wird das Kontrollkästchen **Maschinenprofil verwenden (für Azure Active Directory erforderlich)** automatisch aktiviert. Klicken Sie auf **Wählen Sie ein Maschinenprofil**, um eine VM- oder ARM-Vorlagenspezifikation aus einer Liste mit Ressourcengruppen auszuwählen. Virtuelle Maschinen im Katalog können folgende Konfigurationen vom ausgewählten Maschinenprofil übernehmen:

Validieren Sie die ARM-Vorlagenspezifikation, um sicherzustellen, dass sie als Maschinenprofil zum Erstellen eines Maschinenkatalogs verwendet werden kann. Es gibt zwei Möglichkeiten zur Validierung der ARM-Vorlagenspezifikation:

- Klicken Sie nach Auswahl der ARM-Vorlagenspezifikation aus der Liste der Ressourcengruppen auf **Weiter**. Wenn die ARM-Vorlagenspezifikation Fehler enthält, werden Fehlermeldungen angezeigt,
- Führen Sie einen der folgenden PowerShell-Befehle aus:
  - <!JEKYLL@5300@2>
  - <!JEKYLL@5300@3>

Beispiele für Konfigurationen, die VMs von einem Maschinenprofil übernehmen können:

- Beschleunigtes Netzwerk
- Startdiagnose
- Caching des Hostdatenträgers (bei OS- und MCSIO-Datenträgern)
- Maschinengröße (sofern nicht anders angegeben)
- Für VM platzierte Tags

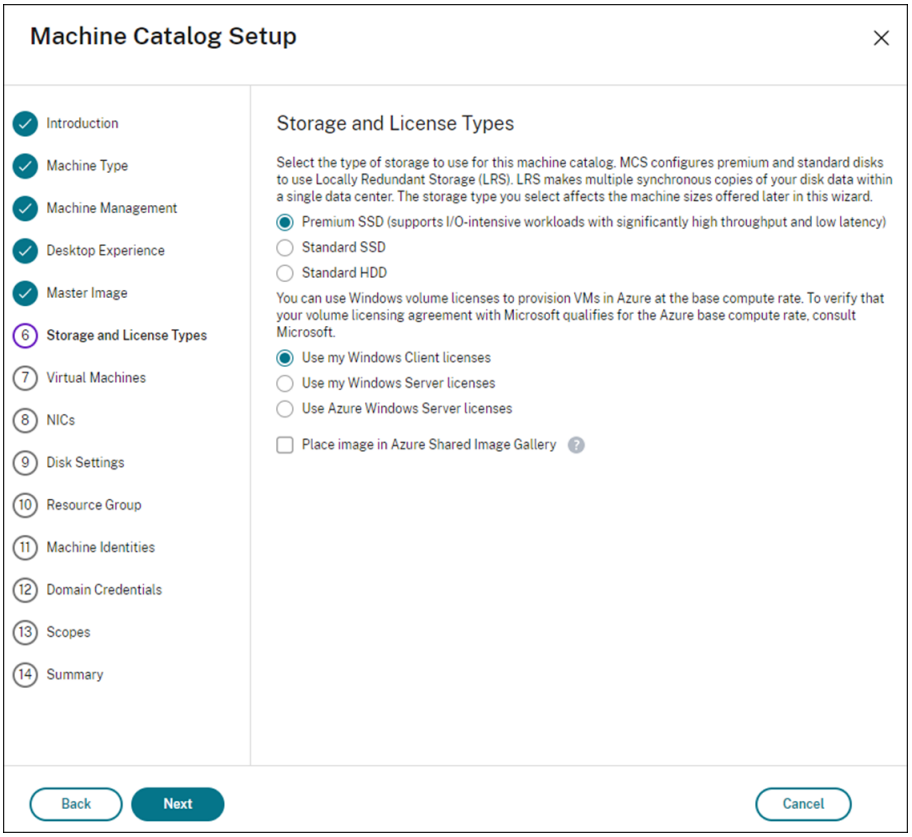
Nachdem Sie den Katalog erstellt haben, können Sie die Konfigurationen anzeigen, die das Image vom Maschinenprofil erbt. Wählen Sie auf dem Knoten **Maschinenkataloge** den Katalog aus, um die Details im unteren Bereich anzuzeigen. Klicken Sie dann auf die Registerkarte **Vorlageneigenschaften**, um die Eigenschaften des Maschinenprofils anzuzeigen. Im Abschnitt **Tags** werden bis zu drei Tags angezeigt. Zum Anzeigen aller auf der VM platzierten Tags klicken Sie auf **Alle anzeigen**.

Um VMs mit Maschinenerstellungsdiensten (MCS) auf einem dedizierten Azure-Host bereitzustellen, aktivieren Sie das Kontrollkästchen **Dedizierte Hostgruppe verwenden** und wählen dann eine Hostgruppe aus der Liste aus. Eine Hostgruppe ist eine Ressource, die eine Sammlung dedizierter Hosts darstellt. Ein dedizierter Host ist ein Dienst, der physische Server bereitstellt, die eine oder mehrere virtuelle Maschinen hosten. Ihr Server ist für Ihr Azure-Abonnement reserviert und wird nicht mit anderen Abonnenten geteilt. Bei Verwendung eines dedizierten Hosts stellt Azure sicher, dass nur Ihre VMs auf diesem Host ausgeführt werden. Dieses Feature eignet sich für Szenarios, in denen Sie regulatorische oder interne Sicherheitsanforderungen erfüllen müssen. Weitere Informationen zu Hostgruppen und Überlegungen zu ihrer Verwendung finden Sie unter Dedizierte Azure-Hosts.

> **Wichtig:**
>
> - Es werden nur Hostgruppen mit aktivierter automatischer Azure-Platzierung angezeigt.
> - Durch Verwendung einer Hostgruppe wird die Seite **Virtuelle Maschinen** geändert, die später im Assistenten angezeigt wird. Auf dieser Seite werden nur die Maschinengrößen angezeigt, die in der ausgewählten Hostgruppe enthalten sind. Außerdem sind Verfügbarkeitszonen automatisch ausgewählt und nicht wählbar.

- Die Seite **Speicher- und Lizenztypen** wird nur angezeigt, wenn Sie ein Azure Resource Manager-Image verwenden.

Seite 


Für den Maschinenkatalog können Sie die folgenden Speichertypen verwenden:

- **Premium-SSD.** Bietet Datenträgerspeicherung mit hoher Leistung und niedriger Latenz für VMs mit E/A-intensiven Workloads.
- **Standard-SSD.** Kostengünstige Speicheroption, die für Workloads geeignet ist, die eine gleichmäßige Leistung bei niedrigeren IOPS-Raten erfordern.
- **Standard-HDD.** Zuverlässiger, kostengünstiger Datenträgerspeicher, der für VMs mit latenzunempfindlichen Workloads geeignet ist.
- **Kurzlebiger Azure-Betriebsystemdatenträger**. Kostengünstige Speicheroption mit Wiederverwendung des lokalen VM-Datenträgers zum Hosten des Betriebssystemdatenträgers. Alternativ können Sie mit PowerShell Maschinen mit kurzlebigen Betriebsystemdatenträgern erstellen. Weitere Informationen finden Sie unter Kurzlebige Azure-Datenträger. Beachten Sie bei der Verwendung kurzlebiger Betriebssystemdatenträger Folgendes:
  - Kurzlebige Azure-Betriebssystemdatenträger und MCS-E/A können nicht gleichzeitig aktiviert werden.
  - Zum Aktualisieren von Maschinen, die kurzlebige Betriebssystemdatenträger verwenden, müssen Sie ein Image auswählen, dessen Größe die des Cachedatenträgers bzw. des temporären Datenträgers der VM nicht übersteigt.
  - Sie können die später im Assistenten angebotene Option **VM und Systemdatenträger**

**während Energiezyklen beibehalten** nicht verwenden.

> **Hinweis:**
>
> Der Identitätsdatenträger wird unabhängig vom gewählten Speichertyp immer mit Standard-SSD erstellt.

Der gewählte Speichertyp bestimmt, welche Maschinengrößen auf der Seite **Virtuelle Maschinen** des Assistenten angeboten werden. MCS konfiguriert Premium- und Standarddatenträger für die Verwendung von lokal redundantem Speicher (LRS). LRS erstellt mehrere synchrone Kopien Ihrer Daten in einem Datencenter. Bei kurzlebigen Azure-Betriebssystemdatenträgern wird das Betriebssystem auf dem lokalen VM-Datenträger gespeichert. 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 Windows- oder Linux-Lizenzen verwendet werden sollen.

- Windows-Lizenzen: Mit Windows-Lizenzen und Windows-Images (Azure- oder benutzerdefinierte Images) können Sie Windows-VMs in Azure zu geringeren Kosten ausführen. Es gibt zwei Arten von Lizenzen:
  - **Windows Server-Lizenz**. Ermöglicht die Verwendung Ihrer Windows Server- oder Azure Windows Server-Lizenzen und somit die Nutzung des Azure-Hybridvorteils. Einzelheiten finden Sie unter https://azure.microsoft.com/en-us/pricing/hybrid-benefit/. Der Azure-Hybridvorteil senkt die Kosten des Ausführens von VMs in Azure auf die Grundgebühr für Computekapazität, da keine Gebühren für zusätzliche Windows Server-Lizenzen aus dem Azure-Katalog erhoben werden.
  - **Windows-Clientlizenz**. Ermöglicht die Verwendung Ihrer Windows 10- und Windows 11-Lizenzen in Azure und somit die Ausführung von Windows 10- und Windows 11-VMs in Azure ohne Erfordernis zusätzlicher Lizenzen. Weitere Informationen finden Sie unter Clientzugriffslizenzen und Verwaltungslizenzen.

Sie können mit folgendem PowerShell-Befehl überprüfen, ob eine VM den Lizenzierungsvorteil nutzt: <!JEKYLL@5300@4>.

- Bei Windows Server-Lizenzen muss der Lizenztyp **Windows_Server** sein. Weitere Anweisungen finden Sie unter https://docs.microsoft.com/en-us/azure/virtual-machines/windows/hybrid-use-benefit-licensing/.

- Bei Windows-Clientlizenzen muss der Lizenztyp **Windows_Client** sein. Weitere Anweisungen finden Sie unter https://docs.microsoft.com/en-us/azure/virtual-machines/windows/windows-desktop-multitenant-hosting-deployment/.

Alternativ können Sie zur Überprüfung das PowerShell-SDK <!JEKYLL@5300@5> verwenden. Beispiel: <!JEKYLL@5300@6>. Weitere Informationen zu diesem Cmdlet finden Sie unter https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Get-ProvScheme/.

- Linux-Lizenzen: Bei Verwendung eigener Linux-Lizenzen (Bring Your Own Subscription oder BYOS) müssen Sie für die Software nicht zahlen. Die BYOS-Gebühr umfasst nur die Hardware für die Rechenleistung. Es gibt zwei Arten von Lizenzen:

  * **RHEL_BYOS**: Um den Typ RHEL_BYOS zu verwenden, aktivieren Sie Red Hat Cloud Access in Ihrem Azure-Abonnement.
  * **SLES_BYOS**: Die BYOS-Versionen von SLES beinhalten Unterstützung von SUSE.

  Sie können den LicenseType-Wert unter <!JEKYLL@5300@7> und <!JEKYLL@5300@8> auf Linux-Optionen setzen.

  Beispiel für das Festlegen von LicenseType auf RHEL_BYOS unter <!JEKYLL@5300@9>:

  <!JEKYLL@5300@10>

  Beispiel für das Festlegen von LicenseType auf SLES_BYOS unter <!JEKYLL@5300@11>:

  <!JEKYLL@5300@12>

  > **Hinweis:**
  >
  > Wenn der Wert <!JEKYLL@5300@13> leer ist, werden als Standardwert die Azure Windows-Serverlizenz oder Azure Linux-Lizenz verwendet, abhängig vom OsType-Wert.

  Beispiel für einen leeren Wert für LicenseType:

  <!JEKYLL@5300@14>

Lesen Sie die folgenden Dokumente, um mehr über Lizenztypen und ihre Vorteile zu erfahren:

- https://docs.microsoft.com/en-us/dotnet/api/microsoft.azure.management.compute.models.virtualmachine.licensetype?view=azure-dotnet
- https://docs.microsoft.com/en-us/azure/virtual-machines/linux/azure-hybrid-benefit-linux

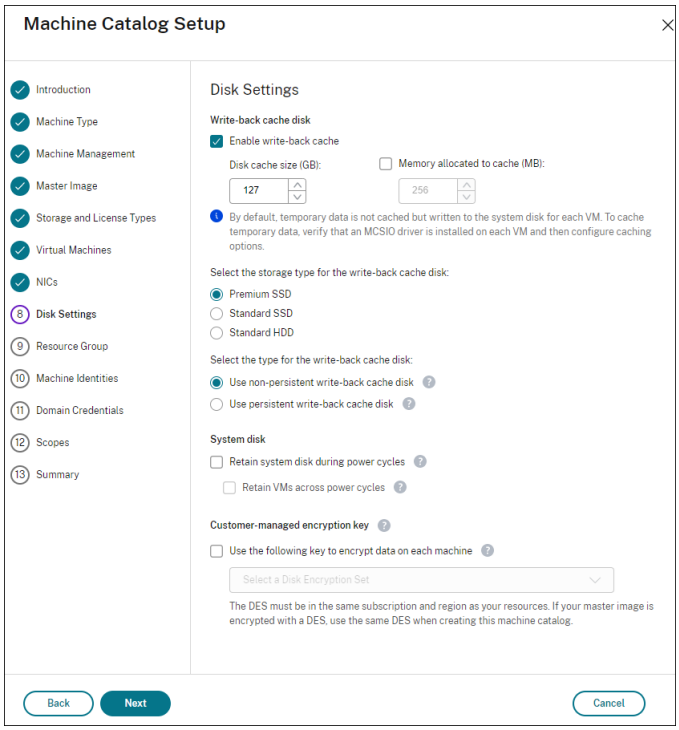
Azure Compute Gallery (früher Azure Shared Image Gallery) ist ein Repository zum Verwalten und Freigeben von Images. Damit können Sie Images in Ihrer gesamten Organisation verfügbar

machen. Wir empfehlen Ihnen, beim Erstellen großer nicht-persistenter Maschinenkataloge ein Image in SIG zu speichern, da sich VDA-Betriebssystemdatenträger dadurch schneller zurücksetzen lassen. Nachdem Sie **Vorbereitetes Image in der Azure Compute Gallery platzieren** ausgewählt haben, wird der Abschnitt **Azure Compute Gallery-Einstellungen** angezeigt, in dem Sie weitere Azure Compute Gallery-Einstellungen angeben können:

  - **Verhältnis von virtuellen Maschinen zu Imagereplikaten**. Hier können Sie das Verhältnis von virtuellen Maschinen zu Imagereplikaten angeben, die Azure beibehalten soll. Standardmäßig speichert Azure ein Imagereplikat pro 40 nicht-persistente Maschinen. Bei persistenten Maschinen ist diese Zahl voreingestellt auf 1000.
  - **Maximale Replikate**. Hier können Sie die maximale Anzahl von Image-Replikaten angeben, die Azure speichern soll. Der Standardwert ist 10.

- Geben Sie auf der Seite **VMs** an, wie viele VMs Sie erstellen möchten. Sie müssen mindestens eine VM angeben und eine Maschinengröße auswählen. Nach der Katalogerstellung können Sie die Maschinengröße durch Bearbeiten des Katalogs ändern.
- Die Seite **Netzwerkkarten** enthält keine Azure-spezifischen Informationen. Folgen Sie den Anleitungen im Artikel Maschinenkataloge erstellen.
- Wählen Sie auf der Seite **Datenträgereinstellungen**, ob der Zurückschreibcache aktiviert werden soll. Wenn die MCS-Speicheroptimierung aktiviert ist, können Sie beim Erstellen eines Katalogs folgende Einstellungen konfigurieren. Diese Einstellungen gelten für Azure- und für GCP-Umgebungen.



Nach dem Aktivieren des Zurückschreibcache können Sie Folgendes tun:

- Konfigurieren Sie die Größe des Datenträgers und des RAM, die zum Zwischenspeichern temporärer Daten verwendet werden. Weitere Informationen finden Sie unter Konfigurieren eines Cache für temporäre Daten.
- Wählen des Speichertyps für den Datenträger für den Zurückschreibcache. Die folgenden Speichertypen stehen für den Zurückschreibcache-Datenträger zur Verfügung:
  - Premium-SSD
  - Standard-SSD
  - Standard-HDD
- Wählen eines persistenten Datenträgers für den Zurückschreibcache für die bereitgestellten VMs (bei Bedarf). Wählen Sie **Zurückschreibcache aktivieren**, um die Optionen verfügbar zu machen. Die Standardeinstellung ist **Nicht-persistenten Datenträger für Zurückschreibcache verwenden**.
- Wählen Sie einen Datenträgertyp für den Zurückschreibcache aus.
  - **Nicht-persistenten Datenträger für Zurückschreibcache verwenden**. Wenn diese Option ausgewählt ist, wird der Datenträger für den Zurückschreibcache während Energiezyklen gelöscht. Alle darauf umgeleitete Daten gehen verloren. Wenn auf dem temporären Datenträger der VM ausreichend Speicherplatz vorhanden ist, wird er als Host für den Zurückschreibcachedatenträger verwendet, da dies Ihre Kosten reduziert. Nach der Katalogerstellung können Sie überprüfen, ob die bereitgestellten Maschinen den temporären Datenträger verwenden. Klicken Sie dazu auf den Katalog und überprüfen Sie die Informationen auf der Registerkarte **Vorlageneigenschaften**. Bei Verwendung des temporären Datenträgers wird für **Nicht-persistenter Datenträger für Zurückschreibcache** der Wert **Ja (mit dem temporären Datenträger der VM)** angezeigt. Wenn er nicht verwendet wird, wird für **Nicht-persistenter Datenträger für Zurückschreibcache** der Wert **Nein (nicht mit dem temporären Datenträger der VM)** angezeigt.
  - **Persistenter Datenträger für Zurückschreibcache.** Wenn diese Option ausgewählt ist, wird der Zurückschreibcache-Datenträger für die bereitgestellten VMs beibehalten. Die Aktivierung dieser Option erhöht die Speicherkosten.
- Wählen Sie aus, ob VMs und Systemdatenträger für VDAs bei Energiezyklen beibehalten werden sollen.

  **VM und Systemdatenträger während Neustarts beibehalten**. Verfügbar, wenn Sie **Zurückschreibcache aktivieren** ausgewählt haben. Standardmäßig werden VMs und die Systemdatenträger beim Herunterfahren gelöscht und beim Starten neu erstellt. Wenn Sie die VM-Neustartzeiten reduzieren möchten, wählen Sie diese Option. Allerdings erhöht die Aktivierung dieser Option auch die Speicherkosten.

- Wählen Sie aus, ob Sie **Einsparung von Speicherkosten** aktivieren möchten. Wenn diese Option aktiviert ist, wird der Speicherdatenträger beim Herunterfahren der VM auf Standard-HDD herabgestuft, um Speicherkosten zu senken. Beim Neustart wechselt die VM wieder zu den ursprünglichen Einstellungen. Die Option lässt sich auf Speicher- und Zurückschreibcache-Datenträger anwenden. Alternativ können Sie auch PowerShell verwenden. Siehe Speichertyp beim Herunterfahren einer VM zu einer niedrigeren Ebene ändern.

  > **Hinweis:**
  >
  > Bei Microsoft gelten Einschränkungen für die Änderung des Speichertyps beim Herunterfahren einer VM. Es ist auch möglich, dass Microsoft künftig Änderungen des Speichertyps blockiert. Weitere Informationen finden Sie in diesem Microsoft-Artikel.

- Wählen Sie aus, ob Daten auf den im Katalog bereitgestellten Maschinen verschlüsselt werden sollen. Die serverseitige Verschlüsselung mit einem vom Kunden verwalteten Schlüssel ermöglicht die Verwaltung der Verschlüsselung auf der Ebene verwalteter Datenträger und das Schützen von Daten auf den Maschinen im Katalog. Weitere Informationen finden Sie unter Azure-serverseitige Verschlüsselung.

- Wählen Sie auf der Seite **Ressourcengruppe** aus, ob Sie neue Ressourcengruppen erstellen oder vorhandene verwenden.

  - Wenn Sie Ressourcengruppen erstellen möchten, wählen Sie **Weiter**.
  - Wenn Sie vorhandene Ressourcengruppen verwenden möchten, wählen Sie Gruppen in der Liste **Zum Bereitstellen verfügbare Ressourcengruppen** aus. **Nicht vergessen:** Wählen Sie genügend Gruppen aus, um die Maschinen aufzunehmen, die Sie im Katalog erstellen. Wenn sie nicht ausreichen, werden Sie in einer Meldung darauf hingewiesen. 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.

- Wählen Sie auf der Seite **Maschinenidentitäten** einen Identitätstyp und konfigurieren Sie Identitäten für Maschinen in dem Katalog. Wenn Sie die VMs als **In Azure Active Directory eingebunden** festlegen, können Sie sie zu einer Azure AD-Sicherheitsgruppe hinzufügen. Verfahren:

  1. Wählen Sie im Feld **Identitätstyp** die Option **In Azure Active Directory eingebunden**. Die Option **Azure AD-Sicherheitsgruppe (optional)** wird angezeigt.
  2. Klicken Sie auf **Azure AD-Sicherheitsgruppe: Neu erstellen**.
  3. Geben Sie einen Gruppennamen ein und klicken Sie auf **Erstellen**.
  4. Folgen Sie den angezeigten Anweisungen, um sich bei Azure anzumelden.
     Wenn der Gruppenname in Azure nicht vorliegt, erscheint ein grünes Symbol. Andern-

falls erscheint eine Fehlermeldung, in der Sie aufgefordert werden, einen neuen Namen einzugeben.

5. Geben Sie das Benennungsschema für Maschinenkonten für die VMs ein.

Nach der Katalogerstellung greift Citrix Virtual Apps and Desktops für Sie auf Azure zu und erstellt die Sicherheitsgruppe und eine dynamische Mitgliedschaftsregel für die Gruppe. Basierend auf der Regel werden virtuelle Maschinen mit dem in diesem Katalog angegebenen Benennungsschema automatisch zur Sicherheitsgruppe hinzugefügt.

Um dem Katalog virtuelle Maschinen mit einem anderen Benennungsschema hinzuzufügen, müssen Sie sich bei Azure anmelden. Citrix Virtual Apps and Desktops kann dann auf Azure zugreifen und eine dynamische Mitgliedschaftsregel erstellen, die auf dem neuen Benennungsschema basiert.

Beim Löschen des Katalogs ist für das Löschen der Sicherheitsgruppe aus Azure ebenfalls eine Anmeldung bei Azure erforderlich.

- Die Seiten **Domänenanmeldeinformationen** und **Zusammenfassung** enthalten keine Azure-spezifischen Informationen. Folgen Sie den Anleitungen im Artikel Maschinenkataloge erstellen.

Schließen Sie den Assistenten ab.

### Bedingungen für die Verwendung eines temporären Azure-Datenträgers als Datenträger für den Zurückschreibcache

Sie können den temporären Azure-Datenträger nur dann als Datenträger für den Zurückschreibcache verwenden, wenn alle der folgenden Bedingungen erfüllt sind:

- Der Datenträger für den Zurückschreibcache darf nicht persistent sein, da der temporäre Azure-Datenträger nicht für persistente Daten geeignet ist.
- Die gewählte Azure-VM-Größe muss einen temporären Datenträger einschließen.
- Der kurzlebige Betriebsystemdatenträger muss nicht aktiviert sein.
- Stimmen Sie zu, dass die Datenträgerdatei für den Zurückschreibcache auf dem temporären Azure-Datenträger platziert wird.
- Der temporäre Azure-Datenträger muss größer sein als der Gesamtwert für (Größe des Datenträgers des Zurückschreibecache + reservierter Speicherplatz für Auslagerungsdatei + 1 GB Pufferspeicher).

### Szenarios mit nicht persistentem Datenträger für den Zurückschreibcache

Die folgende Tabelle enthält drei Szenarios, in denen beim Erstellen des Maschinenkatalogs der temporäre Datenträger für den Zurückschreibcache (WBC) verwendet wird.

| Szenario | Ergebnis |
| --- | --- |
| Alle Bedingungen zur Verwendung des temporären Datenträgers für den Zurückschreibcache sind erfüllt. | Die WBC-Datei <!JEKYLL@5300@15> wird auf dem temporären Datenträger abgelegt. |
| Der temporäre Datenträger hat nicht genügend Speicherplatz für den Zurückschreibcache. | Der VHD-Datenträger <!JEKYLL@5300@16> wird erstellt und die WBC-Datei <!JEKYLL@5300@17> wird auf diesem Datenträger abgelegt. |
| Der temporäre Datenträger hat genügend Speicherplatz für den Zurückschreibcache, <!JEKYLL@5300@18> ist jedoch auf **False** gesetzt. | Der VHD-Datenträger <!JEKYLL@5300@19> wird erstellt und die WBC-Datei <!JEKYLL@5300@20> wird auf diesem Datenträger abgelegt. |

### Azure-Vorlagenspezifikation erstellen

Sie können eine Azure-Vorlagenspezifikation im Azure-Portal erstellen und sie in Web Studio und in den PowerShell-Befehlen verwenden, um einen MCS-Maschinenkatalog zu erstellen oder zu aktualisieren.

Azure-Vorlagenspezifikation für eine vorhandene VM erstellen:

1. Gehen Sie zum Azure-Portal. Wählen Sie eine Ressourcengruppe und dann die VM und die Netzwerkschnittstelle aus. Klicken Sie oben im Menü **…** auf **Export template**.
2. Deaktivieren Sie das Kontrollkästchen **Include parameters**, wenn Sie eine Vorlagenspezifikation für die Katalogbereitstellung erstellen möchten.
3. Klicken Sie auf **Add to library**, um die Vorlagenspezifikation später zu ändern.
4. Geben Sie auf der Seite **Importing template** die erforderlichen Informationen wie **Name**, **Subscription**, **Subscription**, **Location** und **Version** ein. Klicken Sie auf **Next: Edit Template**.
5. Sie benötigen außerdem eine Netzwerkschnittstelle als unabhängige Ressource, wenn Sie Kataloge bereitstellen möchten. Daher müssen Sie alle <!JEKYLL@5300@21>-Elemente in der Vorlagenspezifikation entfernen. Beispiel:

   <!JEKYLL@5300@22>

6. Wählen Sie **Review + Create** und erstellen Sie die Vorlagenspezifikation.

7. Überprüfen Sie auf der Seite **Template Specs** die gerade erstellte Vorlagenspezifikation. Klicken Sie auf die Vorlagenspezifikation. Klicken Sie im linken Bereich auf **Versions**.
8. Sie können eine neue Version erstellen, indem Sie auf **Create new version** klicken. Geben Sie eine neue Versionsnummer an, nehmen Sie Änderungen an der aktuellen Vorlagenspezifikation vor und klicken Sie auf **Review + Create**, um die neue Version der Vorlagenspezifikation zu erstellen.

Mit den folgenden PowerShell-Befehlen können Sie Informationen zur Vorlagenspezifikation und Vorlagenversion abrufen:

- Um Informationen über die Vorlagenspezifikation zu erhalten, führen Sie folgenden Befehl aus:

  <!JEKYLL@5300@23>

- Um Informationen über die Version der Vorlagenspezifikation zu erhalten, führen Sie folgenden Befehl aus:

  <!JEKYLL@5300@24>

### Vorlagenspezifikation beim Erstellen oder Aktualisieren eines Katalogs verwenden

Sie können einen MCS-Maschinenkatalog erstellen oder aktualisieren, indem Sie eine Vorlagenspezifikation als Eingabe für das Maschinenprofil verwenden. Hierfür können Sie Web Studio oder PowerShell-Befehle verwenden.

- Verwendung von Web Studio: Siehe Maschinenkatalog unter Verwendung eines Azure Resource Manager-Images in Web Studio erstellen.
- Verwendung von PowerShell: Siehe Vorlagenspezifikation beim Erstellen oder Aktualisieren eines Katalogs mit PowerShell verwenden.

### Azure-serverseitige Verschlüsselung

Citrix Virtual Apps and Desktops unterstützt vom Kunden verwaltete Schlüssel für verwaltete Azure-Datenträger über Azure Key Vault. Mit dieser Unterstützung können Sie Ihre Unternehmens- und Compliance-Anforderungen verwalten, indem Sie die verwalteten Datenträger des Maschinenkatalogs mit Ihrem eigenen Schlüssel verschlüsseln. Weitere Informationen finden Sie unter Serverseitige Verschlüsselung von Azure Disk Storage.

Bei Verwendung dieses Features für verwaltete Datenträger gilt Folgendes:

- Um den Schlüssel zu ändern, mit dem ein Datenträger verschlüsselt ist, ändern Sie den aktuellen Schlüssel im <!JEKYLL@5300@25>. Alle dem <!JEKYLL@5300@26> zugeordneten Ressourcen werden dann mit dem neuen Schlüssel verschlüsselt.

- Wenn Sie den Schlüssel deaktivieren oder löschen, werden alle VMs mit Datenträgern, die den Schlüssel verwenden, automatisch heruntergefahren. Nach dem Herunterfahren können die VMs erst wieder verwendet werden, wenn Sie den Schlüssel wieder aktivieren oder einen neuen Schlüssel zuweisen. Kataloge, die den Schlüssel verwenden, können nicht aktiviert werden und Sie können solchen Katalogen keine VMs hinzufügen.

#### Wichtige Überlegungen bei der Verwendung vom Kunden verwalteter Schlüssel

Beachten Sie die folgenden Punkte bei der Verwendung dieses Features:

- Alle zu von Kunden verwalteten Schlüsseln gehörenden Ressourcen (Azure Key Vaults, Datenträgerverschlüsselungssätze, VMs, Datenträger und Snapshots) müssen demselben Abonnement und derselben Region angehören.
- Ein einmal aktivierter kundenverwalteter Schlüssel kann nicht mehr deaktiviert werden. Wenn Sie einen kundenverwalteten Schlüssel deaktivieren oder entfernen möchten, kopieren Sie alle Daten auf einen anderen verwalteten Datenträger, für den der Schlüssel nicht verwendet wird.
- Datenträger, die aus verschlüsselten benutzerdefinierten Images mit serverseitiger Verschlüsselung und einem kundenverwalteten Schlüssel erstellt wurden, müssen mit demselben kundenverwalteten Schlüssel verschlüsselt werden. Diese Datenträger müssen im selben Abonnement sein.
- Snapshots von Datenträgern, die mit serverseitiger Verschlüsselung und einem kundenverwalteten Schlüssel verschlüsselt wurden, müssen mit demselben kundenverwalteten Schlüssel verschlüsselt werden.
- Datenträger, Snapshots und Images, die mit kundenverwalteten Schlüsseln verschlüsselt wurden, können nicht in anderen Ressourcengruppen oder Abonnements verschoben werden.
- Verwaltete Datenträger, die mit Azure Disk Encryption verschlüsselt sind oder es zuvor einmal waren, können nicht mit kundenverwalteten Schlüsseln verschlüsselt werden.
- Auf der Microsoft-Website finden Sie Informationen zu Limits für Datenträgerverschlüsselungssätze pro Region.

> **Hinweis:**
>
> Weitere Informationen zum Konfigurieren der Azure-serverseitigen Verschlüsselung finden Sie unter Schnellstart: Key Vault-Erstellung mit dem Azure-Portal .

### Vom Kunden verwalteter Schlüssel für Azure

Beim Erstellen eines Maschinenkatalogs können Sie wählen, ob Daten auf den im Katalog bereitzustellenden Maschinen verschlüsselt werden sollen. Die serverseitige Verschlüsselung mit einem vom Kun-

den verwalteten Schlüssel ermöglicht die Verwaltung der Verschlüsselung auf der Ebene verwalteter Datenträger und das Schützen von Daten auf den Maschinen im Katalog. Ein Datenträgerverschlüsselungssatz (DES) repräsentiert einen vom Kunden verwalteten Schlüssel. Um das Feature zu nutzen, müssen Sie zuerst einen DES in Azure erstellen. Ein DES hat folgendes Format:

- <!JEKYLL@5300@27>

Wählen Sie einen DES aus der Liste aus. Der ausgewählte DES muss sich im selben Abonnement und in derselben Region wie Ihre Ressourcen befinden. Wenn Ihr Image mit einem DES verschlüsselt ist, verwenden Sie beim Erstellen des Maschinenkatalogs denselben DES. Sie können den DES nicht mehr ändern, wenn Sie den Katalog erstellt haben.

Wenn Sie einen Katalog mit einem Schlüssel erstellen und später den entsprechenden DES in Azure deaktivieren, können Sie die Maschinen im Katalog nicht mehr einschalten und diesem keine Maschinen mehr hinzufügen.

Weitere Informationen finden Sie unter Creating a machine catalog using customer-managed key.

### Azure-Datenträgerverschlüsselung auf dem Host

Sie können einen MCS-Maschinenkatalog mit Verschlüsselung auf dem Host erstellen. Derzeit unterstützen die Maschinenerstellungsdienste (MCS) nur den Maschinenprofilworkflow für dieses Feature. Sie können eine VM oder eine Vorlagenspezifikation als Eingabe für ein Maschinenprofil verwenden.

Bei diesem Verschlüsselungsverfahren werden Daten nicht über den Azure-Speicher verschlüsselt. Die Daten werden auf dem Hostserver verschlüsselt und dann verschlüsselt durch den Azure-Speicherserver geleitet. Es kommt also zu einer End-to-End-Verschlüsselung der Daten.

**Einschränkungen:**

Die Azure-Datenträgerverschlüsselung auf dem Host:

- wird nicht für alle Azure-Maschinengrößen unterstützt.
- ist nicht kompatibel mit der Azure-Datenträgerverschlüsselung.

Erstellen eines Maschinenkatalogs mit Verschlüsselung auf dem Host:

1. Prüfen Sie, ob die Verschlüsselung auf dem Host für Ihr Abonnement aktiviert ist. Weitere Informationen hierzu finden Sie unter https://learn.microsoft.com/en-us/rest/api/resources/features/get?tabs=HTTP/. Wenn das Feature nicht aktiviert ist, müssen Sie es für das Abonnement aktivieren. Informationen zur Aktivierung des Features für Ihr Abonnement finden Sie unter https://learn.microsoft.com/en-us/azure/virtual-machines/disks-enable-host-based-encryption-portal?tabs=azure-powershell#prerequisites/.
2. Prüfen Sie, ob die Verschlüsselung auf dem Host für die vorliegende Azure-VM-Größe unterstützt wird. Führen Sie dazu in einem PowerShell-Fenster einen der folgenden Befehle aus:

<!JEKYLL@5300@28>

<!JEKYLL@5300@29>

3. Erstellen Sie eine VM oder Vorlagenspezifikation als Eingabe für das Maschinenprofil, im Azure-Portal mit aktivierter Verschlüsselung auf dem Host.

    - Wenn Sie eine VM erstellen möchten, wählen Sie eine VM-Größe, die die Verschlüsselung auf dem Host unterstützt. Nach dem Erstellen der VM ist die VM-Eigenschaft **Encryption at host** aktiviert.
    - Wenn Sie eine Vorlagenspezifikation verwenden möchten, weisen Sie dem Parameter <!JEKYLL@5300@30> den Wert **true** unter <!JEKYLL@5300@31> zu.

4. Erstellen Sie einen MCS-Maschinenkatalog mit Maschinenprofilworkflow, indem Sie eine VM oder Vorlagenspezifikation auswählen.

    - Datenträger/Betriebssystemdatenträger: Die Verschlüsselung erfolgt über einen kundenseitig verwalteten Schlüssel und einen plattformseitig verwalteten Schlüssel.
    - Kurzlebiger Betriebssystemdatenträger: Die Verschlüsselung erfolgt nur über einen plattformseitig verwalteten Schlüssel.
    - Cache-Datenträger: Die Verschlüsselung erfolgt über einen kundenseitig verwalteten Schlüssel und einen plattformseitig verwalteten Schlüssel.

    Sie können den Maschinenkatalog mithilfe von Web Studio oder über PowerShell-Befehle erstellen.

#### Informationen zur Verschlüsselung am Host aus Maschinenprofil abrufen

Sie können Informationen zur Verschlüsselung am Host aus einem Maschinenprofil abrufen, wenn Sie den PowerShell-Befehl mit dem Parameter <!JEKYLL@5300@32> ausführen. Ist der Parameter <!JEKYLL@5300@33> **True**, dann ist die Verschlüsselung am Host für das Maschinenprofil aktiviert.

Beispiel: Wenn die Maschinenprofileingabe eine VM ist, führen Sie den folgenden Befehl aus:

<!JEKYLL@5300@34>

Beispiel: Wenn die Maschinenprofileingabe eine Vorlagenspezifikation ist, führen Sie den folgenden Befehl aus:

<!JEKYLL@5300@35>

### Doppelte Verschlüsselung auf verwalteten Datenträgern

Sie können einen Maschinenkatalog mit doppelter Verschlüsselung erstellen. Bei mit diesem Feature erstellten Katalogen werden alle Datenträger serverseitig mit plattformseitig und kundenseitig ver-

walteten Schlüsseln verschlüsselt. Sie besitzen und verwalten den Azure Key Vault, den Verschlüsselungsschlüssel und die Datenträgerverschlüsselungssätze (DES).

Die doppelte Verschlüsselung besteht aus der plattformseitigen Verschlüsselung (Standard) und der vom Kunden verwalteten Verschlüsselung. Kunden, die ein hohes Sicherheitsniveau erfordern und Risiken bezüglich des Verschlüsselungsalgorithmus, der Implementierung oder kompromittierter Schlüssel befürchten, können die doppelte Verschlüsselung wählen. Persistente Datenträger für OS und Daten, Snapshots und Images werden sämtlich im Ruhezustand doppelt verschlüsselt.

> **Hinweis:**
>
> - Sie können einen Maschinenkatalog mit Web Studio und mit PowerShell-Befehlen erstellen und aktualisieren. Informationen zu PowerShell-Befehlen finden Sie unter Maschinenkatalog mit doppelter Verschlüsselung erstellen.
> - Sie können einen nicht auf Maschinenprofilen basierenden Workflow oder einen auf Maschinenprofilen basierenden Workflow verwenden, um einen Maschinenkatalog mit doppelter Verschlüsselung zu erstellen oder zu aktualisieren.
> - Wenn Sie einen nicht auf Maschinenprofilen basierenden Workflow verwenden, um einen Maschinenkatalog zu erstellen, können Sie die gespeicherte <!JEKYLL@5300@36> wiederverwenden.
> - Wenn Sie ein Maschinenprofil verwenden, können Sie eine VM- oder Vorlagenspezifikation als Eingabe für das Maschinenprofil verwenden.

**Einschränkungen:**

- Die doppelte Verschlüsselung wird für Ultra Disk- und Premium SSD v2-Datenträgern nicht unterstützt.
- Die doppelte Verschlüsselung wird für nicht verwaltete Datenträger nicht unterstützt.
- Wenn Sie den mit einem Katalog verknüpften DiskEncryptionSet-Schlüssel deaktivieren, werden die VMs des Katalogs deaktiviert.
- Alle zu von Kunden verwalteten Schlüsseln gehörenden Ressourcen (Azure Key Vaults, Datenträgerverschlüsselungssätze, VMs, Datenträger und Snapshots) müssen demselben Abonnement und derselben Region angehören.
- Sie können maximal 50 Datenträgerverschlüsselungssätze pro Region und Abonnement erstellen.
- Sie können einen Maschinenkatalog, der bereits eine <!JEKYLL@5300@37> hat, nicht mit einer anderen <!JEKYLL@5300@38> aktualisieren.

### Azure-Ressourcengruppen

Azure Provisioning-Ressourcengruppen sind eine Methode des Provisionings von VMs, über die Benutzern Anwendungen und Desktops bereitgestellt werden. Wenn Sie einen MCS-Maschinenkatalog

erstellen, können Sie vorhandene, leere Azure-Ressourcengruppen hinzufügen oder neue erstellen. Informationen zu Azure-Ressourcengruppen finden Sie in der Dokumentation von Microsoft.

#### Verwendung von Azure-Ressourcengruppen

Es gibt keine Beschränkung für die Anzahl der virtuellen Maschinen, verwalteten Datenträger, Snapshots und Images pro Azure-Ressourcengruppe. (Die Beschränkung auf 240 VMs pro 800 verwaltete Datenträger pro Azure-Ressourcengruppe wurde entfernt.)

- Wenn Sie zum Erstellen eines Maschinenkatalogs einen Dienstprinzipal mit vollem Gültigkeitsbereich verwenden, erstellen die Maschinenerstellungsdienste nur eine Azure-Ressourcengruppe und verwenden nur diese Gruppe für den Katalog.
- Wenn Sie zum Erstellen eines Maschinenkatalogs einen Dienstprinzipal mit eingeschränktem Gültigkeitsbereich verwenden, müssen Sie eine leere, vorab erstellte Azure-Ressourcengruppe für den Katalog angeben.

### Kurzlebige Azure-Datenträger

Ein kurzlebiger Azure-Datenträger ermöglicht die Umnutzung des Cachedatenträgers oder temporären Datenträgers zum Speichern des Betriebssystemdatenträgers für eine virtuelle Azure-Maschine. Dies ist nützlich für Azure-Umgebungen, die anstelle von Standard-HDD-Datenträgern leistungsstärkere SSD-Datenträger erfordern. Informationen zum Erstellen eines Katalogs mit einem kurzlebigen Azure-Datenträger finden Sie unter Katalog mit kurzlebigem Azure-Datenträger erstellen.

> **Hinweis:**
>
> Persistente Kataloge unterstützen keine kurzlebigen Betriebssystemdatenträger.

Kurzlebige Betriebssystemdatenträger erfordern ein Provisioningschema mit verwalteten Datenträgern und Shared Image Gallery.

#### Speichern einer temporären kurzlebigen OS-Datenträgers

Sie können einen kurzlebigen OS-Datenträger auf dem Temp- bzw. Ressourcendatenträger der VM speichern. So können Sie einen kurzlebigen OS-Datenträger mit VMs verwenden, die über keinen oder nur unzureichenden Cache verfügen. Solche VMs verfügen über einen Temp- bzw. Ressourcendatenträger zum Speichern eines kurzlebigen OS-Datenträgers (z. B. <!JEKYLL@5300@39>).

Beachten Sie Folgendes:

- Kurzlebige Datenträger werden entweder auf dem VM-Cachedatenträger oder auf dem temporären bzw. Ressourcendatenträger der VM gespeichert. Die Cachedatenträger ist dem temporären Datenträger vorzuziehen, es sei denn, der Cachedatenträger ist zu klein für den Inhalt des Betriebsystemdatenträgers.
- Entsteht bei Updates ein neues Image, das größer als der Cachedatenträger und kleiner als der Temp-Datenträger ist, wird der kurzlebige OS-Datenträger durch den Temp-Datenträger der VM ersetzt.

#### Kurzlebige Azure-Betriebssystemdatenträger und MCS-Speicheroptimierung (MCS-E/A)

Kurzlebige Azure-Betriebssystemdatenträger und MCS-E/A können nicht gleichzeitig aktiviert werden.

Wichtige Punkte:

- Sie können keinen Maschinenkatalog mit gleichzeitig aktiviertem kurzlebigem Betriebssystemdatenträger und MCS-E/A erstellen.
- Die PowerShell-Parameter (<!JEKYLL@5300@40> und <!JEKYLL@5300@41>) schlagen mit entsprechender Fehlermeldung fehl, wenn Sie sie in <!JEKYLL@5300@42> oder <!JEKYLL@5300@43> auf **true** festlegen.
- Bei bestehenden Maschinenkatalogen, für die bei der Erstellung beide Features aktiviert wurden, ist weiterhin Folgendes möglich:
  - Aktualisieren des Maschinenkatalogs
  - Hinzufügen oder Löschen von VMs
  - Löschen des Maschinenkatalogs

### Azure Compute Gallery

Verwenden Sie Azure Compute Gallery (früher Azure Shared Image Gallery) als Repository mit veröffentlichten Images für per MCS bereitgestellte Maschinen in Azure. Sie können ein veröffentlichtes Image in der Image Gallery speichern, um die Erstellung und Hydration von Betriebssystemdatenträgern zu beschleunigen und die OS- und Anwendungsstartzeiten nicht persistenter VMs zu verbessern. Die Shared Image Gallery enthält die folgenden drei Elemente:

- *Gallery*: Hier werden Images gespeichert. MCS erstellt je eine Gallery für jeden Maschinenkatalog.
- *Imagedefinition*: Diese Definition enthält Informationen zum veröffentlichten Image (Betriebssystemtyp/-zustand, Azure-Region). MCS erstellt eine Imagedefinition für jedes Image, das für den Katalog erstellt wurde.

- *Imageversion:* Jedes Image in einer Shared Image Gallery kann mehrere Versionen haben, und jede Version kann mehrere Replikate in verschiedenen Regionen haben. Jedes Replikat ist eine vollständige Kopie des veröffentlichten Images.

> **Hinweis:**
>
> Die Shared Image Gallery-Funktion ist nur mit verwalteten Datenträgern kompatibel. Sie ist nicht für Legacy-Maschinenkataloge verfügbar.

Weitere Informationen finden Sie unter Übersicht über Azure Compute Gallery.

Informationen zum Erstellen oder Aktualisieren eines Maschinenkatalogs mithilfe eines Azure Compute Gallery-Images und PowerShell finden Sie unter Maschinenkatalog mit einem Azure Compute Gallery-Image erstellen oder aktualisieren.

### Vertrauliche Azure-VMs

Azure Confidential Computing-VMs stellen sicher, dass Ihr virtueller Desktop im Arbeitsspeicher verschlüsselt und bei der Verwendung geschützt ist.

Sie können MCS verwenden, um einen Katalog mit vertraulichen Azure-VMs zu erstellen. Sie müssen den Maschinenprofil-basierten Workflow verwenden, um einen solchen Katalog zu erstellen. Sie können sowohl die VM- als auch die ARM-Vorlagenspezifikation als Eingabe für das Maschinenprofil verwenden.

#### Wichtige Überlegungen zu vertraulichen VMs

Im Hinblick auf unterstützte VM-Größen und die Erstellung von Maschinenkatalogen mit vertraulichen VMs gilt es, Folgendes zu beachten:

- Unterstützte VM-Größen:
  - DCasv5-Serie
  - DCadsv5-Serie
  - ECasv5-Serie
  - ECadsv5-Serie
- Erstellen von Maschinenkatalogen mit vertraulichen VMs.
  - Sie können mithilfe von Web Studio- und PowerShell-Befehlen einen Maschinenkatalog mit vertraulichen Azure-VMs erstellen.
  - Sie müssen einen maschinenprofilbasierten Workflow verwenden, um einen Maschinenkatalog mit vertraulichen Azure-VMs zu erstellen. Sie können eine VM oder eine Vorlagenspezifikation als Maschinenprofileingabe verwenden.

- Für das Masterimage und das als Eingabe verwendete Maschinenprofil muss derselbe Sicherheitstyp aktiviert werden. Es gibt folgende Sicherheitstypen:
  - **VMGuestStateOnly**: Vertrauliche VM, bei der nur der VM-Gastzustand verschlüsselt ist
  - **DiskWithVMGuestState**: Vertrauliche VM, bei der sowohl der Betriebssystemdatenträger als auch der VM-Gastzustand mit einem plattformverwalteten oder einem vom Kunden verwalteten Schlüssel verschlüsselt sind. Es können normale und auch kurzlebige Betriebssystemdatenträger verschlüsselt werden.
- Über den Parameter "AdditionalData"können Sie Informationen zu vertraulichen VMs verschiedener Ressourcentypen, etwa verwaltete Datenträger, Snapshots, Azure Compute Gallery-Image, VM und ARM-Vorlagenspezifikation abrufen. Beispiel:

  <!JEKYLL@5300@44>

  Es gibt folgende zusätzlichen Daten:

  - DiskSecurityType
  - ConfidentialVMDiskEncryptionSetId
  - DiskSecurityProfiles

  Führen Sie folgenden Befehl aus, um die Confidential Compute-Eigenschaft für eine Maschinengröße abzurufen: <!JEKYLL@5300@45>

  Das "additional data"-Feld ist <!JEKYLL@5300@46>.
- Sie können den Sicherheitstyp eines Masterimages oder eines Maschinenprofils nicht von "vertraulich"in "nicht vertraulich"oder umgekehrt ändern.
- Für jede falsche Konfiguration erhalten Sie eine entsprechende Fehlermeldung.

#### Masterimages und Maschinenprofile vorbereiten

Bevor Sie einen Satz vertraulicher VMs erstellen, gehen Sie wie folgt vor, um ein Masterimage und ein Maschinenprofil für sie vorzubereiten:

1. Erstellen Sie im Azure-Portal eine vertrauliche VM mit bestimmten Einstellungen wie:
   - **Sicherheitstyp**: Vertrauliche virtuelle Maschinen
   - **Vertrauliche Betriebssystem-Datenträgerverschlüsselung**: Aktiviert.
   - **Schlüsselverwaltung**: Vertrauliche Datenträgerverschlüsselung mit einem plattformverwalteten Schlüssel
     Weitere Informationen zum Erstellen vertraulicher VMs finden Sie in diesem Microsoft-Artikel.

2. Bereiten Sie das Masterimage auf der erstellten VM vor. Installieren Sie die erforderlichen Anwendungen und den VDA auf der erstellten VM.

   > **Hinweis:**
   >
   > Das Erstellen vertraulicher VMs mit VHD wird nicht unterstützt. Verwenden Sie stattdessen Azure Compute Gallery, verwaltete Datenträger oder Snapshots für diesen Zweck.

3. Erstellen Sie das Maschinenprofil auf eine der folgenden Arten:

   - Verwenden Sie die in Schritt 1 erstellte vorhandene VM, wenn sie die erforderlichen Maschineneigenschaften besitzt.
   - Wenn Sie sich für eine ARM-Vorlagenspezifikation als Maschinenprofil entscheiden, erstellen Sie die Vorlagenspezifikation wie erforderlich. Konfigurieren Sie insbesondere Parameter, die Ihre Anforderungen für vertrauliche VMs erfüllen, wie *SecurityEncryptionType* und *diskEncryptionSet* (für vom Kunden verwaltete Schlüssel). Weitere Informationen finden Sie unter Azure-Vorlagenspezifikation erstellen.

     > **Hinweis:**
     >
     > – Stellen Sie sicher, dass das Masterimage und das Maschinenprofil denselben Sicherheitsschlüsseltyp haben.
     > – Um vertrauliche virtuelle Maschinen zu erstellen, die eine vertrauliche Betriebssystem-Datenträgerverschlüsselung mit einem vom Kunden verwalteten Schlüssel erfordern, stellen Sie sicher, dass die IDs des Datenträgerverschlüsselungssatzes im Masterimage und im Maschinenprofil identisch sind.

#### Vertrauliche VMs mit Web Studio- oder PowerShell-Befehlen erstellen

Um eine Reihe vertraulicher VMs zu erstellen, erstellen Sie einen Maschinenkatalog mit einem Masterimage und einem Maschinenprofil, das von der gewünschten vertraulichen VM abgeleitet wurde.

Um den Katalog mit Web Studio zu erstellen, folgen Sie den unter Maschinenkataloge erstellen beschriebenen Schritten. Beachten Sie die folgenden Überlegungen:

- Wählen Sie auf der Seite **Image** ein Masterimage und ein Maschinenprofil aus, das Sie für die Erstellung der vertraulichen VM vorbereitet haben. Die Auswahl des Maschinenprofils ist obligatorisch und es stehen nur Profile zur Auswahl, die den gleichen Sicherheitsverschlüsselungstyp wie das ausgewählte Masterimage haben.
- Auf der Seite **Virtuelle Maschinen** werden nur Maschinengrößen zur Auswahl angezeigt, die vertrauliche VMs unterstützen.
- Auf der Seite **Datenträgereinstellungen** können Sie den Datenträgerverschlüsselungssatz nicht angeben, da er vom ausgewählten Maschinenprofil übernommen wurde.

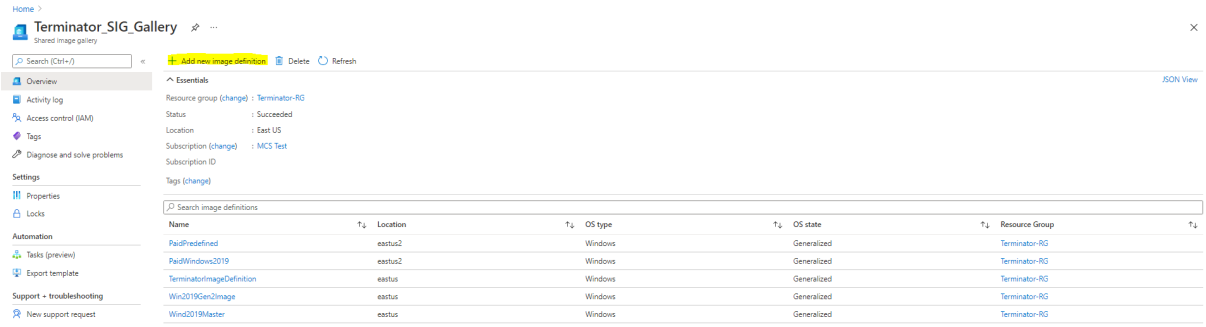
### Azure Marketplace

Citrix Virtual Apps and Desktops unterstützt die Verwendung eines Masterimages mit Abonnementinformationen zum Erstellen von Maschinenkatalogen in Azure. Weitere Informationen finden Sie unter Microsoft Azure Marketplace.

> **Tipp:**
>
> Manchen Images im Azure-Marketplace (z. B. Standard-Windows Server-Image) sind keine Abonnementinformationen angefügt. Das Citrix Virtual Apps and Desktops-Feature ist für kostenpflichtige Images vorgesehen.

#### Vergewissern Sie sich, dass das in der Shared Image Gallery erstellte Image Azure-Abonnementinformationen enthält

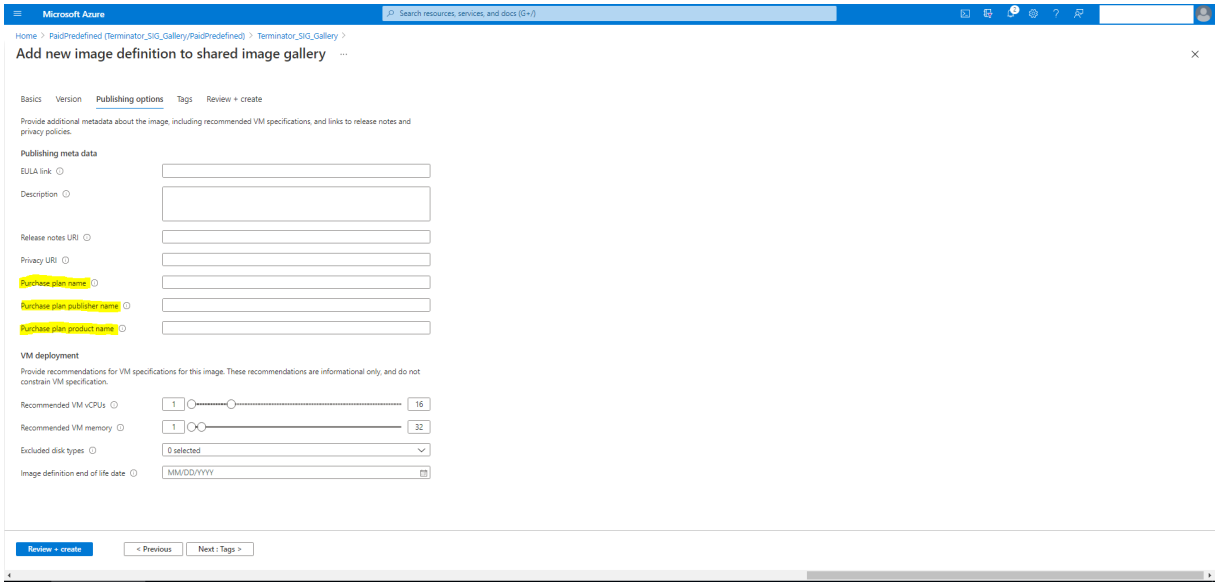
Gehen Sie wie in diesem Abschnitt beschrieben vor, um Images in der Shared Image Gallery in Web Studio anzuzeigen. Diese Images können für ein Masterimage verwendet werden. Um das Image in einer Shared Image Gallery abzulegen, erstellen Sie in der Gallery eine Imagedefinition.



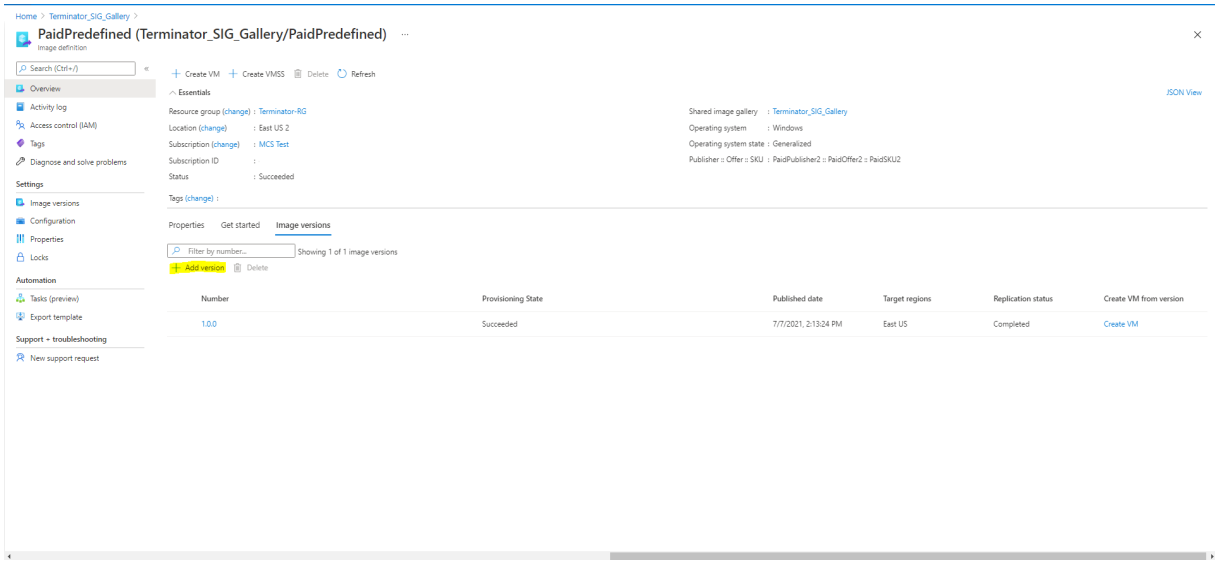

Überprüfen Sie auf der Seite **Veröffentlichungsoptionen** die Informationen zum Abonnement.

Die Informationsfelder sind zunächst leer. Füllen Sie diese Felder mit den Abonnementinformationen für das Image aus. Werden die Informationen nicht angegeben, kann der Maschinenkatalogprozess fehlschlagen.

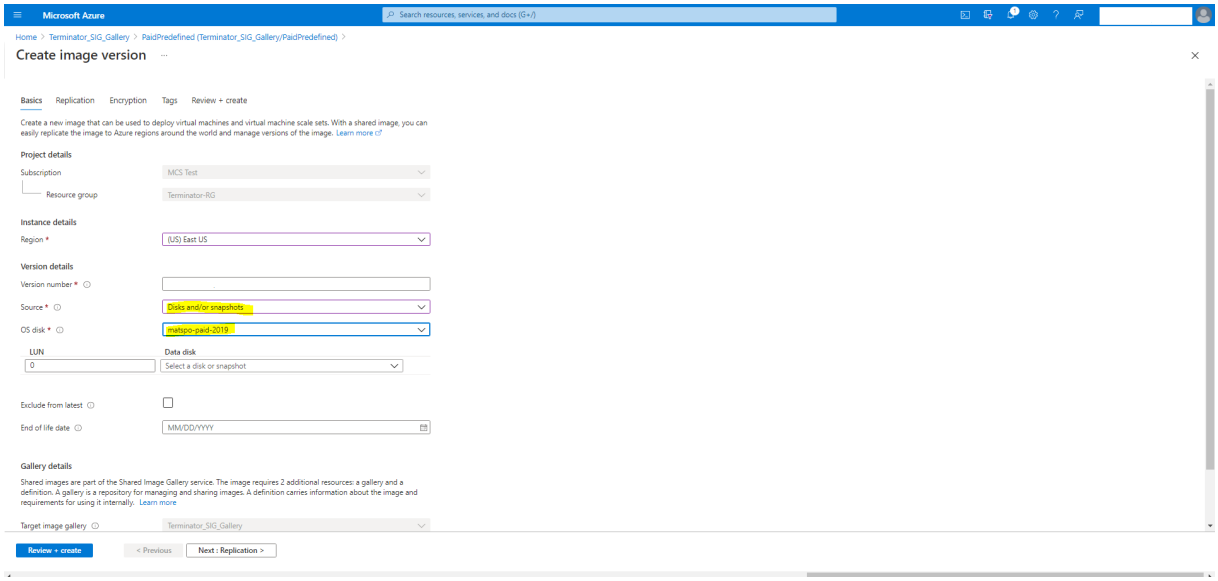



Nach dem Prüfen der Abonnementinformationen erstellen Sie eine Imageversion in der Definition. Diese wird als Masterimage verwendet. Klicken Sie auf **Add Version**:




Wählen Sie im Abschnitt **Version details** den Image-Snapshot oder verwalteten Datenträger als Quelle aus:




## Maschinenkatalog mit PowerShell erstellen

In diesem Abschnitt wird beschrieben, wie Sie Kataloge mit PowerShell erstellen:

- Katalog mit nicht-persistentem Zurückschreibcachedatenträger erstellen
- Katalog mit persistentem Zurückschreibcachedatenträger erstellen
- Startleistung mit MCSIO verbessern
- Vorlagenspezifikation beim Erstellen oder Aktualisieren eines Katalogs mit PowerShell verwenden
- Maschinenkataloge mit vertrauenswürdigem Start
- Eigenschaftswerte für Maschinenprofile verwenden
- Maschinenkatalog mit einem vom Kunden verwalteten Verschlüsselungsschlüssel erstellen
- Maschinenkatalog mit doppelter Verschlüsselung erstellen
- Katalog mit kurzlebigem Azure-Datenträger erstellen
- Dedizierte Azure-Hosts
- Maschinenkatalog mit einem Azure Compute Gallery-Image erstellen oder aktualisieren
- Shared Image Gallery konfigurieren
- Provisioning von Maschinen in spezifischen Verfügbarkeitszonen
- Speichertypen
- Speicherort der Auslagerungsdatei
- Einstellung für die Auslagerungsdatei aktualisieren
- Katalog mit Azure Spot-VMs erstellen
- Backup-VM-Größen konfigurieren
- Tags in allen Ressourcen kopieren
- Provisioning von Katalog-VMs mit installiertem Azure Monitor Agent

### Katalog mit nicht-persistentem Zurückschreibcachedatenträger erstellen

Zum Konfigurieren eines Katalogs mit nicht-persistentem Datenträger für den Zurückschreibcache verwenden Sie den PowerShell-Parameter <!JEKYLL@5300@47>. Die benutzerdefinierte Eigenschaft <!JEKYLL@5300@48> legt fest, ob der temporäre Azure-Speicher zum Speichern der Zurückschreibcachedatei verwendet werden soll. Sie muss beim Ausführen von <!JEKYLL@5300@49> auf "true" gesetzt sein, wenn Sie den temporären Datenträger als Datenträger für den Zurückschreibcache verwenden möchten. Wenn die Eigenschaft nicht festgelegt ist, wird die Standardeinstellung **False** für den Parameter verwendet.

Beispiel der Verwendung des Parameters <!JEKYLL@5300@50> zur Einstellung von <!JEKYLL@5300@51> auf **true**:

<!JEKYLL@5300@52>

> **Hinweis:**
>
> Nachdem Sie für den Maschinenkatalog den lokalen temporären Azure-Speicher als Datenträger für den Zurückschreibecache festgelegt haben, können Sie die Einstellung später nicht in VHD ändern.

### Katalog mit persistentem Zurückschreibcachedatenträger erstellen

Zum Konfigurieren eines Katalogs mit persistentem Datenträger für den Zurückschreibcache verwenden Sie den PowerShell-Parameter <!JEKYLL@5300@53>. Dieser Parameter unterstützt die zusätzliche Eigenschaft <!JEKYLL@5300@54>, welche bestimmt, ob der Zurückschreibcachedatenträger bei von MCS-bereitgestellten Maschinen persistent oder flüchtig ist. Die Eigenschaft <!JEKYLL@5300@55> wird nur verwendet, wenn der Parameter <!JEKYLL@5300@56> angegeben wird und Parameter <!JEKYLL@5300@57> so konfiguriert ist, dass ein Datenträger erstellt wird.

Beispiele für Eigenschaften im Parameter <!JEKYLL@5300@58> vor Unterstützung von <!JEKYLL@5300@59>:

<!JEKYLL@5300@60>

Berücksichtigen Sie bei Verwendung dieser Eigenschaften deren Standardwerte, wenn die Eigenschaften im Parameter <!JEKYLL@5300@61> ausgelassen werden. Die Eigenschaft <!JEKYLL@5300@62> hat zwei mögliche Werte: **true** oder **false**.

Wenn <!JEKYLL@5300@63> auf **true** festgelegt wird, wird der Zurückschreibcachedatenträger nicht gelöscht, wenn der Citrix Virtual Apps and Desktops-Administrator die Maschine mit Web Studio herunterfährt.

Wird <!JEKYLL@5300@64> auf **false** festgelegt, wird der Zurückschreibcachedatenträger gelöscht, wenn der Citrix Virtual Apps and Desktops-Administrator die Maschine mit Web Studio herunterfährt.

> **Hinweis:**
>
> Wird die Eigenschaft <!JEKYLL@5300@65> nicht angegeben, so gilt der Standardwert **false** und der Zurückschreibcachedatenträger wird bei Herunterfahren der Maschine mit Web Studio gelöscht.

Beispiel der Verwendung des Parameters <!JEKYLL@5300@66> zur Einstellung von <!JEKYLL@5300@67> auf "true":

<!JEKYLL@5300@68>

> **Wichtig:**
>
> Die Eigenschaft <!JEKYLL@5300@69> kann nur mit dem PowerShell-Cmdlet <!JEKYLL@5300@70> festgelegt werden. Eine Änderung der <!JEKYLL@5300@71> eines Provisioningschemas nach der Erstellung hat keine Auswirkungen auf den Maschinenkatalog und die Permanenz des Zurückschreibcachedatenträger beim Herunterfahren von Maschinen.

Beispiel der Einstellung von <!JEKYLL@5300@72> zur Verwendung des Zurückschreibcache und Einstellung von <!JEKYLL@5300@73> auf "true":

<!JEKYLL@5300@74>

### Startleistung mit MCSIO verbessern

Sie können die Startleistung für in Azure oder GCP verwaltete Datenträger verbessern, wenn MCSIO aktiviert ist. Verwenden Sie die benutzerdefinierte PowerShell-Eigenschaft <!JEKYLL@5300@75> im Befehl <!JEKYLL@5300@76>, um dieses Feature zu konfigurieren: Optionen für <!JEKYLL@5300@77>:

<!JEKYLL@5300@78><!JEKYLL@5300@79><!JEKYLL@5300@80>

Um dieses Feature zu aktivieren, legen Sie die benutzerdefinierte Eigenschaft <!JEKYLL@5300@81> auf <!JEKYLL@5300@82> fest. Beispiel:

<!JEKYLL@5300@83>

## Vorlagenspezifikation beim Erstellen oder Aktualisieren eines Katalogs mit PowerShell verwenden

Sie können einen MCS-Maschinenkatalog erstellen oder aktualisieren, indem Sie eine Vorlagenspezifikation als Eingabe für das Maschinenprofil verwenden. Hierfür können Sie Web Studio oder PowerShell-Befehle verwenden.

Verwendung von Web Studio: Siehe Maschinenkatalog unter Verwendung eines Azure Resource Manager-Images in Web Studio erstellen.

Mit PowerShell:

1. Öffnen Sie das **PowerShell**-Fenster.
2. Führen Sie <!JEKYLL@5300@84> aus.
3. Erstellen oder aktualisieren Sie einen Katalog.

    - Gehen Sie zum Erstellen eines Katalogs wie folgt vor:

        a) Verwenden Sie den Befehl <!JEKYLL@5300@85> mit einer Vorlagenspezifikation als Eingabe für das Maschinenprofil. Beispiel:

        <!JEKYLL@5300@86>

        b) Beenden Sie die Erstellung des Maschinenkatalogs.

    - Verwenden Sie zum Aktualisieren eines Katalogs den Befehl <!JEKYLL@5300@87> mit einer Vorlagenspezifikation als Eingabe für das Maschinenprofil. Beispiel:

    <!JEKYLL@5300@88>

### Maschinenkataloge mit vertrauenswürdigem Start

Zur problemlosen Erstellung eines Maschinenkatalogs mit vertrauenswürdigem Start verwenden Sie:

- Ein Maschinenprofil mit vertrauenswürdigem Start
- Eine VM-Größe, die vertrauenswürdigen Start unterstützt
- Eine Windows-VM-Version, die vertrauenswürdigen Start unterstützt. Derzeit unterstützen Windows 10, Windows 11, Windows Server 2016, 2019 und 2022 den vertrauenswürdigen Start.

> **Wichtig:**
>
> MCS unterstützt die Erstellung eines neuen Katalogs mit VMs, für die vertrauenswürdiger Start aktiviert ist. Um einen vorhandenen persistenten Katalog und vorhandene VMs zu aktualisieren, müssen Sie jedoch das Azure-Portal verwenden. Sie können den vertrauenswürdigen Start eines nicht persistenten Katalogs nicht aktualisieren. Weitere Informationen finden Sie im Microsoft-Dokument Enable Trusted launch on existing Azure VMs.

Führen Sie den folgenden Befehl aus, um den Bestand des Citrix Virtual Apps and Desktops-Angebots anzuzeigen und zu ermitteln, ob die VM-Größe den vertrauenswürdigen Start unterstützt:

1. Öffnen Sie ein PowerShell-Fenster.
2. Führen Sie **asnp citrix*** aus, um die Citrix-spezifischen PowerShell-Module zu laden.
3. Führen Sie den folgenden Befehl aus:

    <!JEKYLL@5300@89>

4. Führen Sie <!JEKYLL@5300@90> aus.
5. Prüfen Sie den Wert des Attributs <!JEKYLL@5300@91>.
    - Wenn <!JEKYLL@5300@92> **True** ist, unterstützt die VM-Größe den vertrauenswürdigen Start.
    - Wenn <!JEKYLL@5300@93> **False**ist, unterstützt die VM-Größe den vertrauenswürdigen Start nicht.

Bei Azure-PowerShell können Sie den folgenden Befehl verwenden, um die VM-Größen zu ermitteln, die den vertrauenswürdigen Start unterstützen:

<!JEKYLL@5300@94>

Die folgenden Beispiele veranschaulichen, welche von dem Azure PowerShell-Befehl zurückgegebenen VMs den vertrauenswürdigen Start unterstützen.

- *Beispiel 1*: Wenn die Azure-VM nur Generation 1 unterstützt, unterstützt die VM keinen vertrauenswürdigen Start. Daher wird <!JEKYLL@5300@95> nicht angezeigt, wenn Sie den Azure PowerShell-Befehl ausgeführt haben.
- *Beispiel 2*: Wenn die Azure-VM nur Generation 2 unterstützt und der Wert von <!JEKYLL@5300@96> **True** ist, unterstützt die Generation 2-VM-Größe den vertrauenswürdigen Start nicht.
- *Beispiel 3*: Wenn die Azure-VM nur Generation 2 unterstützt und <!JEKYLL@5300@97> nicht angezeigt wird, wenn Sie den PowerShell-Befehl ausgeführt haben, unterstützt die Generation 2-VM-Größe den vertrauenswürdigen Start.

Weitere Informationen zum vertrauenswürdigen Start für virtuelle Azure-Maschinen finden Sie in dem Microsoft-Dokument Vertrauenswürdiger Start für Azure-VMs.

#### Maschinenkatalog mit vertrauenswürdigem Start erstellen

1. Erstellen Sie ein Masterimage, für das vertrauenswürdiger Start aktiviert ist. Weitere Informationen finden Sie in der Microsoft-Dokumentation Unterstützte Images für VMs mit vertrauenswürdigem Start.
2. Erstellen Sie eine VM oder Vorlagenspezifikation mit Sicherheitstyp als **virtuelle Maschinen mit vertrauenswürdigem Start**. Weitere Informationen zum Erstellen einer VM oder Vorlagenspezifikation finden Sie im Microsoft-Dokument Bereitstellen eines virtuellen Computers mit vertrauenswürdigem Start.
3. Erstellen Sie einen Maschinenkatalog mit den Befehlen von Web Studio oder PowerShell.
    - Wenn Sie Web Studio verwenden möchten, lesen Sie Maschinenkatalog unter Verwendung eines Azure Resource Manager-Images in Web Studio erstellen.

- Wenn Sie PowerShell-Befehle verwenden möchten, verwenden Sie den Befehl <!JEKYLL@5300@98> mit der VM oder Vorlagenspezifikation als Maschinenprofileingabe. Eine vollständige Liste der Befehle zum Erstellen eines Katalogs finden Sie unter Erstellen eines Katalogs.

  Beispiel für <!JEKYLL@5300@99> mit VM als Maschinenprofileingabe:

  <!JEKYLL@5300@100>

  Beispiel für <!JEKYLL@5300@101> mit Vorlagenspezifikation als Maschinenprofileingabe:

  <!JEKYLL@5300@102>

**Fehler beim Erstellen von Maschinenkatalogen mit vertrauenswürdigem Start**

Beim Erstellen eines Maschinenkatalogs mit vertrauenswürdigem Start treten in den folgenden Szenarien Fehler auf:

| Szenario | Fehler |
| --- | --- |
| Sie wählen beim Erstellen eines nicht verwalteten Katalogs ein Maschinenprofil aus. | <!JEKYLL@5300@103> |
| Sie wählen beim Erstellen eines Katalogs mit einem nicht verwalteten Datenträger als Masterimage ein Maschinenprofil, das den vertrauenswürdigen Start unterstützt. | <!JEKYLL@5300@104> |
| Sie wählen beim Erstellen eines verwalteten Katalogs mit einer Masterimagequelle, deren Sicherheitstyp “vertrauenswürdiger Start”ist, kein Maschinenprofil aus. | <!JEKYLL@5300@105> |
| Sie wählen ein Maschinenprofil aus, dessen Sicherheitstyp sich von dem des Masterimages unterscheidet. | <!JEKYLL@5300@106> |
| Sie wählen eine VM-Größe, die den vertrauenswürdigen Start nicht unterstützt, verwenden aber beim Erstellen eines Katalogs ein Masterimage, das den vertrauenswürdigen Start unterstützt. | <!JEKYLL@5300@107> |

### Eigenschaftswerte für Maschinenprofile verwenden

Der Maschinenkatalog verwendet die folgenden Eigenschaften, die in den benutzerdefinierten Eigenschaften definiert sind:

- Verfügbarkeitszone
- ID der dedizierten Hostgruppe
- ID des Datenträgerverschlüsselungssatzes
- Betriebssystemtyp
- Lizenztyp
- Speichertyp

Wenn diese benutzerdefinierten Eigenschaften nicht explizit definiert sind, werden die Eigenschaftswerte über die ARM-Vorlagenspezifikation oder VM festgelegt, je nachdem, was als Maschinenprofil verwendet wird. Wenn <!JEKYLL@5300@108> nicht angegeben ist, wird der Wert über das Maschinenprofil festgelegt.

> **Hinweis:**
>
> Wenn einige der Eigenschaften im Maschinenprofil fehlen und nicht in den benutzerdefinierten Eigenschaften definiert sind, werden die Standardwerte der Eigenschaften angewendet, soweit zutreffend.

Im folgenden Abschnitt werden einige Szenarios für <!JEKYLL@5300@109> und <!JEKYLL@5300@110> beschrieben, wenn für <!JEKYLL@5300@111> entweder alle Eigenschaften definiert sind oder Werte aus dem MachineProfile abgeleitet werden.

- New-ProvScheme-Szenarios
  - Im MachineProfile sind alle Eigenschaften definiert und CustomProperties sind nicht definiert. Beispiel:

    <!JEKYLL@5300@112>

    Die folgenden Werte werden als benutzerdefinierte Eigenschaften für den Katalog festgelegt:

    <!JEKYLL@5300@113>
  - Im MachineProfile sind einige Eigenschaften definiert und CustomProperties sind nicht definiert. Beispiel: Im MachineProfile sind nur LicenseType und OsType festgelegt.

    <!JEKYLL@5300@114>

    Die folgenden Werte werden als benutzerdefinierte Eigenschaften für den Katalog festgelegt:

    <!JEKYLL@5300@115>

- Sowohl im MachineProfile als auch in CustomProperties sind alle Eigenschaften definiert. Beispiel:

  <!JEKYLL@5300@116>

  Benutzerdefinierte Eigenschaften haben Priorität. Die folgenden Werte werden als benutzerdefinierte Eigenschaften für den Katalog festgelegt:

  <!JEKYLL@5300@117>

- Einige Eigenschaften sind im MachineProfile definiert und einige Eigenschaften sind in CustomProperties definiert. Beispiel:

  * CustomProperties definieren LicenseType und StorageAccountType
  * MachineProfile definiert LicenseType, OsType und Zonen

  <!JEKYLL@5300@118>

  Die folgenden Werte werden als benutzerdefinierte Eigenschaften für den Katalog festgelegt:

  <!JEKYLL@5300@119>

- Einige Eigenschaften sind im MachineProfile definiert und einige Eigenschaften sind in CustomProperties definiert. Darüber hinaus ist ServiceOffering nicht definiert. Beispiel:

  * CustomProperties definieren StorageType
  * MachineProfile definiert LicenseType

  <!JEKYLL@5300@120>

  Die folgenden Werte werden als benutzerdefinierte Eigenschaften für den Katalog festgelegt:

  <!JEKYLL@5300@121>

- Wenn der OsType weder in CustomProperties noch im MachineProfile definiert ist, gilt Folgendes:

  * Der Wert wird aus dem Masterimage gelesen.
  * Ist das Masterimage ein nicht verwalteter Datenträger, ist der OsType auf Windows eingestellt. Beispiel:

  <!JEKYLL@5300@122>

  Der Wert aus dem Masterimage wird in die benutzerdefinierten Eigenschaften geschrieben, in diesem Fall Linux.

  <!JEKYLL@5300@123>

- Set-ProvScheme-Szenarios

- Ein vorhandener Katalog mit:
  - CustomProperties für <!JEKYLL@5300@124> und OsType
  - MachineProfile <!JEKYLL@5300@125>, das Zonen definiert
- Updates:
  - MachineProfile mpB.vm, das StorageAccountType definiert
  - Ein neuer Satz von benutzerdefinierten Eigenschaften $CustomPropertiesB, der LicenseType und OsType definiert

<!JEKYLL@5300@126>

Die folgenden Werte werden als benutzerdefinierte Eigenschaften für den Katalog festgelegt:

<!JEKYLL@5300@127>

- Ein vorhandener Katalog mit:
  - CustomProperties für S<!JEKYLL@5300@128> und OsType
  - MachineProfile <!JEKYLL@5300@129>, das StorageAccountType und LicenseType definiert
- Updates:
  - Ein neuer Satz von benutzerdefinierten Eigenschaften $CustomPropertiesB, der StorageAccountType und OsType definiert.

<!JEKYLL@5300@130>

Die folgenden Werte werden als benutzerdefinierte Eigenschaften für den Katalog festgelegt:

<!JEKYLL@5300@131>

- Ein vorhandener Katalog mit:
  - CustomProperties für <!JEKYLL@5300@132> und OsType
  - MachineProfile <!JEKYLL@5300@133>, das Zonen definiert
- Updates:
  - Ein MachineProfile mpB.vm, das StorageAccountType und LicenseType definiert
  - <!JEKYLL@5300@134> ist nicht angegeben

<!JEKYLL@5300@135>

Die folgenden Werte werden als benutzerdefinierte Eigenschaften für den Katalog festgelegt:

<!JEKYLL@5300@136>

### Provisioning von Katalog-VMs mit installiertem Azure Monitor Agent

Azure Monitoring ist ein Dienst, mit dem Sie Telemetriedaten aus Ihren Azure-und On-Premises-Umgebungen erfassen, analysieren und umsetzen können.

Azure Monitor Agent (AMA) sammelt Überwachungsdaten aus Rechenressourcen wie virtuellen Maschinen und übermittelt die Daten an Azure Monitor. Derzeit unterstützt der Dienst das Erfassen von Ereignisprotokollen sowie Syslog- und Leistungsmetriken, die dann an die Datenquellen Azure Monitor Metrics und Azure Monitor Logs gesendet werden.

Die Überwachung wird durch eindeutige Identifizierung der VMs in den Überwachungsdaten ermöglicht. Hierfür können Sie die VMs eines MCS-Maschinenkatalogs mit AMA als installierter Erweiterung bereitstellen.

#### Anforderungen

- Berechtigungen: Vergewissern Sie sich, dass Sie über die unter Erforderliche Azure-Berechtigungen angegebenen Azure-Mindestberechtigungen und über die folgenden Berechtigungen zur Verwendung von Azure Monitor verfügen:
  - <!JEKYLL@5300@137>
  - <!JEKYLL@5300@138>
  - <!JEKYLL@5300@139>
  - <!JEKYLL@5300@140>
  - <!JEKYLL@5300@141>
- Datensammlungsregel: Richten Sie eine Datensammlungsregel im Azure-Portal ein. Informationen zum Einrichten einer Datensammlungsregel finden Sie unter Create a data collection rule. Datensammlungsregeln sind plattformspezifisch (Windows oder Linux). Vergewissern Sie sich, dass Sie eine Datensammlungsregel gemäß der erforderlichen Plattform erstellen.
  AMA verwendet Datensammlungsregeln zum Verwalten der Zuordnung zwischen Ressourcen (wie VMs) und Datenquellen (wie Azure Monitor Metrics und Azure Monitor Logs).
- Standard-Workspace: Erstellen Sie einen Workspace im Azure-Portal. Informationen zum Erstellen eines Workspace finden Sie unter Create a Log Analytics workspace. Wenn Sie Protokolle und Daten sammeln, werden die Informationen in einem Workspace gespeichert. Ein Workspace hat eine eindeutige Workspace-ID und Ressourcen-ID. Der Workspace-Name muss für eine bestimmte Ressourcengruppe eindeutig sein. Nachdem Sie einen Workspace erstellt haben, konfigurieren Sie Datenquellen und Lösungen, um ihre Daten im Workspace zu speichern.
- Überwachungserweiterungen in Positivliste: Die Erweiterungen <!JEKYLL@5300@142> und <!JEKYLL@5300@143> sind von Citrix definierte Erweiterungen auf der Positivliste. Zur Anzeige

der Erweiterungen auf der Positivliste verwenden Sie den PoSH-Befehl <!JEKYLL@5300@144>.

- Masterimage: Microsoft empfiehlt, Erweiterungen von einer vorhandenen Maschine zu entfernen, bevor eine neue Maschine damit erstellt wird. Wenn die Erweiterungen nicht entfernt werden, kann dies zu unerwartetem Verhalten durch verbliebene Dateien führen. Weitere Informationen finden Sie unter If the VM is recreated from an existing VM.

Erstellen von Katalog-VMs mit aktiviertem AMA:

1. Richten Sie eine Maschinenprofilvorlage ein.
   - Wenn Sie eine VM als Maschinenprofilvorlage verwenden:
     a) Erstellen Sie eine VM im Azure-Portal.
     b) Schalten Sie die VM ein.
     c) Fügen Sie die VM der Datensammlungsregel unter **Ressourcen** hinzu. Dadurch wird der Agent auf der Vorlagen-VM installiert.

     > **Hinweis:**
     >
     > Wenn Sie einen Linux-Katalog erstellen müssen, richten Sie eine Linux-Maschine ein.

   - Wenn Sie eine Vorlagenspezifikation als Maschinenprofilvorlage verwenden möchten:
     a) Richten Sie eine Vorlagenspezifikation ein.
     b) Fügen Sie der generierten Vorlagenspezifikation die folgende Erweiterungs- und Datensammlungsregelzuordnung hinzu:

        <!JEKYLL@5300@145>

2. Erstellen oder aktualisieren Sie einen vorhandenen MCS-Maschinenkatalog.
   - Zum Erstellen eines neuen MCS-Katalogs:
     a) Wählen Sie die VM oder Vorlagenspezifikation als Maschinenprofil in Web Studio aus.
     b) Fahren Sie mit den nächsten Schritten zur Katalogerstellung fort.
   - Zum Aktualisieren eines vorhandenen MCS-Katalogs verwenden Sie die folgenden PoSH-Befehle:
     - Um die aktualisierte Maschinenprofilvorlage für neue VMs bereitzustellen, führen Sie den folgenden Befehl aus:

       <!JEKYLL@5300@146>

     - Zum Aktualisieren vorhandener VMs mit der aktualisierten Maschinenprofilvorlage:

       <!JEKYLL@5300@147>

3. Schalten Sie Katalog-VMs ein.

4. Überprüfen Sie im Azure-Portal, und ob die Überwachungserweiterung auf der VM installiert ist und ob die VM unter den Ressourcen der Datensammlungsregel angezeigt wird. Nach einigen Minuten werden die Überwachungsdaten auf dem Azure Monitor angezeigt.

#### Problembehandlung

Informationen zur Problembehandlung für Azure Monitor Agent finden Sie hier:

- https://learn.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-troubleshoot-windows-vm/
- https://learn.microsoft.com/en-us/azure/azure-resource-manager/troubleshooting/create-troubleshooting-template/

### Maschinenkatalog mit einem vom Kunden verwalteten Verschlüsselungsschlüssel erstellen

Schritte zum Erstellen eines Maschinenkatalogs mit einem vom Kunden verwalteten Verschlüsselungsschlüssel:

1. Öffnen Sie ein PowerShell-Fenster.
2. Führen Sie <!JEKYLL@5300@148> aus, um die Citrix-spezifischen PowerShell-Module zu laden.
3. Geben Sie <!JEKYLL@5300@149> ein.
4. Geben Sie <!JEKYLL@5300@150> ein.
5. Geben Sie <!JEKYLL@5300@151> ein.
6. Geben Sie <!JEKYLL@5300@152> ein, um die Liste der Datenträgerverschlüsselungssätze abzurufen.
7. Kopieren Sie die ID eines Datenträgerverschlüsselungssets.
8. Erstellen Sie die Zeichenfolge einer benutzerdefinierten Eigenschaft, die die ID des Datenträgerverschlüsselungssets enthält. Beispiel:

   <!JEKYLL@5300@153>

9. Erstellen Sie einen Identitätspool, falls noch nicht vorhanden. Beispiel:

   <!JEKYLL@5300@154>

10. Führen Sie den Befehl New-ProvScheme aus. Beispiel:

    <!JEKYLL@5300@155>

11. Beenden Sie die Erstellung des Maschinenkatalogs.

### Maschinenkatalog mit doppelter Verschlüsselung erstellen

Sie können einen Maschinenkatalog mit Web Studio und mit PowerShell-Befehlen erstellen und aktualisieren.

Schritte zum Erstellen eines Maschinenkatalogs mit doppelter Verschlüsselung:

1. Erstellen Sie einen Azure Key Vault und DES mit plattformseitig und kundenseitig verwalteten Schlüsseln. Informationen zum Erstellen eines Azure Key Vault und eines DES finden Sie unter Verwenden des Azure-Portals zum Aktivieren der doppelten Verschlüsselung von ruhenden Daten auf verwalteten Datenträgern.
2. Um die in Ihrer Hostingeinheit verfügbaren DiskEncryptionSets anzuzeigen, gehen Sie wie folgt vor:

   a) Öffnen Sie ein **PowerShell**-Fenster.
   b) Führen Sie die folgenden PowerShell-Befehle aus:

      i. <!JEKYLL@5300@156>
      ii. <!JEKYLL@5300@157>
      iii. <!JEKYLL@5300@158>
      iv. <!JEKYLL@5300@159> (z. B. azure-east)
      v. <!JEKYLL@5300@160>
      vi. <!JEKYLL@5300@161>

   Sie können eine ID des <!JEKYLL@5300@162> verwenden, um einen Katalog unter Verwendung benutzerdefinierter Eigenschaften zu erstellen oder zu aktualisieren.
3. Wenn Sie einen Maschinenprofilworkflow verwenden möchten, erstellen Sie eine VM- oder Vorlagenspezifikation als Eingabe für das Maschinenprofil.

   - Wenn Sie eine VM als Maschinenprofileingabe verwenden möchten:
     a) Erstellen Sie eine VM im Azure-Portal.
     b) Gehen Sie zu **Datenträger > Schlüsselverwaltung**, um die VM direkt mit einem <!JEKYLL@5300@163> zu verschlüsseln.
   - Wenn Sie eine Vorlagenspezifikation als Maschinenprofileingabe verwenden möchten:
     a) Fügen Sie in der Vorlage unter <!JEKYLL@5300@164> den Parameter <!JEKYLL@5300@165> hinzu und fügen Sie die ID des DES für die doppelte Verschlüsselung hinzu.
4. Erstellen Sie den Maschinenkatalog.

   - Wenn Sie Web Studio verwenden, führen Sie zusätzlich zu den Schritten unter Maschinenkataloge erstellen einen der folgenden Schritte aus.

- Wenn Sie keinen auf Maschinenprofilen basierenden Workflow verwenden, wählen Sie auf der Seite **Datenträgereinstellungen** die Option **Verwenden Sie den folgenden Schlüssel, um Daten auf jeder Maschine zu verschlüsseln**. Wählen Sie dann den DES für die doppelte Verschlüsselung aus der Dropdownliste aus. Fahren Sie mit der Erstellung des Katalogs fort.
- Wenn Sie den Maschinenprofil-Workflow verwenden, wählen Sie auf der Seite **Image** ein Masterimage und ein Maschinenprofil aus. Vergewissern Sie sich, dass die Eigenschaften des Maschinenprofils eine DES-ID enthalten.

Alle im Katalog erstellten Maschinen werden mit dem Schlüssel doppelt verschlüsselt, der dem von Ihnen ausgewählten DES zugeordnet ist.

- Wenn Sie PowerShell-Befehle verwenden, führen Sie einen der folgenden Schritte aus:
  - Wenn Sie keinen auf Maschinenprofilen basierenden Workflow verwenden, fügen Sie dem Befehl <!JEKYLL@5300@166> die benutzerdefinierte Eigenschaft <!JEKYLL@5300@167> hinzu. Beispiel:

    <!JEKYLL@5300@168>

  - Wenn Sie einen Maschinenprofil-basierten Workflow verwenden, verwenden Sie eine Maschinenprofileingabe im Befehl <!JEKYLL@5300@169>. Beispiel:

    <!JEKYLL@5300@170>

5. Schließen Sie die Katalogerstellung mit dem Remote PowerShell SDK ab. Informationen zum Erstellen eines Katalogs mit dem Remote PowerShell SDK finden Sie unter https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/. Alle im Katalog erstellten Maschinen werden mit dem Schlüssel doppelt verschlüsselt, der dem von Ihnen ausgewählten DES zugeordnet ist.

#### Unverschlüsselten Katalog zur Verwendung der doppelten Verschlüsselung konvertieren

Sie können den Verschlüsselungstyp eines Maschinenkatalogs nur aktualisieren (mithilfe benutzerdefinierter Eigenschaften oder eines Maschinenprofils), wenn der Katalog zuvor unverschlüsselt war.

- Wenn Sie keinen auf Maschinenprofilen basierenden Workflow verwenden, fügen Sie dem Befehl <!JEKYLL@5300@171> die benutzerdefinierte Eigenschaft DiskEncryptionSetId hinzu. Beispiel:

  <!JEKYLL@5300@172>

- Wenn Sie einen Maschinenprofil-basierten Workflow verwenden, verwenden Sie eine Maschinenprofileingabe im Befehl <!JEKYLL@5300@173>. Beispiel:

<!JEKYLL@5300@174>

Alle neuen VMs, die Sie dem Katalog hinzufügen, werden nun mit dem Schlüssel doppelt verschlüsselt, der dem von Ihnen ausgewählten DES zugeordnet ist.

#### Überprüfen, ob ein Katalog doppelt verschlüsselt ist

- In Web Studio:
  1. Gehen Sie zu **Maschinenkataloge**.
  2. Wählen Sie den Katalog aus, den Sie überprüfen möchten. Klicken Sie am unteren Bildschirmrand auf die Registerkarte **Vorlageneigenschaften**.
  3. Überprüfen Sie unter **Azure-Details** die DES-ID in **Datenträgerverschlüsselungssatz**. Ist die DES-ID des Katalogs leer, ist der Katalog nicht verschlüsselt.
  4. Vergewissern Sie sich im Azure-Portal, dass es sich bei dem Verschlüsselungstyp des der DES-ID zugeordneten DES um plattformseitig und kundenseitig verwaltete Schlüssel handelt.
- Mit PowerShell:
  1. Öffnen Sie das **PowerShell**-Fenster.
  2. Führen Sie <!JEKYLL@5300@175> aus, um die Citrix-spezifischen PowerShell-Module zu laden.
  3. Verwenden Sie <!JEKYLL@5300@176>, um die Informationen des Maschinenkatalogs abzurufen. Beispiel:

     <!JEKYLL@5300@177>
  4. Rufen Sie die benutzerdefinierte DES-ID-Eigenschaft des Maschinenkatalogs ab. Beispiel:

     <!JEKYLL@5300@178>
  5. Vergewissern Sie sich im Azure-Portal, dass es sich bei dem Verschlüsselungstyp des der DES-ID zugeordneten DES um plattformseitig und kundenseitig verwaltete Schlüssel handelt.

### Katalog mit kurzlebigem Azure-Datenträger erstellen

Zur Verwendung kurzlebiger Datenträger müssen Sie die benutzerdefinierte Eigenschaft <!JEKYLL@5300@179> bei der Ausführung von <!JEKYLL@5300@180> auf **true** festlegen.

> **Hinweis:**
>
> Wenn die benutzerdefinierte Eigenschaft <!JEKYLL@5300@181> auf **false** festgelegt oder kein Wert angegeben wird, verwenden alle bereitgestellten VDAs weiterhin einen bereitgestellten Betriebssystemdatenträger.

Nachfolgend finden Sie Beispiele benutzerdefinierter Eigenschaften zur Verwendung im Provisioningschema:

<!JEKYLL@5300@182>

### Kurzlebigen Datenträger für einen Katalog konfigurieren

Verwenden Sie zum Konfigurieren eines kurzlebigen Azure-Betriebssystemdatenträgers den Parameter <!JEKYLL@5300@183> in <!JEKYLL@5300@184>. Setzen Sie den Wert des Parameters <!JEKYLL@5300@185> auf **true**.

> **Hinweis:**
>
> Um dieses Feature zu nutzen, müssen Sie auch die Parameter <!JEKYLL@5300@186> und <!JEKYLL@5300@187> aktivieren.

Beispiel:

<!JEKYLL@5300@188>

### Wichtige Überlegungen für kurzlebige Datenträger

Berücksichtigen Sie die folgenden Einschränkungen, wenn Sie das Provisioning kurzlebiger Betriebssystemdatenträger mit <!JEKYLL@5300@189> durchführen:

- Die für den Katalog verwendete VM-Größe muss kurzlebige Betriebssystemdatenträger unterstützen.
- Der einer VM-Größe zugeordnete Cachedatenträger oder temporäre Datenträger muss größer oder genauso groß sein wie der Betriebssystemdatenträger.
- Der temporäre Datenträger muss größer als der Cachedatenträger sein.

Berücksichtigen Sie diese Punkte auch bei folgenden Aufgaben:

- Erstellen des Provisioningschemas.
- Ändern des Provisioningschemas.
- Aktualisieren des Images.

### Dedizierte Azure-Hosts

Sie können mit MCS das Provisioning von VMs auf dedizierten Azure-Hosts ausführen. Vor dem Provisioning von VMs auf dedizierten Azure-Hosts führen Sie folgende Schritte aus:

- Erstellen Sie eine Hostgruppe.
- Erstellen Sie Hosts in der Hostgruppe.
- Vergewissern Sie sich, dass genügend Hostkapazität für die Erstellung von Katalogen und virtuellen Maschinen reserviert ist.

Sie können einen Katalog mit Maschinen erstellen, deren Host-Tenancy über das folgende PowerShell-Skript definiert wird:

<!JEKYLL@5300@190>

Wenn Sie mit MCS virtuelle Maschinen auf dedizierten Azure-Hosts bereitstellen, berücksichtigen Sie Folgendes:

- Ein *dedizierter Host* ist eine Katalogeigenschaft und kann nach der Katalogerstellung nicht mehr geändert werden. Dedizieren für Mandanten wird derzeit in Azure nicht unterstützt.
- Bei Verwendung des Parameters <!JEKYLL@5300@191> ist eine vorkonfigurierte Azure-Hostgruppe in der Region der Hostingeinheit erforderlich.
- Die automatische Platzierung in Azure ist erforderlich. Das Feature beantragt das Onboarding des mit der Hostgruppe verknüpften Abonnements. Weitere Informationen finden Sie unter VM Scale Set on Azure Dedicated Hosts - Public Preview. Wenn die automatische Platzierung nicht aktiviert ist, tritt in MCS bei der Katalogerstellung ein Fehler auf.

### Maschinenkatalog mit einem Azure Compute Gallery-Image erstellen oder aktualisieren

Als Image zum Erstellen eines Maschinenkatalogs können Sie Images auswählen, die Sie in der Azure Compute Gallery erstellt haben.

Damit diese Images angezeigt werden, müssen Sie folgende Schritte ausführen:

1. Konfigurieren Sie eine Citrix Virtual Apps and Desktops-Site.
2. Stellen Sie eine Verbindung mit Azure Resource Manager her.
3. Erstellen Sie im Azure-Portal eine Ressourcengruppe. Weitere Informationen finden Sie unter Erstellen einer Azure Compute Gallery-Instanz über das Portal.
4. Erstellen Sie in der Ressourcengruppe eine Azure Compute Gallery.
5. Erstellen Sie in der Azure Compute Gallery eine Imagedefinition.
6. Erstellen Sie in der Imagedefinition eine Imageversion.

Verwenden Sie folgende PowerShell-Befehle, um einen Maschinenkatalog mit einem Image aus der Azure Compute Gallery zu erstellen oder zu aktualisieren:

1. Öffnen Sie ein PowerShell-Fenster.
2. Führen Sie <!JEKYLL@5300@192> aus, um die Citrix-spezifischen PowerShell-Module zu laden.
3. Wählen Sie eine Ressourcengruppe und listen Sie dann alle Kataloge in der Ressourcengruppe auf.

   <!JEKYLL@5300@193>
4. Wählen Sie einen Katalog und listen Sie dann alle Imagedefinitionen des Katalogs auf.

   <!JEKYLL@5300@194>
5. Wählen Sie eine Imagedefinition und listen Sie dann alle Imageversionen der Imagedefinition auf.

   <!JEKYLL@5300@195>
6. Zum Erstellen und Aktualisieren eines MCS-Katalogs verwenden Sie die folgenden Elemente:

   - Ressourcengruppe
   - Katalog
   - Katalogimagedefinition
   - Katalogimageversion

   Informationen zum Erstellen eines Katalogs mit dem Remote PowerShell SDK finden Sie unter https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

### Shared Image Gallery konfigurieren

Mit dem Befehl <!JEKYLL@5300@196> erstellen Sie ein Provisioningschema mit Unterstützung für Shared Image Gallery. Verwenden Sie den Befehl <!JEKYLL@5300@197>, um dieses Feature für ein Provisioningschema zu aktivieren bzw. deaktivieren und um die Replikatquote und die Anzahl maximaler Replikate zu ändern.

Zu Unterstützung der Shared Image Gallery-Funktion wurden Provisioningschemata um drei benutzerdefinierte Eigenschaften erweitert:

<!JEKYLL@5300@198>

- Legt fest, ob die Shared Image Gallery zum Speichern der veröffentlichten Images verwendet wird. Bei Auswahl von **True** wird das Image als Shared Image Gallery-Image gespeichert. Andernfalls wird es als Snapshot gespeichert.
- Gültige Werte sind **True** und **False**.

- Der Standardwert bei nicht definierter Eigenschaft ist **False**.

<!JEKYLL@5300@199>

- Definiert das Verhältnis von Maschinen zu Replikaten der Galerie-Imageversion.
- Gültige Werte sind ganze Zahlen größer als 0.
- Bei nicht definierter Eigenschaft werden Standardwerte verwendet. Der Standardwert für persistente Betriebssystemdatenträger beträgt 1000 und der Standardwert für nicht-persistente Betriebssystemdatenträger beträgt 40.

<!JEKYLL@5300@200>

- Definiert die Anzahl maximaler Replikate für jede Galerie-Imageversion.
- Gültige Werte sind ganze Zahlen größer als 0.
- Der Standardwert bei nicht definierter Eigenschaft ist 10.
- Azure unterstützt derzeit bis zu 10 Replikate pro Galerie-Imageversion. Wenn diese Eigenschaft auf einen Wert festgelegt ist, der den Azure-Höchstwert übersteigt, versucht MCS, den angegebenen Wert zu verwenden. Azure generiert einen Fehler, der von MCS protokolliert wird, und die aktuelle Replikatanzahl wird unverändert beibehalten.

> **Tipp:**
>
> Wenn Sie die Shared Image Gallery zum Speichern eines veröffentlichten Images für Kataloge verwenden, die mit MCS bereitgestellt werden, legt MCS die Anzahl der Galerie-Imageversionsreplikate basierend auf der Anzahl der Maschinen im Katalog, der Replikatquote und der Anzahl maximaler Replikate fest. Zur Berechnung der Replikatanzahl wird die Maschinenanzahl im Katalog durch die Replikatquote dividiert (und auf den nächsten Ganzzahlwert aufgerundet) und dann gemäß der Anzahl maximaler Replikate begrenzt. Ein Beispiel: Bei eine Replikatquote von 20 und einem Höchstwert von 5 wird für 0–20 Maschinen ein Replikat erstellt, für 21–40 Maschinen 2 Replikate, für 41–60 Maschinen 3 Replikate, für 61–80 Maschinen 4 Replikate und für 81 Maschinen (und mehr) 5 Replikate.

### Anwendungsfall: Aktualisieren der Shared Image Gallery-Replikatquote und der Anzahl maximaler Replikate

Der vorhandene Maschinenkatalog verwendet Shared Image Gallery. Verwenden Sie den Befehl <!JEKYLL@5300@201>, um die benutzerdefinierten Eigenschaften für alle vorhandenen Maschinen im Katalog und alle zukünftigen Maschinen zu aktualisieren:

<!JEKYLL@5300@202>

### Anwendungsfall: Konvertieren eines Snapshot-Katalogs in einen Shared Image Gallery-Katalog

Führen Sie für diesen Anwendungsfall folgende Schritte aus:

1. Führen Sie <!JEKYLL@5300@203> aus, wobei der Flag <!JEKYLL@5300@204> auf **True** gesetzt ist. Fügen Sie optional die Eigenschaften <!JEKYLL@5300@205> und <!JEKYLL@5300@206> hinzu.
2. Aktualisieren Sie den Katalog.
3. Starten Sie die Maschinen neu, um ein Update zu erzwingen.

Beispiel:

<!JEKYLL@5300@207>

> **Tipp:**
>
> Die Parameter <!JEKYLL@5300@208> und <!JEKYLL@5300@209> sind nicht erforderlich. Nachdem der Befehl <!JEKYLL@5300@210> abgeschlossen ist, wurde das Shared Image Gallery-Image noch nicht erstellt. Sobald der Katalog für die Verwendung der Galerie konfiguriert ist, speichert das nächste Katalogupdate das veröffentlichte Image in der Galerie. Der Befehl zum Katalogupdate erstellt die Galerie, das Galerie-Image und die Imageversion. Durch den Neustart der Maschinen werden sie aktualisiert, und es wird gegebenenfalls die Replikatanzahl aktualisiert. Alle vorhandenen nicht-persistenten Maschinen werden dann mit dem Shared Image Gallery-Image zurückgesetzt, und alle neu bereitgestellten Maschinen werden mit diesem Image erstellt. Der alte Snapshot wird innerhalb weniger Stunden automatisch bereinigt.

### Anwendungsfall: Konvertieren eines Shared Image Gallery-Katalogs in einen Snapshot-Katalog

Führen Sie für diesen Anwendungsfall folgende Schritte aus:

1. Führen Sie <!JEKYLL@5300@211> aus, wobei der Flag <!JEKYLL@5300@212> auf **False** gesetzt oder nicht definiert ist.
2. Aktualisieren Sie den Katalog.
3. Starten Sie die Maschinen neu, um ein Update zu erzwingen.

Beispiel:

<!JEKYLL@5300@213>

> **Tipp:**
>
> Im Gegensatz zum Update von einem Snapshot-Katalog auf einen Shared Image Gallery-Katalog sind die benutzerdefinierten Daten für jede Maschine noch nicht auf die neuen

> benutzerdefinierten Eigenschaften aktualisiert. Führen Sie den folgenden Befehl aus, um die ursprünglichen benutzerdefinierten Shared Image Gallery-Eigenschaften anzuzeigen: <!JEKYLL@5300@214>. Nach Abschluss des Befehls <!JEKYLL@5300@215> ist der Imagesnapshot noch nicht erstellt. Sobald konfiguriert ist, dass der Katalog nicht mehr die Galerie verwendet, speichert das nächste Katalogupdate das veröffentlichte Image als Snapshot. Alle vorhandenen nicht-persistenten Maschinen werden dann mit dem Snapshot zurückgesetzt, und alle neu bereitgestellten Maschinen werden aus dem Snapshot erstellt. Durch Neustart werden die Maschinen aktualisiert. Die benutzerdefinierten Maschinendaten werden dabei aktualisiert und zeigen an, dass <!JEKYLL@5300@216> auf **False** gesetzt ist. Die alten Shared Image Gallery-Assets (Galerie, Image und Version) werden automatisch innerhalb weniger Stunden bereinigt.

## Provisioning von Maschinen in spezifischen Verfügbarkeitszonen

Sie können das Provisioning von Maschinen auch in spezifischen Verfügbarkeitszonen in Azure-Umgebungen ausführen. Das ist mit PowerShell möglich.

> **Hinweis:**
>
> Wenn keine Zonen angegeben werden, lässt MCS Azure die Maschinen innerhalb der Region platzieren. Werden mehrere Zonen angegeben, verteilt MCS die Maschinen nach dem Zufallsprinzip in den Zonen.

### Verfügbarkeitszonen über PowerShell konfigurieren

Mit <!JEKYLL@5300@217> in PowerShell können Sie die Elemente des Angebots anzeigen. Um beispielsweise das *Serviceangebot Eastern US* <!JEKYLL@5300@218> anzuzeigen:

<!JEKYLL@5300@219>

Zum Anzeigen der Zonen verwenden Sie den Parameter <!JEKYLL@5300@220>:

<!JEKYLL@5300@221>

Werden keine Verfügbarkeitszone angegeben, bleibt die Art und Weise, wie Maschinen bereitgestellt werden, unverändert.

Um Verfügbarkeitszonen über PowerShell zu konfigurieren, verwenden Sie die benutzerdefinierte Eigenschaft **Zones** von <!JEKYLL@5300@222>. Die Eigenschaft **Zones** definiert eine Liste von Verfügbarkeitszonen für das Provisioning von Maschinen. Diese Zonen können eine oder mehrere Verfügbarkeitszonen enthalten. Beispiel: <!JEKYLL@5300@223> für die Zonen 1 und 3.

Verwenden Sie den Befehl <!JEKYLL@5300@224>, um die Zonen für ein Provisioningschema zu aktualisieren.

Wird eine ungültige Zone angegeben, wird das Provisioningschema nicht aktualisiert und eine Fehlermeldung mit Anweisungen zur Korrektur des ungültigen Befehls angezeigt.

> **Tipp:**
>
> Wenn Sie eine ungültige benutzerdefinierte Eigenschaft angeben, wird das Provisioningschema nicht aktualisiert und eine Fehlermeldung angezeigt.

## Speichertypen

Wählen Sie Speichertypen für virtuelle Maschinen in Azure-Umgebungen, die MCS verwenden. Für Ziel-VMs unterstützt MCS Folgendes:

- OS-Datenträger: SSD Premium, SSD oder HDD
- Zurückschreibcache-Datenträger: SSD Premium, SSD oder HDD

Berücksichtigen Sie bei Verwendung dieser Speichertypen Folgendes:

- Ihre VM muss den ausgewählten Speichertyp unterstützen.
- Wenn Ihre Konfiguration einen kurzlebigen Azure-Datenträger enthält, wird keine Option für die Einstellung des Zurückschreibcache-Datenträgers angeboten.

> **Tipp:**
>
> <!JEKYLL@5300@225> ist für einen Betriebssystemspeichertyp und mit Speicherkonto konfiguriert. <!JEKYLL@5300@226> ist für den Zurückschreibcache konfiguriert. Für einen normalen Katalog ist <!JEKYLL@5300@227> erforderlich. Wenn <!JEKYLL@5300@228> nicht konfiguriert ist, wird <!JEKYLL@5300@229> als Standard für <!JEKYLL@5300@230> verwendet.

Wenn WBCDiskStorageType nicht konfiguriert ist, wird StorageType als Standard für WBCDiskStorageType verwendet.

### Speichertypen konfigurieren

Verwenden Sie den Parameter <!JEKYLL@5300@231> in <!JEKYLL@5300@232>, um Speichertypen für VMs zu konfigurieren. Stellen Sie den Wert des Parameters <!JEKYLL@5300@233> auf einen der unterstützten Speichertypen ein.

Im Folgenden finden Sie einen Beispielsatz für den Parameter <!JEKYLL@5300@234> in einem Provisioningschema:

<!JEKYLL@5300@235>

#### Zonenredundanten Speicher aktivieren

Sie können bei der Katalogerstellung einen zonenredundanten Speicher (ZRS) auswählen. Ihre Azure Managed Disk wird dann synchron über mehrere Verfügbarkeitszonen repliziert, sodass Sie Ihre Daten bei einem Ausfall in einer Zone mithilfe der Redundanz in den übrigen Zonen wiederherstellen können.

In den benutzerdefinierten Speichertypeigenschaften können Sie **Premium_ZRS** und **Standard-SSD_ZRS** angeben. Der ZRS-Speicher kann mithilfe vorhandener benutzerdefinierter Eigenschaften oder über die Vorlage **MachineProfile** festgelegt werden. Der ZRS wird auch für den Befehl <!JEKYLL@5300@236> mit den Parametern <!JEKYLL@5300@237> und <!JEKYLL@5300@238> unterstützt und Sie können vorhandene Maschinen von LRS in ZRS ändern.

**Einschränkungen:**

- Nur für verwaltete Datenträger unterstützt
- Nur mit Premium- und Standard-SSDs unterstützt
- Keine Unterstützung mit <!JEKYLL@5300@239>
- Nur in bestimmten Regionen verfügbar.
- Beim Erstellen großer Mengen an ZRS-Datenträgern sinkt die Leistung von Azure. Fahren Sie die Maschinen daher beim ersten Einschalten gestaffelt hoch (weniger als 300 Maschinen gleichzeitig).

**Zonenredundanten Speicher als Datenträgerspeichertyp festlegen** Sie können einen zonenredundanten Speicher bei der Katalogerstellung auswählen oder den Speichertyp in einem vorhandenen Katalog aktualisieren.

**Zonenredundanten Speicher mithilfe von PowerShell-Befehlen auswählen** Wenn Sie einen neuen Katalog in Azure mit dem PowerShell-Befehl <!JEKYLL@5300@240> erstellen, verwenden Sie für <!JEKYLL@5300@241> den Wert <!JEKYLL@5300@242>.
Beispiel:

<!JEKYLL@5300@243>

Nach Auswahl dieses Werts prüft eine dynamische API, ob er ordnungsgemäß verwendet werden kann. Folgende Ausnahmen können auftreten, wenn ZRS für Ihren Katalog nicht zulässig ist:

- **StorageTypeAtShutdownNotSupportedForZrsDisks**: Die benutzerdefinierte Eigenschaft “StorageTypeAtShutdown”kann nicht mit ZRS verwendet werden.
- **StorageAccountTypeNotSupportedInRegion**: Diese Ausnahme tritt auf, wenn Sie versuchen, ZRS in einer nicht unterstützten Azure-Region zu verwenden.
- **ZrsRequiresManagedDisks**: Sie können zonenredundanten Speicher nur mit verwalteten Datenträgern verwenden.

Sie können den Datenträgerspeichertyp mit den folgenden benutzerdefinierten Eigenschaften festlegen:

- <!JEKYLL@5300@244>
- <!JEKYLL@5300@245>
- <!JEKYLL@5300@246>

> **Hinweis:**
>
> Bei der Katalogerstellung wird der Betriebssystemdatenträger <!JEKYLL@5300@247> des Maschinenprofils verwendet, wenn die benutzerdefinierten Eigenschaften nicht festgelegt sind.

## Diagnoseeinstellungen auf VMs und NICs aus einem Maschinenprofil erfassen

Sie können Diagnoseeinstellungen auf VMs und NICs aus einem Maschinenprofil erfassen, während Sie einen Maschinenkatalog erstellen, einen vorhandenen Maschinenkatalog aktualisieren und vorhandene VMs aktualisieren.

Sie können eine VM- oder Vorlagenspezifikation als Maschinenprofilquelle erstellen.

### Wichtige Schritte

1. Richten Sie die erforderlichen IDs in Azure ein. Sie müssen diese IDs in der Vorlagenspezifikation angeben.
    - Speicherkonto
    - Protokollanalysen-Workspace
    - Event Hub-Namespace mit den Standardtarifpreisen
2. Erstellen Sie eine Maschinenprofilquelle.
3. Erstellen Sie einen neuen Maschinenkatalog, aktualisieren Sie einen vorhandenen Katalog oder aktualisieren Sie vorhandene VMs.

### Erforderliche IDs in Azure einrichten

Richten Sie eine der folgenden Optionen in Azure ein:

- Speicherkonto
- Protokollanalysen-Workspace
- Event Hub-Namespace mit den Standardtarifpreisen

**Speicherkonto einrichten** Erstellen Sie ein Standardspeicherkonto in Azure. Geben Sie in der Vorlagenspezifikation die vollständige Resourcen-ID für das Speicherkonto als <!JEKYLL@5300@248> an.

Sobald VMs so eingerichtet sind, dass sie Daten im Speicherkonto protokollieren, finden Sie die Daten unter dem Container <!JEKYLL@5300@249>.

**Workspace für Protokollanalysen einrichten** Erstellen Sie einen Workspace für Protokollanalysen. Geben Sie in der Vorlagenspezifikation die vollständige Ressourcen-ID für den Protokollanalysen-Workspace als workspaceId an.

Sobald VMs so eingerichtet sind, dass sie Daten im Workspace protokollieren, können Daten unter "Protokolle"in Azure abgefragt werden. Sie können den folgenden Befehl in Azure unter "Protokolle" ausführen, um die Anzahl aller von einer Ressource protokollierten Metriken anzuzeigen:

'AzureMetrics

**Event Hub einrichten** Gehen Sie wie folgt vor, um einen Event Hub im Azure-Portal einzurichten:

1. Erstellen Sie einen Event Hub-Namespace mit den Standardtarifpreisen.
2. Erstellen Sie einen Event Hub unter dem Namespace.
3. Navigieren Sie im Event Hub zu **Aufzeichnung**. Schalten Sie den Schalter EIN, um mit dem Avro-Ausgabetyp aufzunehmen.
4. Erstellen Sie einen neuen Container in einem vorhandenen Speicherkonto, um die Protokolle zu erfassen.
5. Geben Sie in der Vorlagenspezifikation `eventHubAuthorizationRuleId` im folgenden Format an: `/subscriptions/093f4c12-704b-4b1d-8339-f339e7557f60/resourcegroups/matspo/providers/Microsoft.EventHub/namespaces/matspoeventhub/authorizationrules/RootManageSharedAccessKey`
6. Geben Sie den Namen des Event Hubs an.

Sobald VMs so eingerichtet sind, dass sie Daten im Event Hub protokollieren, werden die Daten im konfigurierten Speichercontainer erfasst.

#### Maschinenprofilquelle erstellen

Sie können eine VM- oder Vorlagenspezifikation als Maschinenprofilquelle erstellen.

**VM-basiertes Maschinenprofil mit Diagnoseeinstellungen erstellen** Wenn Sie eine VM als Maschinenprofil erstellen möchten, richten Sie zunächst die Diagnoseeinstellungen auf der

Vorlagen-VM selbst ein. Sie können die detaillierten Anweisungen in der Microsoft-Dokumentation Diagnose-Einstellungen in Azure Monitor nachlesen.

Sie können die folgenden Befehle ausführen, um zu überprüfen, ob der VM oder Netzwerkkarte jetzt Diagnoseeinstellungen zugeordnet sind:

```
az monitor diagnostic-settings list --resource-group matspo --resource
    matspo-tog-cc2659 --resource-type microsoft.network/
    networkInterfaces
<!--NeedCopy-->
```

```
az monitor diagnostic-settings list --resource-group matspo --resource
    matspo-tog-cc2 --resource-type microsoft.compute/virtualMachines
<!--NeedCopy-->
```

**Erstellen Sie ein auf Vorlagenspezifikationen basierendes Maschinenprofil mit Diagnoseeinstellungen** Wenn Sie eine VM verwenden möchten, für die bereits Diagnoseeinstellungen aktiviert sind, und sie in eine ARM-Vorlagenspezifikation exportieren möchten, werden diese Einstellungen nicht automatisch in die Vorlage aufgenommen. Sie müssen die Diagnoseeinstellungen in der ARM-Vorlage manuell hinzufügen oder ändern.

Wenn Sie jedoch eine VM als Maschinenprofil verwenden möchten, stellt MCS sicher, dass die kritischen Diagnoseeinstellungen genau erfasst und auf die Ressourcen in Ihrem MCS-Katalog angewendet werden.

1. Erstellen Sie eine Standardvorlagenspezifikation, die eine VM und mindestens eine Netzwerkkarte definiert.
2. Fügen Sie zusätzliche Ressourcen hinzu, um die Diagnoseeinstellungen gemäß der Spezifikation bereitzustellen: Microsoft.Insights diagnosticSettings. Verweisen Sie für den Bereich anhand des Namens mit einer teilweisen ID entweder auf eine VM oder eine Netzwerkkarte, die in der Vorlage enthalten ist. Um beispielsweise Diagnoseeinstellungen zu erstellen, die an eine VM mit dem Namen Test-VM in der Vorlagenspezifikation angehängt sind, geben Sie den Bereich wie folgt an:

   ```
   "scope": "microsoft.compute/virtualMachines/test-VM",
   <!--NeedCopy-->
   ```

3. Verwenden Sie die Vorlagenspezifikation als Maschinenprofilquelle.

#### Katalog mit Diagnoseeinstellungen erstellen oder aktualisieren

Nachdem Sie eine Maschinenprofilquelle erstellt haben, können Sie jetzt einen Maschinenkatalog mit einem `New-ProvScheme`-Befehl erstellen, einen vorhandenen Maschinenkatalog mit einem `Set-`

`ProvScheme`-Befehl aktualisieren und vorhandene VMs mithilfe eines `Request-ProvVMUpdate` -Befehls aktualisieren.

### Speicherort der Auslagerungsdatei

In Azure-Umgebungen wird die Auslagerungsdatei beim Erstellen der VM an einem geeigneten Speicherort eingerichtet. Die Einstellung der Auslagerungsdatei wird im Format <`page file location`>[`min size`] [`max size`] konfiguriert (Größe in MB). Weitere Informationen finden Sie in diesem Microsoft-Dokument zum Bestimmen der geeigneten Auslagerungsdatei.

Wenn Sie während der Image-Vorbereitung `ProvScheme` erstellen, wird der Speicherort der Auslagerungsdatei von MCS anhand bestimmter Regeln festgelegt. Nachdem Sie `ProvScheme` erstellt haben, gilt Folgendes:

- Das Ändern der VM-Größe wird blockiert, wenn sich die Größe der eingehenden VM von der Einstellung für die Auslagerungsdatei unterscheidet.
- Das Aktualisieren des Maschinenprofils wird blockiert, wenn sich das Dienstangebot ändert, da sich durch Aktualisierung des Maschinenprofils die Einstellung für die Auslagerungsdatei unterscheidet.
- Die Eigenschaften des kurzlebigen Betriebssystemdatenträgers (EOS) und von MCSIO können nicht geändert werden.

#### Speicherort der Auslagerungsdatei bestimmen

Da Features wie EOS und MCSIO einen bestimmten Speicherort voraussetzen, schließen sie einander aus. Die folgende Tabelle zeigt, welcher Speicherort der Auslagerungsdatei je nach Feature erwartet wird:

| Feature | Erwarteter Speicherort der Auslagerungsdatei |
|---|---|
| EOS | OS-Datenträger |
| MCSIO | Zuerst temporärer Azure-Datenträger, andernfalls Zurückschreibcache-Datenträger |

> **Hinweis:**
>
> Selbst wenn die Image-Vorbereitung getrennt von der Erstellung des Provisioningschemas erfolgt, bestimmt MCS den Speicherort der Auslagerungsdatei korrekt. Der Standardspeicherort der Auslagerungsdatei befindet sich auf dem Betriebssystemdatenträger.

**Szenarien zum Einrichten der Auslagerungsdatei**

Die Tabelle beschreibt einige mögliche Szenarien zum Einrichten der Auslagerungsdatei während der Image-Vorbereitung und beim Aktualisieren des Provisioningschemas:

| Während | Szenario | Ergebnis |
|---|---|---|
| Imagevorbereitung | Quellimage-Auslagerungsdatei wird auf dem temporären Datenträger eingerichtet, während die im Provisioningschema angegebene VM-Größe keinen temporären Datenträger hat. | Auslagerungsdatei wird auf dem Betriebssystemdatenträger gespeichert |
| Imagevorbereitung | Quellimage-Auslagerungsdatei wird auf dem Betriebssystemdatenträger eingerichtet, während die im Provisioningschema angegebene VM-Größe einen temporären Datenträger hat. | Auslagerungsdatei wird auf dem temporären Datenträger gespeichert |
| Imagevorbereitung | Quellimage-Auslagerungsdatei wird auf dem temporären Datenträger eingerichtet, während der kurzlebige Betriebssystemdatenträger im Provisioningschema aktiviert wird. | Auslagerungsdatei wird auf dem Betriebssystemdatenträger gespeichert |
| Aktualisierung des Provisioningschemas | Sie versuchen, das Provisioningschema zu aktualisieren, die ursprüngliche VM-Größe hat einen temporären Datenträger und die Ziel-VM hat keinen temporären Datenträger. | Änderung wird mit Fehlermeldung abgelehnt |

| Während | Szenario | Ergebnis |
| --- | --- | --- |
| Aktualisierung des Provisioningschemas | Sie versuchen, das Provisioningschema zu aktualisieren, die ursprüngliche VM-Größe hat keinen temporären Datenträger und die Ziel-VM hat einen temporären Datenträger. | Änderung wird mit Fehlermeldung abgelehnt |

### Einstellung für die Auslagerungsdatei aktualisieren

Sie können die Einstellung für die Auslagerungsdatei (einschließlich Speicherort und Größe) auch explizit per PowerShell-Befehl festlegen. Dadurch wird der von MCS festgelegte Wert überschrieben. Hierfür führen Sie den Befehl `New-ProvScheme` aus und fügen die folgenden benutzerdefinierten Eigenschaften hinzu:

- `PageFileDiskDriveLetterOverride`: Laufwerksbuchstabe für Speicherort der Auslagerungsdatei
- `InitialPageFileSizeInMB`: Anfangsgröße der Auslagerungsdatei (in MB)
- `MaxPageFileSizeInMB`: Maximalgröße der Auslagerungsdatei (in MB)

Beispiel für die Verwendung der benutzerdefinierten Eigenschaften:

```
-CustomProperties '<CustomProperties xmlns=" http://schemas.citrix.com
   /2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org/2001/
   XMLSchema-instance"> `
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false
   "/> `
<Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `
<Property xsi:type="StringProperty" Name="
   PageFileDiskDriveLetterOverride" Value="d"/> `
<Property xsi:type="StringProperty" Name="InitialPageFileSizeInMB"
   Value="2048"/> `
<Property xsi:type="StringProperty" Name="MaxPageFileSizeInMB" Value
   ="8196"/> `
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
   Premium_LRS"/> `
<Property xsi:type="StringProperty" Name="LicenseType" Value="
   Windows_Client"/> `
</CustomProperties>'
<!--NeedCopy-->
```

Einschränkungen:

- Sie können die Einstellung für die Auslagerungsdatei nur aktualisieren, wenn Sie mit dem Befehl

`New-ProvScheme` ein Provisioningschema erstellen. Die Einstellung für die Auslagerungsdatei kann später nicht geändert werden.

- Geben Sie alle Eigenschaften zur Einstellung der Auslagerungsdatei (`PageFileDiskDriveLetterOverr` , `InitialPageFileSizeInMB` und `MaxPageFileSizeInMB`) in den benutzerdefinierten Eigenschaften an, oder geben Sie keine davon an.
- Die Anfangsgröße der Auslagerungsdatei muss zwischen 16 MB und 16777216 MB liegen.
- Die Maximalgröße der Auslagerungsdatei muss größer oder gleich der Anfangsgröße der Auslagerungsdatei und kleiner als 16777216 MB sein.
- Dieses Feature wird in Web Studio nicht unterstützt.

## Katalog mit Azure Spot-VMs erstellen

Mit Azure Spot-VMs können Sie die ungenutzte Rechenkapazität von Azure zu erheblichen Kosteneinsparungen nutzen. Die Fähigkeit, eine Azure Spot-VM zuzuweisen, hängt jedoch von der aktuellen Kapazität und den Preisen ab. Es kann daher sein, dass Azure Ihre laufende VM entfernt, die VM nicht erstellen kann oder die VM gemäß der Entfernungsrichtlinie nicht einschaltet. Azure Spot-VMs eignen sich demgemäß gut für einige unkritische Anwendungen und Desktops. Weitere Informationen finden Sie unter Azure Spot-VMs verwenden.

### Einschränkungen

- Nicht alle VM-Größen werden für Azure Spot-VMs unterstützt. Weitere Informationen finden Sie unter Einschränkungen.

  Sie können den folgenden PowerShell-Befehl ausführen, um zu überprüfen, ob eine VM-Größe Spot-VMs unterstützt oder nicht. Wenn eine VM-Größe Spot-VM unterstützt, ist `SupportsSpotVM` **True**.

  ```
  1  (Get-Item "XDHyp:\HostingUnits\azure-res-conn2\serviceoffering.
        folder\Standard_D2ds_v4.serviceoffering"). AdditionalData
  2  <!--NeedCopy-->
  ```

- Derzeit unterstützen Azure Spot-VMs den Ruhezustand nicht.

### Voraussetzung

Beim Erstellen der Maschinenprofilquelle (VM- oder Vorlagenspezifikation) für den Azure Spot-VMs-Katalog müssen Sie Azure Spot Instance auswählen (wenn Sie eine VM verwenden) oder `priority` als `Spot` festlegen (wenn Sie die Vorlagenspezifikation verwenden).

**Schritte zum Erstellen eines Katalogs mit Azure Spot-VMs**

1. Erstellen Sie eine Maschinenprofilquelle (VM oder Startvorlage).

   - Informationen zum Erstellen einer VM über das Azure-Portal finden Sie unter Azure Spot-VMs über das Azure-Portal bereitstellen.
   - Um eine Vorlagenspezifikation zu erstellen, fügen Sie die folgenden Eigenschaften unter **resources > type: Microsoft.Compute/virtualMachines > properties** in der Vorlagenspezifikation hinzu. Beispiel:

```
"priority": "Spot",
"evictionPolicy": "Deallocate",
"billingProfile": {

"maxPrice": 0.01
 }

<!--NeedCopy-->
```

   > **Hinweis:**
   >
   > - Die Entfernungsrichtlinie kann auf **Zuweisung aufheben** oder **Löschen** lauten.
   >   - Für nicht persistente VMs legt MCS die Entfernungsrichtlinie immer auf **Löschen** fest. Wenn die VM entfernt wird, wird sie zusammen mit allen nicht persistenten Datenträgern (z. B. OS-Datenträger) gelöscht. Alle persistenten Datenträger (z. B. Identitätsdatenträger) werden nicht gelöscht. Ein OS-Datenträger ist jedoch persistent, wenn der Katalogtyp persistent ist oder die benutzerdefinierte Eigenschaft `PersistOsDisk` auf True gesetzt ist. Analog dazu ist ein WBC-Datenträger persistent, wenn die benutzerdefinierte Eigenschaft `PersistWbc` auf **True** gesetzt ist.
   >   - Für persistente VMs legt MCS die Entfernungsrichtlinie immer auf "Zuordnung aufheben"fest. Wenn die VM entfernt wird, wird ihre Zuordnung aufgehoben. An den Datenträgern werden keine Änderungen vorgenommen.
   > - Der Höchstpreis ist der Preis, den Sie pro Stunde zu zahlen bereit sind. Wenn Sie **Nur Kapazität** verwenden, ist dies **-1**. Der Höchstpreis kann nur Null, -1 oder eine Dezimalzahl größer als Null sein. Weitere Informationen finden Sie unter Preisgestaltung.

2. Sie können den folgenden PowerShell-Befehl ausführen, um zu überprüfen, ob ein Maschinenprofil Azure Spot-VM-fähig ist oder nicht. Wenn der Parameter `SpotEnabled` auf **True** und `SpotEvictionPolicy` auf **Deallocate** oder **Delete** gesetzt ist, ist das Maschinenprofil für Azure Spot-VM aktiviert. Beispiel:

   - Wenn es sich bei der Maschinenprofilquelle um eine VM handelt, führen Sie den folgenden Befehl aus:

```
(Get-Item "XDHyp:\HostingUnits\azure-res-conn2\machineprofile
    .folder\fifthcolumn.resourcegroup\kb-spot-delete.vm").
    AdditionalData
<!--NeedCopy-->
```

- Wenn die Maschinenprofilquelle eine Vorlagenspezifikation ist, führen Sie den folgenden Befehl aus:

```
(Get-Item "XDHyp:\HostingUnits\azure-res-conn2\machineprofile
    .folder\fifthcolumn.resourcegroup\fc-aeh-templatespec.
    templatespec\14.0.0-spot-delete.templatespecversion").
    AdditionalData
<!--NeedCopy-->
```

3. Erstellen Sie einen Maschinenkatalog unter Verwendung eines Maschinenprofils mit dem PowerShell-Befehl `New-ProvScheme`.

Mit dem Befehl `Set-ProvScheme` können Sie einen Katalog aktualisieren. Vorhandene VMs können Sie auch mit dem PowerShell-Befehl `Set-ProvVmUpdateTimeWindow` aktualisieren. Das Maschinenprofil wird beim nächsten Einschalten aktualisiert.

#### Entfernen von VMs auf einer laufenden Azure Spot-VM

Wenn die Rechenkapazität nicht verfügbar ist oder der Preis pro Stunde höher ist als der konfigurierte Höchstpreis, entfernt Azure eine laufende Spot-VM. Standardmäßig werden Sie nicht über einen Entfernungsvorgang informiert. Die VM friert einfach ein und wird entfernt. Microsoft empfiehlt, geplante Ereignisse zur Überwachung von Entfernungsvorgängen zu verwenden. Weitere Informationen finden Sie unter Entfernungsvorgänge kontinuierlich überwachen. Sie können auch Skripts von einer VM aus ausführen, um vor dem Entfernen eine Benachrichtigung zu erhalten. Microsoft bietet beispielsweise das Python-Abfrageskript ScheduledEvents.cs.

#### Problembehandlung

- Mit dem Befehl `Get-ProvVM` können Sie die Spot-VM-Eigenschaften in den customMachineData der bereitgestellten VM anzeigen. Wenn das Feld "Priorität"auf **Spot** gesetzt ist, wird Spot verwendet.
- Sie können im Azure-Portal überprüfen, ob eine VM Spot verwendet:
  1. Suchen Sie die VM im Azure-Portal.
  2. Gehen Sie zur **Übersichtsseite**.
  3. Scrollen Sie nach unten und suchen Sie den Abschnitt **Azure Spot**.

  - Wenn Spot nicht verwendet wird, ist dieses Feld leer.
  - Wenn Spot verwendet wird, sind die Felder **Azure Spot** und **Azure Spot-Entfernungsrichtlinie** gesetzt.

1. Sie können das Abrechnungsprofil oder den Höchstpreis pro Stunde für die VM auf der Konfigurationsseite überprüfen.

### Backup-VM-Größen konfigurieren

In einer öffentlichen Cloud kann die Kapazität für eine bestimmte VM-Größe manchmal knapp werden. Wenn Sie Azure Spot-VMs verwenden, werden die VMs je nach Kapazitätsanforderungen von Azure jederzeit entfernt. Wenn die Kapazität auf Azure nicht ausreicht oder die Spot-VM beim Einschalten ausfällt, greift MCS auf die Backup-VM-Größe zurück. Sie können über die benutzerdefinierte Eigenschaft `BackupVmConfiguration` eine Liste der Backup-VM-Größen bereitstellen, während Sie einen MCS-Maschinenkatalog erstellen oder aktualisieren. MCS versucht, auf die Backup-VM-Größen in der Reihenfolge zurückzugreifen, die Sie in der Liste angegeben haben.

Wenn MCS eine bestimmte Backup-Konfiguration für die VM verwendet, bleibt diese Konfiguration bis zum nächsten Shutdown aktiv. Beim nächsten Einschalten versucht MCS, die primäre VM-Konfiguration zu starten. Tritt ein Fehler auf, versucht MCS erneut, eine Konfiguration für die Backup-VM-Größe gemäß der Liste zu starten.

Dieses Feature wird für folgende Elemente unterstützt:

- einen Katalog, der ein Maschinenprofil verwendet
- persistente und nicht persistente MCS-Maschinenkataloge
- Azure-Umgebungen aktuell

#### Wichtige Überlegungen

- Sie können mehr als eine Backup-VM-Größe in der Liste angeben.
- Die Liste muss eindeutig sein.
- Sie können die Instanztypeigenschaft für jede VM in der Liste hinzufügen. Der Typ ist entweder **Spot** oder **Regulär**. Wenn der Typ nicht angegeben ist, betrachtet MCS die VM als **Regulär**.
- Sie können die Liste der Backup-VM-Größen eines vorhandenen Katalogs mit `Set-ProvScheme`-PowerShell-Befehlen ändern.
- Sie können die vorhandenen VMs, die anhand des mit dem Katalog verknüpften Provisioningschemas erstellt wurden, mit dem Befehl `Set-ProvVMUpdateTimeWindow` aktualisieren.
- Sie können die Liste der Backup-VM-Größen für eine ausgewählte Anzahl vorhandener MCS-VMs mit dem Befehl `Set-ProvVM` konfigurieren. Um jedoch die Aktualisierungen anzuwenden,

legen Sie mit `Set-ProvVMUpdateTimeWindow` ein Aktualisierungszeitfenster für die verwendeten VMs fest und starten Sie sie innerhalb des Fensters. Wenn der Befehl `Set-ProvVm` auf einer VM ausgeführt wird, verwendet die VM die auf ihr festgelegte Backup-VM-Größenliste weiterhin, auch wenn die Liste im Provisioningschema später aktualisiert wird. Sie können `Set-ProvVM` mit `-RevertToProvSchemeConfiguration` ausführen, damit die VM die Backupliste im Provisioningschema verwendet.

#### Katalog mit Backup-VM-Größen erstellen

1. Öffnen Sie ein **PowerShell**-Fenster.
2. Führen Sie `asnp citrix*` aus, um die Citrix-spezifischen PowerShell-Module zu laden.
3. Erstellen Sie einen Brokerkatalog. In diesem Katalog sind Maschinen eingetragen, die gerade erstellt werden.
4. Erstellen Sie einen Identitätspool. Dieser wird zu einem Container für AD-Konten, die für die zu erstellenden Maschinen erstellt wurden.
5. Erstellen Sie ein Provisioningschema mit dem Maschinenprofil. Beispiel:

   - Wenn Sie nur eine Liste mit regulären VM-Größen bereitstellen möchten, führen Sie Folgendes aus:

```
New-ProvScheme -ProvisioningSchemeName "azure-catalog" -
    MasterImageVM "XDHyp:\HostingUnits\azure-zones\image.
    folder\helenli.resourcegroup\helenli-master1-mcsio-
    snapshot.snapshot"
-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=`"LicenseType`"
    Value=`"Windows_Server`"/>
<Property xsi:type=`"StringProperty`" Name=`"PersistWBC`"
    Value=`"true`"/>  <Property xsi:type=`"StringProperty`"
    Name=`"BackupVmConfiguration`" Value=`"['ServiceOffering':
     'Standard_D2as_v4', 'ServiceOffering': 'Standard_D2s_v3',
     'ServiceOffering': 'C']`"/>
</CustomProperties>"
<!--NeedCopy-->
```

   - Wenn Sie eine Liste gemischter VM-Größen (reguläre und Spot-VMs) bereitstellen möchten, führen Sie Folgendes aus:

```
New-ProvScheme -ProvisioningSchemeName "azure-catalog" -
    MasterImageVM "XDHyp:\HostingUnits\azure-zones\image.
    folder\helenli.resourcegroup\helenli-master1-mcsio-
    snapshot.snapshot"
-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=`"LicenseType`"
    Value=`"Windows_Server`"/>
<Property xsi:type=`"StringProperty`" Name=`"PersistWBC`"
    Value=`"true`"/>  <Property xsi:type=`"StringProperty`"
    Name=`"BackupVmConfiguration`" Value=`"[{
'ServiceOffering': 'Standard_D2as_v4', 'Type': 'Spot' }
, {
'ServiceOffering': 'Standard_D2s_v3', 'Type': 'Regular' }
, {
'ServiceOffering': 'Standard_D2s_v3', 'Type': 'Spot' }
]`"/>
</CustomProperties>"
<!--NeedCopy-->
```

6. Aktualisieren Sie den Brokerkatalog mit der eindeutigen ID des Provisioningschemas.
7. Erstellen Sie virtuelle Maschinen und fügen Sie sie dem Katalog hinzu.

#### Vorhandenen Katalog aktualisieren

Sie können mit dem Befehl `Set-ProvScheme` ein Provisioningschema aktualisieren. Beispiel:

```
Set-ProvScheme -ProvisioningSchemeName "azure-catalog"
-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=`"LicenseType`" Value=`"
    Windows_Server`"/>
<Property xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"true`
    "/>
<Property xsi:type=`"StringProperty`" Name=`"BackupVmConfiguration`"
    Value=`"[{
 'ServiceOffering': 'Standard_D2as_v4', 'Type': 'Spot' }
 , {
```

```
 'ServiceOffering': 'Standard_D2s_v3', 'Type': 'Regular' }
 , {
 'ServiceOffering': 'Standard_D2s_v3', 'Type': 'Spot' }
 ]`"/>
</CustomProperties>"
<!--NeedCopy-->
```

### Vorhandene VMs aktualisieren

Sie können vorhandene VMs in einem Katalog mit dem PowerShell-Befehl `Set-ProvVMUpdateTimeWindow` aktualisieren. Beim nächsten Einschalten aktualisiert der Befehl innerhalb des angegebenen Zeitfensters die VMs, die mit dem Provisionschema erstellt wurden, das dem Katalog zugeordnet ist. Beispiel:

- `Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -StartTimeInUTC "3/12/2022 3am"-DurationInMinutes 60`
- `Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -StartsNow -DurationInMinutes 60`

> **Hinweis:**
>
> `StartsNow` gibt die geplante Startzeit an. `DurationInMinutes` ist das Zeitfenster des Zeitplans.

Sie können die Liste der Backup-VM-Größen für eine ausgewählte Anzahl vorhandener MCS-VMs mit dem Befehl `Set-ProvVM` konfigurieren. Um jedoch die Aktualisierungen anzuwenden, legen Sie mit `Set-ProvVMUpdateTimeWindow` ein Aktualisierungszeitfenster für die verwendeten VMs fest und starten Sie sie innerhalb des Fensters. Beispiel:

1. Führen Sie den Befehl `Set-ProvVM` aus, um die Größenliste der Backup-VM für eine ausgewählte vorhandene MCS-VM zu konfigurieren. Beispiel:

```
Set-ProvVM -VMName "Vm-001"
-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=`"LicenseType`" Value=`
    "Windows_Server`"/>
<Property xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"
    true`"/>
<Property xsi:type=`"StringProperty`" Name=`"BackupVmConfiguration
    `" Value=`"[{
```

```
 'ServiceOffering': 'Standard_D2as_v4', 'Type': 'Spot' }
 , {
 'ServiceOffering': 'Standard_D2s_v3', 'Type': 'Regular' }
 , {
 'ServiceOffering': 'Standard_D2s_v3', 'Type': 'Spot' }
 ]`"/>
</CustomProperties>"
<!--NeedCopy-->
```

2. Führen Sie den Befehl `Set-ProvVMUpdateTimeWindow` aus, um die Aktualisierungen anzuwenden. Beispiel:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -
    StartsNow -DurationInMinutes 60
<!--NeedCopy-->
```

### Tags in allen Ressourcen kopieren

Sie können in einem Maschinenprofil angegebene Tags auf alle Ressourcen (z. B. mehrere Netzwerkkarten und Betriebssystem-, Identitäts- und Zurückschreibdatenträger) einer neuen VM oder bestehenden VM in einem Maschinenkatalog kopieren. Die Maschinenprofilquelle kann eine VM oder ARM-Vorlagenspezifikation sein.

> **Hinweis:**
>
> Sie müssen die Richtlinie für die Tags hinzufügen (siehe Zuweisen von Richtliniendefinitionen für Tagkonformität) oder die Tags in einer Maschinenprofilquelle hinzufügen, um die Tags für die Ressourcen beizubehalten.

#### Voraussetzungen

Erstellen Sie die Maschinenprofilquelle (VM oder ARM-Vorlagenspezifikation), um Tags für VM, Datenträger und Netzwerkkarten dieser VM zu haben.

- Wenn Sie eine VM als Maschinenprofil-Eingabe haben möchten, wenden Sie Tags auf die VM und alle Ressourcen im Azure-Portal an. Siehe Anwenden von Tags mit dem Azure-Portal.
- Wenn Sie die ARM-Vorlagenspezifikation als Maschinenprofil-Eingabe verwenden, fügen Sie den folgenden Tag-Block unter jeder Ressource hinzu.

```
 "tags": {

"TagC": "Value3"
 }
,
<!--NeedCopy-->
```

> **Hinweis:**
>
> Eine Vorlagenspezifikation kann maximal einen Datenträger und muss mindestens eine Netzwerkkarte enthalten.

#### Tags an die Ressourcen einer VM in einem neuen Maschinenkatalog kopieren

1. Erstellen Sie einen nicht persistenten oder persistenten Katalog mit einer VM oder einer ARM-Vorlagenspezifikation als Maschinenprofil-Eingabe.
2. Fügen Sie dem Katalog eine VM hinzu und schalten Sie sie ein. Sie müssen sehen, dass die im Maschinenprofil angegebenen Tags an die entsprechenden Ressourcen der VM kopiert wurden.

   > **Hinweis:**
   >
   > Stimmt die Anzahl der im Maschinenprofil angegebenen Netzwerkkarten nicht mit der Anzahl Netzwerkkarten, die die VMs verwenden sollen, überein, wird eine Fehlermeldung angezeigt.

#### Tags für Ressourcen einer vorhandenen VM ändern

1. Erstellen Sie ein Maschinenprofil mit Tags für alle Ressourcen.
2. Aktualisieren Sie den vorhandenen Maschinenkatalog mit dem aktualisierten Maschinenprofil. Beispiel:

   ```
   Set-ProvScheme -ProvisioningSchemeName <YourCatalogName> -
       MachineProfile <PathToYourMachineProfile>
   <!--NeedCopy-->
   ```

3. Schalten Sie die VM aus, auf der Sie die Updates anwenden möchten.
4. Fordern Sie ein geplantes Update für die VM an. Beispiel:

   ```
   Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName <
       YourCatalogName>  -VMName machine1 -StartsNow -
       DurationInMinutes -1
   <!--NeedCopy-->
   ```

5. Schalten Sie die VM ein.
6. Sie müssen sehen, dass die im Maschinenprofil angegebenen Tags an die entsprechenden Ressourcen wurden.

> **Hinweis:**
>
> Stimmt die Anzahl der im Maschinenprofil angegebenen Netzwerkkarten nicht mit der in

> `Set-ProvScheme` angegebenen Anzahl Netzwerkkarten überein, wird eine Fehlermeldung angezeigt.

### So geht es weiter

- Wenn Sie den ersten Katalog erstellen, werden Sie von Web Studio zum Erstellen einer Bereitstellungsgruppe geleitet.
- Informationen zum gesamten Konfigurationsprozess finden Sie unter Installation und Konfiguration
- Informationen zur Verwaltung von Katalogen finden Sie unter Maschinenkataloge verwalten und Microsoft Azure-Katalog verwalten.

### Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Verbindung zu Microsoft Azure Resource Manager
- Maschinenkataloge erstellen

## Microsoft System Center Virtual Machine Manager-Katalog erstellen

June 27, 2024

Unter Maschinenkataloge erstellen werden die Assistenten zum Erstellen eines Maschinenkatalogs beschrieben. Die folgenden Informationen beziehen sich speziell auf Microsoft System Center Virtual Machine Manager (VMM)-Virtualisierungsumgebungen.

> **Hinweis:**
>
> Bevor Sie einen VMM-Katalog erstellen, müssen Sie eine Verbindung zu VMM hergestellt haben. Siehe Verbindung zu Microsoft System Center Virtual Machine Manager.

### Erstellen einer Master-VM

1. Installieren Sie einen VDA auf der Master-VM und wählen Sie die Option zur Desktopoptimierung und Leistungssteigerung aus.
2. Erstellen Sie einen Snapshot der Master-VM, um diesen als Backup zu verwenden.
3. Erstellen Sie virtuelle Desktops.

### MCS auf SMB 3-Dateifreigaben

Bei Maschinenkatalogen, die mit MCS auf SMB 3-Dateifreigaben für VM-Speicherung erstellt wurden, müssen die Anmeldeinformationen die folgenden Anforderungen erfüllen. Diese Anforderungen stellen sicher, dass Aufrufe von der Hypervisor Communications Library (HCL) des Controllers erfolgreich mit dem SMB-Speicher verbunden werden:

- 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. Tun Sie dies, wenn Sie VMM 2012 SP1 mit Hyper-V unter Windows Server 2012 verwenden. Weitere Informationen finden Sie unter CTX137465.

Die HCL öffnet mit `CredSSP` eine Verbindung zur Hyper-V-Maschine. Dabei werden mit Kerberos verschlüsselte Benutzeranmeldeinformationen an die Hyper-V-Maschine übergeben. Die **PowerShell**-Befehle in der Sitzung auf der Hyper-V-Remotemaschine werden mit den angegebenen Anmeldeinformationen ausgeführt. In diesem Fall sind es die Anmeldeinformationen des VMM-Benutzers, sodass Kommunikationsbefehle zum Speicher ordnungsgemäß funktionieren.

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 MCS-Provisioningschema (Maschinenkatalog). Die Master-VM wird durch dieses Schema geklont und vereinfacht, damit sie zum Erstellen von VMs 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:

  1. Upload der Identitätsdisk durch die HCL auf die Hyper-V-Maschine über die Administratorfreigabe.
  2. Der Datenträger wird von der Hyper-V-Maschine über ein PowerShell-Skript, das in der Remote-PowerShell-Sitzung ausgeführt wird, in den SMB-Speicher kopiert. Auf der Hyper-V-Maschine wird ein Ordner erstellt, dessen Berechtigungen nur für den VMM-Benutzer gesperrt sind (über die remote PowerShell-Verbindung).
  3. Die HCL löscht die Datei aus der Administratorfreigabe.
  4. Wenn der Upload des Identitätsdatenträgers durch die HCL auf die Hyper-V-Maschine abgeschlossen ist, werden die Identitätsdatenträger von der Remote-PowerShell-Sitzung in den SMB-Speicher kopiert. Anschließend werden sie aus der Hyper-V-Maschine gelöscht.

  Falls der Ordner des Identitätsdatenträgers gelöscht wird, wird er neu erstellt, damit er zur Wiederverwendung verfügbar ist.

- **Download von Identitätsdisks:** Wie beim Upload wird die Identitätsdisk über die Hyper-V-Maschine an die HCL übergeben. Beim folgenden Prozess wird, falls noch nicht vorhanden, ein Ordner erstellt, der nur VMM-Benutzerbenutzerberechtigungen auf dem Hyper-V-Server hat.

  1. Die Disk wird über ein PowerShell-Skript von der Hyper-V-Maschine aus dem SMB-Speicher in den lokalen Hyper-V-Speicher kopiert. Das Skript wird in der PowerShell V3-Remotesitzung ausgeführt.
  2. Die HCL liest den Datenträger aus der Administratorfreigabe der Hyper-V-Maschine in den Speicher.
  3. Die HCL löscht die Datei aus der Administratorfreigabe.

### Katalog mit einem Maschinenprofil erstellen

Sie können ein Maschinenprofil verwenden, um einen MCS-Maschinenkatalog in System Center Virtual Machine Manager-(SCVMM)-Umgebungen zu erstellen und zu aktualisieren. Sie können auch verschachtelte Virtualisierung und vTPM aktivieren.

### Wichtige Überlegungen

- Das Masterimage kann nur ein Snapshot und keine VM sein.
- Sie können VM nur als Maschinenprofilquelle verwenden.
- Sie können VTPM über die Hyper-V-Konsole und nicht über die SCVMM-Konsole konfigurieren.
- Wenn für das Masterimage vTPM aktiviert ist, müssen Sie vTPM auf der Maschinenprofilquelle aktivieren.
- vTPM wird nur auf Maschinen der Generation 2 unterstützt.
- Die folgenden Parameter überschreiben die in einem Maschinenprofil erfassten Werte, sofern sie separat angegeben werden:
  - VMCpuCount
  - VMMemoryMB
  - Datenträgerspeicher
- Sie können einen vorhandenen Katalog mit dem Befehl `Set-ProvScheme` aktualisieren.

### Vorgehensweise zum Erstellen eines Katalogs mit einem Maschinenprofil

1. Erstellen Sie eine VM als Maschinenprofilquelle. Weitere Informationen finden Sie unter Virtuelle Maschinen in der VMM-Fabric bereitstellen. Sie können die einmal ausgewählte **Generation** nicht mehr ändern.
   - Wenn Sie die verschachtelte Virtualisierung aktivieren möchten, aktivieren Sie auf der Seite **Quelle auswählen** das Kontrollkästchen **Verschachtelte Virtualisierung aktivieren**.
   - Wenn Sie vTPM aktivieren möchten, melden Sie sich nach dem Erstellen der VM beim Hyper-V-Host an und suchen Sie Ihre VM im **Hyper-V-Manager**. Klicken Sie mit der rechten Maustaste auf die VM und gehen Sie dann zu **Einstellungen**. Markieren Sie unter **Sicherheit** das Kontrollkästchen **Trusted Platform Module aktivieren**.
2. Öffnen Sie ein **PowerShell**-Fenster.
3. Führen Sie `asnp citrix*` aus, um die Citrix-spezifischen PowerShell-Module zu laden.
4. Erstellen Sie einen Brokerkatalog. In diesem Katalog sind Maschinen eingetragen, die gerade erstellt werden.
5. Erstellen Sie einen Identitätspool. Dieser wird zu einem Container für AD-Konten, die für die zu erstellenden Maschinen erstellt wurden.
6. Erstellen Sie ein Provisioningschema mit dem Maschinenprofil. Beispiel:

```
New-ProvScheme -HostingUnitName "<hostingunit name>"
-IdentityPoolName "ID1" -MasterImageVM "XDHyp:\HostingUnits\HU1<
    path to the checkpoint/snapshot>"
-ProvisioningSchemeName "<catalogname>"  -MachineProfile "XDHyp:<
    path to the machine profile VM>"
<!--NeedCopy-->
```

7. Damit wird der Brokerkatalog mit der eindeutigen ID des Provisioningschemas aktualisiert.
8. Erstellen Sie virtuelle Maschinen und fügen Sie sie dem Katalog hinzu.

Sie können einen vorhandenen Katalog mit dem Befehl Set-ProvScheme aktualisieren. Beispiel:

```
Set-ProvScheme -ProvisioningSchemeName "<catalogname>" -MachineProfile
    "XDHyp:<path to the machine profile VM>"
<!--NeedCopy-->
```

### So geht es weiter

- Wenn Sie den ersten Katalog erstellen, werden Sie von Web Studio zum Erstellen einer Bereitstellungsgruppe geleitet.
- Informationen zum gesamten Konfigurationsprozess finden Sie unter Installation und Konfiguration
- Informationen zur Verwaltung von Katalogen finden Sie unter Maschinenkataloge verwalten und Microsoft System Center Virtual Machine Manager-Katalog verwalten.

### Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Verbindung zu Microsoft System Center Virtual Machine Manager
- Maschinenkataloge erstellen

## Nutanix-Katalog erstellen

June 27, 2024

Unter Maschinenkataloge erstellen werden die Assistenten zum Erstellen eines Maschinenkatalogs beschrieben. Die folgenden Informationen beziehen sich speziell auf Nutanix-Virtualisierungsumgebungen.

> **Hinweis:**
>
> Bevor Sie einen Nutanix-Katalog erstellen, müssen Sie eine Verbindung zu Nutanix hergestellt haben. Siehe Verbindung zu Nutanix.

### Erstellen eines Maschinenkatalogs mit einem Nutanix-Snapshot

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. Weitere Informationen finden Sie in der Nutanix-Dokumentation.

Im Assistenten für die Katalogerstellung:

- Die Seiten **Betriebssystem** und **Maschinenverwaltung** enthalten keine Nutanix-spezifischen Informationen.
- Die Seiten **Container** bzw. **Cluster und Container** sind Nutanix-spezifisch.

  Wenn Sie Maschinen mit Nutanix AHV XI als Ressourcen bereitstellen, wird die Seite **Container** angezeigt. Wählen Sie einen Container, in dem die Identitätsdatenträger der VMs platziert werden.

  Wenn Sie Maschinen mit Nutanix AHV Prism Central (PC) als Ressourcen bereitstellen, wird die Seite **Cluster und Container** angezeigt. Wählen Sie den Cluster für die Bereitstellung von VMs und anschließend einen Container.
- Wählen Sie auf der Seite **Image** 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.
- Wählen Sie auf der Seite **Netzwerkkarten** den NIC-Typ zum Filtern der zugehörigen Netzwerke. Es gibt zwei Arten von Netzwerkkarten: **VLAN** und **OVERLAY**. Wählen Sie eine oder mehrere Netzwerkkarten, die das Masterimage enthält, und anschließend für jede Netzwerkkarte das zugehörige virtuelle Netzwerk.
- Die Seiten **Maschinenidentitäten**, **Domänenanmeldeinformationen**, **Bereiche** und **Zusammenfassung** enthalten keine Nutanix-spezifischen Informationen.

### Einschränkung

Beim Erstellen eines MCS-Katalogs mit Nutanix-Hostverbindung (insbesondere Nutanix AHV-Plugin 2.7.1) wird die Festplattengröße der bereitgestellten VMs in Web Studio falsch angezeigt. Die angezeigte Größe ist viel kleiner (1 GB) als die tatsächliche Speichergröße (50 GB). Die Festplattengröße wird in der Nutanix-Konsole korrekt angezeigt.

### So geht es weiter

- Wenn Sie den ersten Katalog erstellen, werden Sie von Web Studio zum Erstellen einer Bereitstellungsgruppe geleitet.
- Informationen zum gesamten Konfigurationsprozess finden Sie unter Installation und Konfiguration
- Informationen zur Verwaltung von Katalogen finden Sie unter Maschinenkataloge verwalten.

### Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Verbindung zu Nutanix
- Verbindung zu Nutanix-Cloud und Partnerlösungen
- Maschinenkataloge erstellen

## VMware-Katalog erstellen

June 27, 2024

Unter Maschinenkataloge erstellen werden die Assistenten zum Erstellen eines Maschinenkatalogs beschrieben. Die folgenden Informationen beziehen sich speziell auf VMware-Virtualisierungsumgebungen.

> **Hinweis:**
>
> Bevor Sie einen VMware-Katalog erstellen, müssen Sie eine Verbindung zu VMware hergestellt haben. Siehe Verbindung zu VMware.

### 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.

> **Hinweis:**
>
> Sie können mit MCS VMs in einer vSAN 8.0-Umgebung bereitstellen.

### Maschinenkatalog mit einem Maschinenprofil erstellen

Sie können einen MCS-Maschinenkatalog mithilfe eines Maschinenprofils erstellen. Die Quelle der Eingabe des Maschinenprofils ist eine VMware-Vorlage. Das Maschinenprofil erfasst die Hardwareeigenschaften aus einer VMware-Vorlage und wendet sie auf die neu bereitgestellten virtuellen Maschinen im Katalog an.

> **Hinweis:**
>
> - Die Masterimage-Eingabe (Snapshot) und die Maschinenprofileingabe (VMware-Vorlage) müssen entweder beide vTPM-aktiviert oder beide vTPM-deaktiviert sein. Diese Regel gilt sowohl für `New-ProvScheme` als auch für `Set-ProvScheme`.
> - Wenn das Masterimage vTPM-aktiviert ist, kann die VMware-Vorlage nur aus derselben VM-Quelle stammen wie das Masterimage.
> - Die Speicherverschlüsselungsrichtlinie unterstützt nur vollständige Klons.

Die VMware-Vorlage im Maschinenprofil muss während des Kataloglebenszyklus vorhanden sein, damit virtuelle Maschinen für den Katalog bereitgestellt werden können. Ohne VMware-Vorlage können Sie keine neuen virtuellen Maschinen bereitstellen. Wenn eine VMware-Vorlage gelöscht wird, müssen Sie mithilfe des Befehls `Set-ProvScheme` eine neue Vorlage bereitstellen.

- MCS erfasst die Eigenschaften von VMware-Vorlagen. Mit dem Befehl Get-Provscheme können Sie eine VMware-Vorlage mit Verweis auf gespeicherte Eigenschaften der VMware-Vorlage erstellen.
- Wenn der Maschinenkatalog und die bereitgestellten VMs vorhanden sind, kann alternativ eine mit MCS bereitgestellte Maschine verwendet werden, um eine VMware-Vorlage zu erstellen.

Basierend auf verschiedenen Betriebssystemen können Sie einen Maschinenkatalog mit verschiedenen Konfigurationen erstellen:

- Ist Windows 11 auf dem Masterimage installiert, muss vTPM für das Masterimage aktiviert sein. Daher muss an die VMware-Vorlage, die eine Quelle für das Maschinenprofil ist, vTPM angefügt sein.

- Ist Windows 10 auf dem Masterimage ohne angefügtes vTPM installiert, können Sie einen Maschinenkatalog mit einer VMware-Vorlage ohne vTPM als Quelle für das Maschinenprofil erstellen.

Es gibt eine weitere Konfiguration, bei der Sie einen Maschinenkatalog im Komplettklon-Kopiermodus erstellen können, wobei die Maschinenprofilvorlage mit der Speicherverschlüsselungsrichtlinie angewendet wird.

Gehen Sie zu Erstellen eines Maschinenkatalog mit PowerShell und einem Maschinenprofil als Eingabe folgendermaßen vor:

1. Öffnen Sie ein **PowerShell**-Fenster.
2. Führen Sie `asnp citrix*` aus.
3. Führen Sie die folgenden Befehle aus:

    - Gehen Sie zum Erstellen eines Maschinenkatalogs mit einer VMware-Vorlage mit angefügtem vTPM als Quelle für die Maschinenprofileingabe und dem Windows 11-Masterimage wie folgt vor:

```
$identityPool = New-AcctIdentityPool  -IdentityPoolName "<
    string>"
-NamingScheme "<string>-###"
-NamingSchemeType Numeric
-Domain "<domain name"
-ZoneUid "<Uid>"  -Scope @()
<!--NeedCopy-->
```

```
$provScheme =New-ProvScheme  -CleanOnBoot
-HostingUnitName "vSanRg"
-IdentityPoolName "<string>"
-InitialBatchSizeHint 1
-MasterImageVM "XDHyp:\HostingUnits<hosting unit name><
    snapshot name>.snapshot"
-NetworkMapping @{
"0"="XDHyp:\HostingUnits<hosting unit name>\<network name>.
    network" }

-ProvisioningSchemeName "<string>"
-Scope @() -VMCpuCount 4
-VMMemoryMB 6144
-MachineProfile "XDHyp:\HostingUnits<hosting unit name><
    template name>.template" -TenancyType Shared
-FunctionalLevel "L7_20"
<!--NeedCopy-->
```

```
$catalog = New-BrokerCatalog
-AllocationType "Static"
-PersistUserChanges  "OnLocal"
-Description "<string>"
```

```
-IsRemotePC $False
-MinimumFunctionalLevel 'L7_9'
-Name "<catalog name>"
-ProvisioningType 'MCS'
-Scope @()
-SessionSupport "SingleSession" -ZoneUid "<Uid>"
<!--NeedCopy-->
```

```
Set-BrokerCatalog -Name "<string>"
-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
<!--NeedCopy-->
```

- Gehen Sie zum Erstellen eines Maschinenkatalogs mit einer VMware-Vorlage ohne vTPM als Quelle für das Maschinenprofil und dem Windows10-Masterimage wie folgt vor:

```
$identityPool = New-AcctIdentityPool
-IdentityPoolName "<string>"
-NamingScheme "<string>-###" -NamingSchemeType Numeric
-Domain "<domain name>"
-ZoneUid "<Uid>"  -Scope @()
<!--NeedCopy-->
```

```
$provScheme =New-ProvScheme
-CleanOnBoot -HostingUnitName "<string>"
-IdentityPoolName "<string>"
-InitialBatchSizeHint 1
-MasterImageVM "XDHyp:\HostingUnits<hosting unit name><
   snapshot name>.snapshot
-NetworkMapping @{
"0"="XDHyp:\HostingUnits<hosting unit name>\<string>.network"
    }

-ProvisioningSchemeName "<string>"  -Scope @() -VMCpuCount 4
    -VMMemoryMB 8192
-MachineProfile "XDHyp:\HostingUnits<hosting unit name><
   template name>.template"
-TenancyType Shared  -FunctionalLevel "L7_20"
<!--NeedCopy-->
```

```
$catalog = New-BrokerCatalog
-AllocationType "Static"
-PersistUserChanges  "OnLocal"
-Description "<string>"
-IsRemotePC $False
-MinimumFunctionalLevel 'L7_9' -Name "<string>" -
   ProvisioningType 'MCS' -Scope @()
-SessionSupport "SingleSession" -ZoneUid "<Uid"
<!--NeedCopy-->
```

```
Set-BrokerCatalog -Name "<string>"
-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
<!--NeedCopy-->
```

- Gehen Sie zum Erstellen eines Maschinenkatalogs unter Verwendung des Komplettklon-Kopiermodus und Anwendung der Maschinenprofilvorlage mit der Speicherverschlüsselungsrichtlinie folgendermaßen vor:

```
$identityPool = New-AcctIdentityPool
-IdentityPoolName "<string>"
-NamingScheme "<string>-###"
-NamingSchemeType Numeric
-Domain "<domain name>"
-ZoneUid "<Uid>"  -Scope @()
<!--NeedCopy-->
```

```
$provScheme =New-ProvScheme
-HostingUnitName "<string>"
-IdentityPoolName "<string>"
-InitialBatchSizeHint 1
-MasterImageVM "XDHyp:\HostingUnits<hosting unit name><
   snapshot name>.snapshot"
-NetworkMapping @{
"0"="XDHyp:\HostingUnits<hosting unit name>\<string>.network"
    }

-ProvisioningSchemeName "<string>"
-Scope @() -VMCpuCount 4  -VMMemoryMB 8192 -MachineProfile "
   XDHyp:\HostingUnits<hosting unit name><template name>.
   template"
-TenancyType Shared
-FunctionalLevel "L7_20" -UseFullDiskCloneProvisioning
<!--NeedCopy-->
```

```
$catalog = New-BrokerCatalog
-AllocationType "Static"
-PersistUserChanges  "OnLocal"
-Description "<string>"  -IsRemotePC $False
-MinimumFunctionalLevel 'L7_9'
-Name "<string>" -ProvisioningType 'MCS' -Scope @()
-SessionSupport "SingleSession" -ZoneUid "<Uid>"
<!--NeedCopy-->
```

```
Set-BrokerCatalog -Name "<string>"
-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
<!--NeedCopy-->
```

Verwenden Sie den Befehl Set-ProvScheme, um ein Maschinenprofil zu aktualisieren. Beispiel:

```
Set-ProvScheme -ProvisioningSchemeName 'name' -IdentityPoolName 'name'
   -MachineProfile 'XDHyp:\HostingUnits<hosting unit name><template
   name>.template'
<!--NeedCopy-->
```

### Nach mehreren NICs suchen

Bei den vorbereitenden Checks für mehrere Netzwerkkarten erhalten Sie verschiedene Fehlermeldungen, wenn Sie ein Maschinenprofil und den Parameter `NetworkMapping` in den Befehlen `New-ProvScheme` und `Set-ProvScheme` verwenden.

Die vorbereitende Checkliste für mehrere Netzkkarten lautet wie folgt:

- Nur die Anzahl der Netzwerkkarten aus der Maschinenprofilvorlage wird verwendet und validiert. Das Netzwerk, auf das diese Netzwerkkarten verweisen, wird nicht verwendet oder anhand der Netzwerke der Hostingeinheit validiert.
- Wenn die Anzahl der Netzwerkkarten in der Maschinenprofilvorlage größer ist als die Anzahl der Netzwerke in der Hosteinheit, erhalten Sie eine Fehlermeldung.
- Wenn die Anzahl der Netzwerkkarten in der Maschinenprofilvorlage null ist, erhalten Sie eine Fehlermeldung.
  Wenn die Anzahl der Netzwerkkarten in der Maschinenprofilvorlage eins ist, gilt Folgendes:
  - If no network mapping is specified in the `New-ProvScheme` or `Set-ProvScheme` command, and the hosting unit network is one, then the hosting unit network is used.
  - If network mapping is specified, then the specified network mapping is used if it is valid.
- Wenn die Anzahl der Netzwerkkarten in der Maschinenprofilvorlage größer als 1 ist oder die Netzwerkanzahl der Hosteinheit größer als 1 ist, dann gilt Folgendes:
  - Für den Befehl ist eine gültige Netzwerkzuordnung erforderlich, die eine Zuordnung für jede Netzwerkkarte bereitstellen sollte (d. h., die NetworkMapping-Anzahl sollte mit der Anzahl der Netzwerkkarten des Maschinenprofils übereinstimmen).
  - In der Hostingeinheit können nicht mehrere Netzwerkkarten demselben Netzwerk zugeordnet werden.
  - Die Anzahl von `NetworkMapping` und die Anzahl der Netzwerkkarten des Maschinenprofils müssen kleiner oder gleich der Netzwerkanzahl der Hostingeinheit sein.
  - `NetworkMapping` muss für jede ID von 0 bis n-1 angegeben werden, wobei n die Anzahl der Netzwerkadapter in der Maschinenprofilvorlage ist.

### Problembehandlung

Wenn der Katalog nicht erstellt werden kann, lesen Sie bitte CTX294978.

### So geht es weiter

- Wenn Sie den ersten Katalog erstellen, werden Sie von Web Studio zum Erstellen einer Bereitstellungsgruppe geleitet.

- Informationen zum gesamten Konfigurationsprozess finden Sie unter Installation und Konfiguration
- Informationen zur Verwaltung von Katalogen finden Sie unter Maschinenkataloge verwalten und VMware-Katalog verwalten.

### Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Verbindung zu VMware
- Maschinenkataloge erstellen

## Kataloge mit verschiedenen Einbindungstypen erstellen

June 27, 2024

Mit MCS können Sie Maschinen mit On-Premises-AD-Verbindung oder mit Azure AD-Hybrideinbindung bereitstellen.

Informationen zum Konfigurieren von Maschinenidentitäten in Web Studio finden Sie unter Erstellen von Maschinenkatalogen.

Weitere Informationen zum Erstellen von mit der Maschinenidentität verbundenen Katalogen finden Sie in den folgenden Abschnitten:

- Kataloge mit Azure Active Directory-Hybrideinbindung erstellen

## Kataloge mit Azure Active Directory-Hybrideinbindung erstellen

June 27, 2024

> **Hinweis:**
>
> Seit Juli 2023 hat Microsoft Azure Active Directory (Azure AD) in Microsoft Entra ID umbenannt. In diesem Dokument bezieht sich jeder Verweis auf Azure Active Directory, Azure AD oder AAD jetzt auf Microsoft Entra ID.

In diesem Artikel wird beschrieben, wie Sie Kataloge mit Azure Active Directory-Hybrideinbindung erstellen.

Sie können mit Azure AD verbundene Kataloge mit Web Studio oder PowerShell erstellen.

Informationen zu Anforderungen, Einschränkungen und Überlegungen finden Sie unter Azure Active Directory-Hybrideinbindung.

### Web Studio verwenden

Die folgenden Informationen ergänzen die Anweisungen unter Erstellen von Maschinenkatalogen. Folgen Sie zum Erstellen eines Katalogs mit Azure AD-Hybrideinbindung den allgemeinen Anweisungen in dem Artikel. Achten Sie besonders auf die spezifischen Details für Kataloge mit Azure AD-Hybrideinbindung.

Im Assistenten für die Katalogerstellung:

- Wählen Sie auf der Seite **Maschinenidentitäten** die Option **Azure Active Directory-Hybrideinbindung**. Die erstellten Maschinen gehören einer Organisation und sind mit einem Active Directory Domain Services-Konto dieser Organisation angemeldet. Sie existieren in der Cloud und on-premises.

> **Hinweis:**
>
> Wenn Sie **Azure Active Directory-Hybrideinbindung** als Identitätstyp auswählen, benötigt jede Maschine im Maschinenkatalog ein AD-Computerkonto.

### PowerShell verwenden

Nachfolgend sind die den Web Studio-Vorgängen entsprechenden PowerShell-Schritte aufgeführt. Informationen zum Erstellen eines Katalogs mit dem Remote PowerShell SDK finden Sie unter https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

Der Unterschied zwischen mit einem On-Premises-AD verbundenen Katalogen und solchen mit Azure AD-Hybrideinbindung liegt in der Erstellung des Identitätspools und der Maschinenkonten.

Zum Erstellen eines Identitätspools mit den Konten für Kataloge mit Azure AD-Hybrideinbindung gehen Sie folgendermaßen vor:

```
1 New-AcctIdentityPool -AllowUnicode -IdentityType "HybridAzureAD" -
    Domain "corp.local" -IdentityPoolName "HybridAADJoinedCatalog" -
    NamingScheme "HybridAAD-VM-##" -NamingSchemeType "Numeric" -OU "CN=
    AADComputers,DC=corp,DC=local" -Scope @() -ZoneUid "81291221-d2f2-49
    d2-ab12-bae5bbd0df05"
2 New-AcctADAccount -IdentityPoolName "HybridAADJoinedCatalog" -Count 10
    -ADUserName "corp\admin1" -ADPassword $password
3 Set-AcctAdAccountUserCert -IdentityPoolName "HybridAADJoinedCatalog" -
    All -ADUserName "corp\admin1" -ADPassword $password
4 <!--NeedCopy-->
```

> **Hinweis:**
>
> `$password` ist das Kennwort für ein AD-Benutzerkonto mit Schreibberechtigung.

Alle anderen Befehle zum Erstellen von Katalogen mit Azure AD-Hybrideinbindung sind mit denen für herkömmliche On-Premises-AD-Kataloge identisch.

### Anzeigen des Status der Azure AD-Hybrideinbindung

In Web Studio wird der Status der Azure AD-Hybrideinbindung angezeigt, wenn die Maschinen mit Azure AD-Hybrideinbindung in einer Bereitstellungsgruppe eingeschaltet sind. Um den Status anzuzeigen, identifizieren Sie mit Suchen diese Maschinen und prüfen Sie dann die **Maschinenidentität** für jede Maschine auf der Registerkarte **Details** im unteren Bereich. Die folgenden Informationen können unter **Maschinenidentität** angezeigt werden:

- Azure AD-Hybrideinbindung
- Noch nicht mit Azure AD verbunden

> **Hinweis:**
>
> - Möglicherweise kommt es beim ersten Einschalten einer Maschine zu einer verzögerten Azure AD-Hybrideinbindung. Ursache ist das standardmäßige Synchronisierungsintervall für die Maschinenidentität (30 Minuten in Azure AD Connect). Maschinen erhalten erst dann eine Azure AD-Hybrideinbindung, wenn die Maschinenidentität über Azure AD Connect mit Azure AD synchronisiert wurde.
> - Maschinen ohne Azure AD-Hybrideinbindung werden nicht beim Delivery Controller registriert. Ihr Registrierungsstatus wird als **Initialisierung** angezeigt.

Bei Verwendung von Web Studio können Sie außerdem erfahren, warum Maschinen nicht verfügbar sind. Klicken Sie dazu im Knoten **Suchen** auf eine Maschine, aktivieren Sie im unteren Bereich auf der Registerkarte **Details** die Option **Registrierung**, und lesen Sie dann den Tooltip, um weitere Informationen zu erhalten.

### Problembehandlung

Wenn Maschinen keine Azure AD-Hybrideinbindung aufweisen, gehen Sie wie folgt vor:

- Überprüfen Sie, ob das Maschinenkonto über das Microsoft Azure AD-Portal mit Azure AD synchronisiert wurde. Bei erfolgter Synchronisierung wird **Noch nicht mit Azure AD verbunden** angezeigt und die Registrierung ist ausstehend.

  Um Maschinenkonten mit Azure AD zu synchronisieren, stellen Sie Folgendes sicher:

  - Das Maschinenkonto befindet sich in der Organisationseinheit, die für die Synchronisierung mit Azure AD konfiguriert ist. Maschinenkonten ohne **userCertificate**-Attribut werden nicht mit Azure AD synchronisiert, selbst wenn sie in der Organisationseinheit sind, die für die Synchronisierung konfiguriert ist.
  - Das Attribut **userCertificate** wird im Maschinenkonto aufgefüllt. Verwenden Sie Active Directory Explorer, um das Attribut anzuzeigen.
  - Azure AD Connect muss nach Erstellung des Maschinenkontos mindestens eine Synchronisierung ausgeführt haben. Ist dies nicht der Fall, führen Sie in der PowerShell-Konsole der Azure AD Connect-Maschine den Befehl `Start-ADSyncSyncCycle -PolicyType Delta` manuell aus, um eine sofortige Synchronisierung auszulösen.

- Überprüfen Sie, ob das von Citrix verwaltete Geräteschlüsselpaar für die Azure AD-Hybrideinbindung einwandfrei an die Maschine übertragen wurde, indem Sie den Wert von **DeviceKeyPairRestored** unter **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix** prüfen.

  Vergewissern Sie sich, dass der Wert 1 ist. Falls nicht, sind folgende Gründe möglich:

  - `IdentityType` des Identitätspools, der dem Provisioningschema zugeordnet ist, ist nicht auf `HybridAzureAD` festgelegt. Sie können dies überprüfen, indem Sie `Get-AcctIdentityPool` ausführen.
  - Die Maschine wurde nicht mit dem Provisioningschema des Maschinenkatalogs bereitgestellt.
  - Die Maschine ist nicht mit der lokalen Domäne verbunden. Die Verbindung mit der lokalen Domäne ist eine Voraussetzung für die Azure AD-Hybrideinbindung.

- Überprüfen Sie Diagnosemeldungen mit dem Befehl `dsregcmd /status /debug` auf der per MCS bereitgestellten Maschine.

  - War die Azure AD-Hybrideinbindung erfolgreich, lautet der Wert für **AzureAdJoined** und **DomainJoined** in der Befehlszeilenausgabe **YES**.

  - Falls nicht, konsultieren Sie die Microsoft-Dokumentation zur Problembehandlung: https://docs.microsoft.com/en-us/azure/active-directory/devices/troubleshoot-hybrid-join-windows-current.

  - Wird die Fehlermeldung **Server Message: The user certificate is not found on the device with id: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx** angezeigt, führen Sie den folgenden PowerShell-Befehl aus, um das Benutzerzertifikat zu reparieren:

    ```
    1  Repair-AcctIdentity -IdentityAccountName TEST\VM1 -Target
          UserCertificate
    2  <!--NeedCopy-->
    ```

    Weitere Informationen zu dem Problem mit dem Benutzerzertifikat finden Sie unter CTX566696.

# Maschinenkataloge verwalten

June 28, 2024

> **Hinweis:**
>
> Sie können Ihre Citrix Virtual Apps and Desktops-Bereitstellung mithilfe von zwei Verwaltungskonsolen verwalten: Web Studio (webbasiert) und Citrix Studio (Windows-basiert). Dieser Artikel behandelt nur Web Studio. Informationen zu Citrix Studio finden Sie im entsprechenden Artikel in Citrix Virtual Apps and Desktops 7 2212 oder früher.

## Einführung

Sie können Maschinen in Maschinenkatalogen hinzufügen, entfernen und umbenennen, Maschinenbeschreibungen ändern und die Active Directory-Computerkonten des Katalogs verwalten.

Zur Verwaltung von Katalogen kann auch die Sorge dafür gehören, dass jede Maschine über die neuesten Betriebssystemupdates verfügt. Dies schließt Antivirenupdates, Betriebssystemupgrades und Konfigurationsänderungen ein.

- 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 Katalogen mit statischen (permanent zugewiesenen) oder Remote-PC-Zugriff-Maschinen verwalten Sie Updates an den Benutzermaschinen Web 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 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.

### Maschinenkataloge verwalten

Sie können einen Maschinenkatalog auf zweierlei Art verwalten:

- Web Studio verwenden
- PowerShell verwenden

### Web Studio verwenden

In diesem Abschnitt wird beschrieben, wie Sie Kataloge mit Web Studio verwalten:

- Katalogdetails anzeigen
- Maschinen zum Maschinenkatalog hinzufügen
- Löschen von Maschinen aus einem Maschinenkatalog
- Bearbeiten eines Katalogs
- Umbenennen von Maschinenkatalogen
- Verschieben eines Maschinenkatalogs in eine andere Zone
- Löschen eines Katalogs
- Verwalten von Active Directory-Computerkonten in einem Maschinenkatalog
- Aktualisieren von Maschinenkatalogen
- Funktionsebene ändern oder Änderung rückgängig machen
- Klonen von Katalogen
- Organisieren von Katalogen mit Ordnern

### Katalogdetails anzeigen

1. Verwenden Sie die Suchfunktion, um einen bestimmten Maschinenkatalog zu finden. Anweisungen finden Sie unter Nach Instanzen suchen.
2. Wählen Sie aus den Suchergebnissen nach Bedarf einen Katalog aus.
3. In der folgenden Tabelle finden Sie Beschreibungen der Katalogspalten.

4. Klicken Sie im unteren Detailbereich auf eine Registerkarte, um weitere Informationen zu diesem Katalog zu erhalten.

| Spalte | Beschreibung |
| --- | --- |
| Maschinenkatalog | Der Name und der Zuteilungstyp des Katalogs. Zu den Zuteilungstypen gehören Zufällig: Maschinen im Katalog werden einem Benutzer nach dem Zufallsprinzip zugewiesen. Permanent: Maschinen im Katalog sind einem Benutzer dauerhaft zugewiesen. |
| Maschinentyp | Der unterstützte Sitzungstyp der Maschinen im Katalog. Mögliche Werte: Betriebssystemtyp: Multisitzungs-OS (virtuell); Benutzerdaten: Verwerfen. Betriebssystemtyp: Multisitzungs-OS (virtuell); Benutzerdaten: auf lokalem Datenträger Betriebssystemtyp: Einzelsitzungs-OS (Remote-PC-Zugriff) Betriebssystemtyp: Einzelsitzungs-OS (virtuell); Provisioningmethode: Manuell; Benutzerdaten: Verwerfen Betriebssystemtyp: Einzelsitzungs-OS (virtuell); Provisioningmethode: Citrix Virtual Desktops (MCS-Maschinen), Citrix Provisioning Services; Benutzerdaten: auf lokalem Datenträger |
| Maschinenanzahl | Die Anzahl der Maschinen im Katalog. |
| Zugewiesene Anzahl | Die Anzahl der Maschinen im Katalog, die einer Bereitstellungsgruppe zugewiesen sind. |
| Ordner | Der Speicherort des Katalogs im **Maschinenkatalogbaum**. Hier wird der Name des Ordners angezeigt, in dem sich der Katalog befindet (einschließlich des abschließenden umgekehrten Schrägstrichs), oder −, wenn sich der Katalog auf der Stammebene befindet. |
| VDA-Upgrade | VDA-Upgradestatus. Mögliche Werte: Nicht konfiguriert, Geplant, Verfügbar und Aktuell. |
| Imagestatus | Der Status der Imageaktualisierung des Katalogs. Gilt nur für nicht persistente Maschinenkataloge. Mögliche Werte sind: Vollständig aktualisiert, Teilweise aktualisiert, Ausstehende Aktualisierungen, Vorbereitet |

### Maschinen zum Maschinenkatalog hinzufügen

Vorbereitungen:

- Vergewissern Sie sich, dass der Virtualisierungshost genügend Prozessoren, Arbeitsspeicher und Speicher zur Unterbringung der zusätzlichen Maschinen hat.
- Vergewissern Sie sich, 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 Web Studio erstellen, müssen Sie die erforderlichen Domänenadministratorrechte haben.

Hinzufügen von Maschinen zum Maschinenkatalog

1. Melden Sie sich bei Web Studio an.
2. Wählen Sie im linken Bereich **Maschinenkataloge**.
3. Wählen Sie einen Maschinenkatalog und dann in der Aktionsleiste die Option **Maschinen hinzufügen**.
4. Legen Sie die Anzahl der hinzuzufügenden virtuellen Maschinen fest.
5. 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.
6. 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. Vergewissern Sie sich, dass Sie ausreichend Konten für die hinzuzufügenden Maschinen haben. Web Studio verwaltet diese Konten. Gestatten Sie Web Studio, die Kennwörter für alle Konten zurückzusetzen, oder geben Sie das Kontokennwort an (muss für alle Konten gleich sein).

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 Web 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. Melden Sie sich bei Web Studio an.
2. Wählen Sie im linken Bereich **Maschinenkataloge**.
3. Wählen Sie einen Katalog und dann in der Aktionsleiste **Maschinen anzeigen**.
4. Wählen Sie eine oder mehrere Maschinen und dann in der Aktionsleiste **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.

### Bearbeiten eines Katalogs

1. Ändern Sie auf der Seite **Beschreibung** die Beschreibung des Maschinenkatalogs.
2. Wählen Sie im linken Bereich **Maschinenkataloge**.
3. Wählen Sie einen Katalog und dann in der Aktionsleiste **Maschinenkatalog bearbeiten**.
4. Ändern Sie die Bereiche auf der Seite **Geltungsbereiche**.
5. Je nach Katalogtyp werden möglicherweise andere Seiten angezeigt.

   Für Kataloge, die mit einem Azure Resource Manager-Image erstellt wurden, werden die folgenden Seiten angezeigt. Denken Sie daran, dass vorgenommene Änderungen nur für Maschinen gelten, die Sie später zum Katalog hinzufügen. Bestehende Maschinen bleiben unverändert.

   - Ändern Sie auf der Seite **Virtuelle Maschinen** die Maschinengröße und wählen Sie Verfügbarkeitszonen aus, in denen Sie Maschinen erstellen möchten.

     > **Hinweis:**
     >
     > – Es werden nur Maschinengrößen angezeigt, die vom Katalog unterstützt werden.
     > – Wählen Sie gegebenenfalls **Nur in anderen Maschinenkatalogen verwendete Maschinengrößen anzeigen**, um die Liste der Maschinengrößen zu filtern.

   - Wählen Sie auf der Seite **Maschinenprofil**, ob Sie ein Maschinenprofil verwenden oder ändern möchten.
   - (Nur sichtbar, wenn der Katalog mit einer dedizierten Hostgruppen konfiguriert ist) Wählen Sie auf der Seite **Dedizierte Hostgruppe** aus, ob eine Hostgruppe geändert werden soll.
   - Wählen Sie auf der Seite **Speicher- und Lizenztypen** aus, ob der Speichertyp, der Lizenztyp und die Azure Compute Gallery-Einstellungen geändert werden sollen (nur verfügbar, wenn **Vorbereitetes Image in der Azure Compute Gallery platzieren** verwendet wird).

> **Hinweis:**
>
> Wenn die neue Einstellung die aktuelle Maschinengröße nicht unterstützt, wird eine Warnung angezeigt, dass durch eine Änderung der Einstellung die Maschinengröße zurückgesetzt wird. Wenn Sie fortfahren möchten, erscheint neben dem Menü **Virtuelle Maschinen** ein roter Punkt, durch den Sie aufgefordert werden, eine neue Maschinengröße auszuwählen.

- Wählen Sie auf der Seite **Lizenztyp**, ob Sie die Windows- oder die Linux-Lizenzeinstellung ändern möchten.

Für Remote-PC-Zugriff-Kataloge werden die folgenden Seiten angezeigt:

- Auf der Seite **Energieverwaltung** ändern Sie die Energieverwaltungseinstellungen und wählen eine Energieverwaltungsverbindung aus.
- Verwenden Sie die Seite **Organisationseinheiten** zum Hinzufügen und Entfernen von Active Directory-Organisationseinheiten.

6. Klicken Sie auf **Übernehmen**, um die vorgenommenen Änderungen zu übernehmen, und klicken Sie dann auf **Speichern**.

### Umbenennen von Maschinenkatalogen

1. Melden Sie sich bei Web Studio an.
2. Wählen Sie im linken Bereich **Maschinenkataloge**.
3. Wählen Sie einen Katalog und dann in der Aktionsleiste **Maschinenkatalog umbenennen**.
4. 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 mit den zugehörigen VMs in eine andere Zone verschieben, wirkt sich dies negativ auf die Leistung aus.

1. Melden Sie sich bei Web Studio an.
2. Wählen Sie im linken Bereich **Maschinenkataloge**.
3. Wählen Sie einen Katalog und dann in der Aktionsleiste **Verschieben**.
4. 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 Sie führen keine getrennten Sitzungen durch.
- 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. Melden Sie sich bei Web Studio an.
2. Wählen Sie im linken Bereich **Maschinenkataloge**.
3. Wählen Sie einen Katalog und dann in der Aktionsleiste **Maschinenkatalog löschen**.
4. 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. Melden Sie sich bei Web Studio an.
2. Wählen Sie im linken Bereich **Maschinenkataloge**.
3. Wählen Sie einen Maschinenkatalog und dann in der Aktionsleiste **Active Directory-Konten verwalten**.
4. 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.

Geben Sie an, ob Active Directory-Konten beibehalten, deaktiviert oder gelöscht werden sollen, wenn Sie Maschinen aus einem Katalog entfernen oder einen Katalog löschen.

## Aktualisieren von Maschinenkatalogen

Wir empfehlen, 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. Dadurch werden Ausfallzeiten für die Benutzer minimiert. Masterimages dürfen nicht gelöscht, verschoben oder umbenannt werden. Sie können einen Katalog nicht zu ihrer Verwendung wiederherstellen.

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 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. Schalten Sie die virtuelle Maschine aus.
5. Erstellen Sie einen Snapshot der VM. Geben Sie diesem einen aussagekräftigen Namen, der bei der Aktualisierung des Katalogs in Web Studio erkannt wird. Obwohl Web Studio einen Snapshot erstellen kann, empfiehlt Citrix, dass Sie diesen mit der Hypervisor-Verwaltungskonsole erstellen. Wählen Sie dann den Snapshot in Web Studio aus. Dadurch können Sie statt eines automatisch erstellten Namens einen aussagekräftigen Namen und eine Beschreibung zuweisen. Bei GPU-Masterimages können Sie das Masterimage nur über die XenServer-Konsole ändern.

**Masterimage ändern**

Vorbereiten und Verteilen des Updates auf allen Maschinen in einem Katalog

1. Melden Sie sich bei Web Studio an.
2. Wählen Sie im linken Bereich **Maschinenkataloge**.
3. Wählen Sie einen Katalog und dann in der Aktionsleiste **Masterimage ändern**.
4. Wählen Sie auf der Seite **Image** den Host und das Masterimage aus, das Sie verwenden möchten.

   > **Tipp:**
   >
   > Für mit MCS erstellte Kataloge können Sie einen Hinweis zu dem Image angeben. Ein Hinweis kann bis zu 500 Zeichen enthalten. Bei jeder Änderung des Masterimages wird ein Hinweis-Eintrag erstellt, unabhängig davon, ob Sie einen Hinweis hinzufügen. Wenn Sie beim Aktualisieren eines Katalogs keinen Hinweis hinzufügen, wird der Eintrag als Null (-) angezeigt. Um den Hinweisverlauf für ein Image anzuzeigen, wählen Sie den Katalog, klicken Sie im unteren Bereich auf **Vorlageneigenschaften** und klicken Sie dann auf **Hinweisverlauf anzeigen**.

5. Legen Sie auf der Seite **Rolloutstrategie** fest, wann die Aktualisierung der Maschinen im Maschinenkatalog erfolgen soll: beim nächsten Herunterfahren oder sofort.

   > **Hinweis:**
   >
   > Die Seite **Rolloutstrategie** ist für persistente VMs nicht verfügbar, da das Rollout nur für nicht persistente VMs gilt.

6. Überprüfen Sie die Informationen auf der Seite **Zusammenfassung** und klicken Sie auf **Fertigstellen**. Jede Maschine wird nach erfolgter Aktualisierung automatisch neu gestartet.

Um den Fortschritt des Updates zu verfolgen, suchen Sie den Katalog in **Maschinenkatalogen**, um den Fortschrittsbalken und das Fortschrittsdiagramm anzuzeigen.

Wenn Sie einen Katalog nicht in Web Studio, sondern direkt mit dem PowerShell-SDK aktualisieren, geben Sie eine Hypervisorvorlage (**VMTemplates**) an. Verwenden Sie diese Option als Alternative zu einem Image oder einem Imagesnapshot.

**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.
- Einzelsitzungs-OS-Maschinen werden, wenn sie nicht in Verwendung sind bzw. keine Benutzer angemeldet sind, sofort aktualisiert.
- Bei Multisitzungs-OS 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 einen einmaligen Neustart mithilfe von PowerShell planen möchten, konsultieren Sie den Abschnitt Einmaligen Neustart planen.

#### Rollback für Masterimage ausführen

Nach Bereitstellung eines aktualisierten oder neuen Masterimages können Sie diese mit einem Rollback rückgängig machen. Dieser Prozess 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. Was ist neu, die das neue Image erfordern, stehen dann nicht mehr zur Verfügung. Bei einem Rollback einer Maschine ist ein Neustart erforderlich.

1. Melden Sie sich bei Web Studio an.
2. Wählen Sie im linken Bereich **Maschinenkataloge**.
3. Wählen Sie den Katalog und dann in der Aktionsleiste **Rollback für Masterimage ausführen**.
4. Legen Sie fest, wann das ältere Masterimage auf die Maschinen angewendet werden soll (gemäß den Rollout-Anweisungen im vorigen Abschnitt).

Das Rollback wird nur auf Maschinen angewendet, die zurückgesetzt werden müssen. Maschinen, die nicht mit dem neuen oder aktualisierten Masterimage aktualisiert wurden, erhalten keine Benachrichtigung und müssen sich nicht abmelden.

Um den Rollback-Fortschritt zu verfolgen, suchen Sie den Katalog in **Maschinenkatalogen**, um den Fortschrittsbalken und das Fortschrittsdiagramm anzuzeigen.

### Funktionsebene ändern oder Änderung rückgängig machen

Ändern Sie die Funktionsebene für 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.

Führen Sie folgende Schritte aus, bevor Sie die Funktionsebene für einen Maschinenkatalog ändern:

- Starten Sie die aktualisierten Maschinen, damit sie sich bei dem Controller registrieren. Auf diese Weise kann Web Studio feststellen, dass die Maschinen im Maschinenkatalog aktualisiert werden müssen.

Ändern der Funktionsebene für einen Katalog:

1. Melden Sie sich bei Web Studio an.
2. Wählen Sie im linken Bereich **Maschinenkataloge**.
3. Wählen Sie den Katalog aus. Auf der Registerkarte **Details** im unteren Bereich werden Versionsinformationen angezeigt.
4. Wählen Sie **Funktionsebene ändern**. Wenn Web 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. Um einen ordnungsgemäßen Betrieb aller Maschinen sicherzustellen, empfiehlt Citrix, Maschinenprobleme zu beheben, bevor Sie zum Fortfahren auf **Ändern** klicken.

Nach Abschluss der Katalogänderung können Sie Maschinen auf ihre vorherige VDA-Version zurücksetzen, indem Sie zunächst den Maschinenkatalog und dann in der Aktionsleiste **Änderung der Funktionsebene rückgängig machen** wählen.

### Klonen von Katalogen

Beim Klonen von Katalogen ist Folgendes zu berücksichtigen:

- Sie können die Einstellungen für Betriebssystem und Maschinenverwaltung nicht ändern. Der Klon erbt diese Einstellungen vom Original.
- Das Klonen eines Katalogs kann einige Zeit in Anspruch nehmen. Wählen Sie bei Bedarf **Fortschritt ausblenden** aus, um das Klonen im Hintergrund auszuführen.
- Der geklonte Katalog erhält den Namen des Originals und hat das Suffix `Copy`. Der Name kann geändert werden. Weitere Informationen finden Sie unter Umbenennen von Maschinenkatalogen.
- Weisen Sie den geklonten Katalog unbedingt einer Bereitstellungsgruppe zu.

1. Melden Sie sich bei Web Studio an und wählen Sie im linken Bereich **Maschinenkataloge**.
2. Wählen Sie einen Katalog und dann in der Aktionsleiste **Klonen**.
3. Prüfen Sie im Fenster **Ausgewählten Maschinenkatalog klonen** die Einstellungen für den geklonten Katalog und bearbeiten Sie diese nach Bedarf. Wählen Sie **Weiter**, um mit der nächsten Seite fortzufahren.

4. Überprüfen Sie auf der Seite **Zusammenfassung** die Einstellungen und wählen Sie **Fertigstellen**, um das Klonen zu starten.
5. Wählen Sie bei Bedarf **Fortschritt ausblenden** aus, um das Klonen im Hintergrund auszuführen.

## Organisieren von Katalogen mit Ordnern

Sie können Ordner erstellen, um Kataloge für einfachen Zugriff zu organisieren. Sie können beispielsweise Kataloge nach Imagetyp oder Organisationsstruktur organisieren.

### Erstellen von Katalogordnern

Planen Sie zunächst, wie Sie Ihre Kataloge organisieren wollen. Beachten Sie Folgendes:

- Sie können Ordner mit einer Tiefe von bis zu fünf Ebenen verschachteln (mit Ausnahme des Standardstammordners).
- Ein Katalogordner kann Kataloge und Unterordner enthalten.
- Alle Knoten in Web Studio (wie die Knoten **Maschinenkataloge** und **Anwendungen**) teilen sich eine Ordnerstruktur im Back-End. Um Namenskonflikte mit anderen Knoten beim Umbenennen oder Verschieben von Ordnern zu vermeiden, empfehlen wir, Ordnern der ersten Ebene in verschiedenen Knoten unterschiedliche Namen zu geben.

Gehen Sie wie folgt vor, um einen Katalogordner zu erstellen:

1. Wählen Sie im linken Bereich **Maschinenkataloge**.
2. Wählen Sie in der Ordnerhierarchie einen Ordner aus und klicken Sie dann in der **Aktionsleiste** auf **Ordner erstellen**.
3. Geben Sie einen Namen für den neuen Ordner ein und klicken Sie dann auf **Fertig**.

> **Tipp:**
>
> Wenn Sie einen Ordner an einem falschen Speicherort erstellen, können Sie ihn an den korrekten Speicherort ziehen.

### Verschieben von Katalogen

Sie können einen Katalog zwischen Ordnern verschieben. Verfahren:

1. Wählen Sie im linken Bereich **Maschinenkataloge**.
2. Zeigen Sie Kataloge nach Ordnern an. Sie können auch die Option **Alle anzeigen** über der Ordnerhierarchie aktivieren, um alle Kataloge gleichzeitig anzuzeigen.

3. Klicken Sie mit der rechten Maustaste auf einen Katalog und wählen Sie dann **Maschinenkatalog verschieben** aus.
4. Wählen Sie den Ordner aus, in den Sie den Katalog verschieben möchten, und klicken Sie dann auf **Fertig**.

> **Tipp:**
>
> Sie können einen Katalog in einen Ordner ziehen.

#### Verwalten von Katalogordnern

Sie können Katalogordner löschen, umbenennen und verschieben.

Sie können einen Ordner nur löschen, wenn er und seine Unterordner keine Kataloge enthalten.

Gehen Sie wie folgt vor, um einen Ordner zu verwalten:

1. Wählen Sie im linken Bereich **Maschinenkataloge**.
2. Wählen Sie in der Ordnerhierarchie einen Ordner aus und wählen Sie dann eine gewünschte Aktion in der **Aktionsleiste** aus:
   - Wählen Sie zum Umbenennen des Ordners **Ordner umbenennen** aus.
   - Wählen Sie zum Löschen des Ordners **Ordner löschen** aus.
   - Wählen Sie zum Verschieben des Ordners **Ordner verschieben** aus.
3. Folgen Sie den Anweisungen auf dem Bildschirm, um die restlichen Schritte auszuführen.

### PowerShell verwenden

In diesem Abschnitt wird beschrieben, wie Sie Kataloge mit PowerShell verwalten:

- Mit einem Katalog verknüpfte Warnungen und Fehler abrufen
- Einmaligen Neustart planen
- Beschreibung zu einem Image hinzufügen
- Zurücksetzen des OS-Datenträgers
- Ändern der Netzwerkeinstellung für ein vorhandenes Provisioningschema
- Versionen eines Maschinenkatalogs verwalten
- Maschinenkatalog, der nicht auf Maschinenprofilen basiert, in einen auf einem Maschinenprofil basierenden Maschinenkatalog in einer Azure-Umgebung konvertieren
- Identitätsinformationen aktiver Computerkonten reparieren
- Cachekonfiguration eines Maschinenkatalogs ändern
- VDA-Aktualisierungsunterstützung über lokalen Dateifreigabezugriff

### Mit einem Katalog verknüpfte Warnungen und Fehler abrufen

Sie können historische Fehler und Warnungen abrufen, um Probleme mit Ihrem MCS-Maschinenkatalog zu diagnostizieren und zu beheben.

Mithilfe von PowerShell-Befehlen können Sie:

- eine Liste der Fehler und Warnungen abrufen
- Status von Warnungen von **New** in **Acknowledged** ändern
- Fehler oder Warnungen löschen

Ausführen der PowerShell-Befehle:

1. Öffnen Sie ein PowerShell-Fenster.
2. Führen Sie `asnp citrix*` aus, um die Citrix-spezifischen PowerShell-Module zu laden.

Um eine Liste der Fehler und Warnungen abzurufen:

Führen Sie den Befehl `Get-ProvOperationEvent` aus.

- Ohne Parameter: Ruft alle Fehler und Warnungen ab.
- Mit den Parametern `LinkedObjectType` und `LinkedObjectUid`: Ruft alle Fehler und Warnungen, die mit einem bestimmten Provisioningschema verknüpft sind, ab.
- Mit Parameter `EventId`: Ruft den Fehler bzw. die Warnung mit der entsprechenden Ereignis-ID ab.
- Mit Parameter `Filter`: Ruft Fehler oder Warnungen unter Anwendung eines benutzerdefinierten Filters ab.

Statusänderung von Fehlern oder Warnungen von **New** in **Acknowledged**:

Führen Sie den Befehl `Confirm-ProvOperationEvent` aus.

- Mit Parameter `EventId`: Legt den Status des Fehlers bzw. der Warnung mit der entsprechenden Ereignis-ID ab. Sie können die `EventId` eines Fehlers oder einer Warnung als Ausgabe des Befehls `Get-ProvOperationEvent` abrufen.
- Mit den Parametern `LinkedObjectType` und `LinkedObjectUid`: Legt den Status aller Fehler und Warnungen, die mit einem bestimmten Provisioningschema verknüpft sind, fest.
- Mit Parameter `All`: Setzt den Status aller Fehler und Warnungen auf **Acknowledged**.

Fehler oder Warnungen löschen:

Führen Sie den Befehl `Remove-ProvOperationEvent` aus.

- Mit Parameter `EventId`: Entfernt den Fehler bzw. die Warnung mit der entsprechenden Ereignis-ID. Sie können die `EventId` eines Fehlers oder einer Warnung als Ausgabe des Befehls `Get-ProvOperationEvent` abrufen.

- Mit den Parametern `LinkedObjectType` und `LinkedObjectUid`: Löscht alle Fehler und Warnungen, die mit einem bestimmten Provisioningschema verknüpft sind.
- Mit Parameter `All`: Löscht alle Fehler und Warnungen.

Weitere Informationen finden Sie unter Citrix PowerShell SDK.

### Einmaligen Neustart planen

Wenn Sie mit PowerShell einen einmaligen Neustart planen möchten, verwenden Sie die folgenden PowerShell-Befehle für `BrokerCatalogRebootSchedule`, um den Plan für einen Neustart zu erstellen, zu ändern und zu löschen:

- Get-BrokerCatalogRebootSchedule
- New-BrokerCatalogRebootSchedule
- Set-BrokerCatalogRebootSchedule
- Remove-BrokerCatalogRebootSchedule
- Rename-BrokerCatalogRebootSchedule

Beispiel:

- Neustart der VMs im Katalog **BankTellers** planen, der am 3. Februar 2022 zwischen 2:00 Uhr und 4:00 Uhr beginnen soll.

```
C:\PS> New-BrokerCatalogRebootSchedule -Name BankTellers -
    CatalogName BankTellers  -StartDate "2022-02-03" -StartTime "
    02:00" -Enabled $true -RebootDuration 120
<!--NeedCopy-->
```

- Neustart der VMs im Katalog mit UID 17 planen, der am 3. Februar 2022 zwischen 1:00 Uhr und 5:00 Uhr beginnen soll. Zehn Minuten vor dem Neustart erscheint auf jeder VM in allen Benutzersitzungen ein Warnhinweis mit dem Titel **WARNUNG: Ausstehender Neustart** und der Nachricht **Speichern Sie Ihre Arbeit**.

```
C:\PS> New-BrokerCatalogRebootSchedule -Name 'Update reboot' -
    CatalogUid 17 -StartDate "2022-02-03" -StartTime "01:00" -
    Enabled $true -RebootDuration 240 -WarningTitle "WARNING:
    Reboot pending" -WarningMessage "Save your work" -
    WarningDuration 10
<!--NeedCopy-->
```

- Katalogneustartplan umbenennen von **Old Name** in **New Name**.

```
C:\PS> Rename-BrokerCatalogRebootSchedule -Name "Old Name" -
    NewName "New Name"
<!--NeedCopy-->
```

- Alle Katalogneustartpläne mit UID 1 anzeigen und Zeitplan für den Katalogneustart mit UID 1 in **New Name** umbenennen.

```
C:\PS> Get-BrokerCatalogRebootSchedule -Uid 1 | Rename-
    BrokerCatalogRebootSchedule -NewName "New Name" -PassThru
<!--NeedCopy-->
```

- Meldung mit dem Titel **WARNUNG: Ausstehender Neustart** und der Nachricht **Speichern Sie Ihre Arbeit** für Katalogneustartplan **Accounting** einrichten und festlegen, dass die Meldung zehn Minuten vor dem Neustart jeder VM angezeigt wird. Die Meldung wird in jeder Benutzersitzung auf dieser VM angezeigt.

  “‘

  C:\PS> Set-BrokerCatalogRebootSchedule -Name Accounting -WarningMessage “Speichern Sie Ihre Arbeit”-WarningDuration 10 -WarningTitle “WARNUNG: Ausstehender Neustart”

- Alle deaktivierten Neustartpläne anzeigen und anschließend aktivieren.

```
C:\PS> Get-BrokerCatalogRebootSchedule -Enabled $false | Set-
    BrokerCatalogRebootSchedule -Enabled $true
<!--NeedCopy-->
```

- Meldung **Neustart in %m% Minuten** für Katalogneustartplan mit UID 17 einrichten und festlegen, dass die Meldung fünfzehn, zehn und fünf Minuten vor dem Neustart jeder VM angezeigt wird.

```
C:\PS> Set-BrokerCatalogRebootSchedule 17 -WarningMessage "
    Rebooting in %m% minutes." -WarningDuration 15 -
    WarningRepeatInterval 5
<!--NeedCopy-->
```

- Zeitzone für den Katalog **MyCatalog** konfigurieren.

```
C:\PS> Set-BrokerCatalog -Name "MyCatalog" -TimeZone <TimeZone>
<!--NeedCopy-->
```

### Beschreibung zu einem Image hinzufügen

Sie können Informationen zu Änderungen im Zusammenhang mit Image-Updates für Maschinenkataloge hinzufügen. Mit dem Feature können Sie beim Erstellen eines Katalogs oder beim Aktualisieren eines bestehenden Masterimages für einen Katalog eine Beschreibung hinzufügen. Sie können auch Informationen für jedes Masterimage im Katalog anzeigen. Verwenden Sie die folgenden Befehle, um Imagebeschreibungen hinzuzufügen oder anzuzeigen:

- Verwenden Sie den Parameter `MasterImageNote` im Befehl `NewProvScheme`, um beim Erstellen eines Maschinenkatalogs mit einem Masterimage eine Notiz hinzuzufügen. Beispiel:

```
C:\PS>New-ProvScheme -ProvisioningSchemeName <name> -
    HostingUnitName <name> -IdentityPoolName <name> -MasterImageVM
XDHyp:\HostingUnits<hosting unit name><vm name>.vm\Base.snapshot
    -MasterImageNote "Note"
<!--NeedCopy-->
```

- Verwenden Sie den Parameter `MasterImageNote` im Befehl `Publish-ProvMasterVMImage`, um das einem Maschinenkatalog zugeordnete Masterimage zu aktualisieren. Beispiel:

```
C:\PS>Publish-ProvMasterVMImage -ProvisioningSchemeName <name> -
    MasterImageVM XDHyp:\HostingUnits<hosting unit name><vm name>.
    vm\base.snapshot -MasterImageNote "Note"
<!--NeedCopy-->
```

- Verwenden Sie den Befehl Get-ProvSchemeMasterVMImageHistory, um die Informationen für jedes Image anzuzeigen. Beispiel:

```
C:\PS>Get-ProvSchemeMasterVMImageHistory -ProvisioningSchemeName
    MyScheme -Showall
<!--NeedCopy-->
```

Um den Rollback-Fortschritt zu verfolgen, suchen Sie den Katalog in **Maschinenkatalogen**, um den Fortschrittsbalken und das Fortschrittsdiagramm anzuzeigen.

In folgenden Szenarios ist kein Rollback möglich. (Die Option **Rollback für Masterimage ausführen** wird nicht angezeigt).

- Sie haben keine Berechtigung zum Rollback.
- Der Katalog wurde nicht mit MCS erstellt.
- Der Katalog wurde mit einem Image des Betriebssystemdatenträgers erstellt.
- Der zum Erstellen des Katalogs verwendete Snapshot ist beschädigt.
- Benutzeränderungen an den Maschinen in dem Katalog bleiben nicht erhalten.
- Maschinen im Katalog werden ausgeführt.

### Zurücksetzen des OS-Datenträgers

Verwenden Sie den PowerShell-Befehl `Reset-ProvVMDisk`, um den OS-Datenträger einer persistenten VM in einem mit MCS erstellten Maschinenkatalog zurückzusetzen. Derzeit gilt diese Funktion für AWS, Azure, XenServer und Google Cloud. SCVMM- und VMware-Virtualisierungsumgebungen.

Um den PowerShell-Befehl erfolgreich auszuführen, stellen Sie Folgendes sicher:

- Die Ziel-VMs befinden sich in einem persistenten MCS-Katalog.
- Der MCS-Maschinenkatalog funktioniert einwandfrei.
- Hierfür müssen das Provisioningschema und der Host vorhanden sein und das Provisioningschema über korrekte Einträge verfügen.

- Der Hypervisor ist nicht im Wartungsmodus.
- Die Ziel-VMs sind ausgeschaltet und im Wartungsmodus.

Führen Sie die folgenden Schritte aus, um den OS-Datenträger zurückzusetzen:

1. Öffnen Sie ein PowerShell-Fenster.
2. Führen Sie **asnp citrix*** aus, um die Citrix-spezifischen PowerShell-Module zu laden.
3. Führen Sie den PowerShell-Befehl `Reset-ProvVMDisk` auf eine der folgenden Arten aus:

   - Geben Sie die Liste der VMs als durch Trennzeichen getrennte Liste an und führen Sie das Zurücksetzen auf jeder VM durch:

   ```
   Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName ("abc"
       ,"def") -OS
   <!--NeedCopy-->
   ```

   - Geben Sie die Liste der VMs als Ausgabe des Befehls `Get-ProvVM` an und führen Sie das Zurücksetzen auf jeder VM durch:

   ```
   (Get-ProvVM -ProvisioningSchemeName "xxx") | Reset-ProvVMDisk
       "abc" -OS
   <!--NeedCopy-->
   ```

   - Geben Sie eine VM mit Namen an:

   ```
   Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc"
       -OS
   <!--NeedCopy-->
   ```

   - Erstellen Sie einen eigenen Reset-Task für jede vom Befehl `Get-ProvVM` zurückgegebene VM. Dies ist weniger effizient, da jeder Task dieselben redundanten Prüfungen durchführt (z. B. Hypervisor-Funktionsprüfung und Verbindungsprüfung).

   ```
   Get-ProvVM -ProvisioningSchemeName "xxx" | Reset-ProvVMDisk -
       ProvisioningSchemeName "xxx" -OS
   <!--NeedCopy-->
   ```

4. Eine Bestätigungsaufforderung wird angezeigt, in der die zurückzusetzenden VMs zusammen mit einer Warnmeldung aufgeführt sind, dass es sich um einen nicht umkehrbaren Vorgang handelt. Wenn Sie keine Antwort geben und die **Eingabetaste**drücken, findet keine weitere Aktion statt.

   > **Hinweis:**
   >
   > Nehmen Sie VMs erst nach Abschluss der Zurücksetzung aus dem Wartungsmodus und schalten Sie sie ein.

Sie können den PowerShell-Befehl `-WhatIf` ausführen, um die auszuführende Aktion zu drucken und den Vorgang ohne Ausführen der Aktion zu beenden.

Sie können die Bestätigungsaufforderung auch mit einer der folgenden Methoden umgehen:

- Geben Sie den Parameter `-Force` an:

```
Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc"
    -OS -Force
<!--NeedCopy-->
```

- Geben Sie den Parameter `-Confirm:$false` an:

```
Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc"
    -OS -Confirm:$false
<!--NeedCopy-->
```

- Bevor Sie `Reset-ProvVMDisk` ausführen, ändern Sie `$ConfirmPreference` zu **None**:

```
PS C:\Windows\system32> $ConfirmPreference='None'
PS C:\Windows\system32> $ConfirmPreference
None
PS C:\Windows\system32> Reset-ProvVMDisk -
    ProvisioningSchemeName "xxx" -VMName "abc" -OS
<!--NeedCopy-->
```

5. Führen Sie `Get-ProvTask` aus, um den Status der von Befehl `Reset-ProvVMDisk` zurückgegebenen Tasks abzurufen.

### Ändern der Netzwerkeinstellung für ein vorhandenes Provisioningschema

Sie können die Netzwerkeinstellung für ein vorhandenes Provisioningschema ändern, sodass die neuen VMs im neuen Subnetz erstellt werden. Verwenden Sie den Parameter `-NetworkMapping` im Befehl `Set-ProvScheme`, um die Netzwerkeinstellung zu ändern.

> **Hinweis:**
>
> Diese Funktion wird auf Citrix Virtual Apps and Desktops 2203 LTSR CU3 und späteren Versionen unterstützt.

Führen Sie folgende Schritte aus, um die Netzwerkeinstellung für ein vorhandenes Provisioningschema zu ändern:

1. Führen Sie im PowerShell-Fenster den Befehl `asnp citrix*` aus, um die PowerShell-Module zu laden.
2. Führen Sie `(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps` aus, um zum Netzwerkpfad zu gelangen, den Sie ändern möchten.

3. Weisen Sie der neuen Netzwerkeinstellung eine Variable zu. Beispiel:

```
$NewNetworkMap = @{
 "0"= "XDHYP:\HostingUnits\MyNetworks\Network 0.network" }

<!--NeedCopy-->
```

4. Führen Sie `Set-ProvScheme -ProvisioningSchemeName "name"-NetworkMapping $NewNetworkMap` aus.
5. Führen Sie `(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps` aus, um die neue Netzwerkeinstellung für das vorhandene Provisioningschema zu überprüfen.

### Versionen eines Maschinenkatalogs verwalten

Wenn ein MCS-Maschinenkatalog mit dem Befehl `Set-ProvScheme` aktualisiert wird, wird die aktuelle Konfiguration als Version gespeichert. Anschließend können Sie die verschiedenen Versionen des Maschinenkatalogs mithilfe von PowerShell-Befehlen verwalten. Sie haben folgende Möglichkeiten:

- Liste der Versionen eines Maschinenkatalogs anzeigen
- Eine frühere Version verwenden, um den Maschinenkatalog zu aktualisieren
- Version manuell löschen, wenn sie nicht von einer VM dieses Maschinenkatalogs verwendet wird
- Maximale Anzahl von Versionen ändern, die vom Maschinenkatalog beibehalten werden sollen (Standardeinstellung ist 99)

Eine Version enthält die folgenden Informationen eines Maschinenkatalogs:

- VMCpuCount
- VMMemoryMB
- CustomProperties
- ServiceOffering
- MachineProfile
- NetworkMapping
- SecurityGroup

Führen Sie die folgenden Befehle (Beispiele werden angezeigt) aus, um die verschiedenen Versionen eines Maschinenkatalogs zu verwalten.

- So zeigen Sie die Konfigurationsdetails der verschiedenen Versionen eines Maschinenkatalogs an:

```
Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog
<!--NeedCopy-->
```

- So zeigen Sie die Konfigurationsdetails einer bestimmten Version eines Maschinenkatalogs an:

```
Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog -
    Version 2
<!--NeedCopy-->
```

- So zeigen Sie die Gesamtzahl der Versionen an, die einem Maschinenkatalog zugeordnet sind:

  ‘‘‘

  (Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog).Count

- So aktualisieren Sie den Maschinenkatalog mit einer früheren Version:

```
Set-ProvScheme -ProvisioningSchemeName AzureCatalog -Version 2
<!--NeedCopy-->
```

- So löschen Sie eine Version manuell, wenn sie nicht von einer VM dieses Maschinenkatalogs verwendet wird:

```
Remove-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog -
    Version 3
<!--NeedCopy-->
```

- So legen Sie die maximale Anzahl von Versionen fest, die vom Maschinenkatalog beibehalten werden sollen (Standardeinstellung ist 99). Diese Einstellung wird auf alle Kataloge angewendet. In diesem Fall werden beispielsweise maximal 15 Versionen für alle von MCS bereitgestellten Kataloge beibehalten.

```
Set-ProvServiceConfigurationData -Name "MaxProvSchemeVersions" -
    Value 15
<!--NeedCopy-->
```

Wenn die Anzahl der Versionen die maximale Anzahl erreicht, kann keine neue Version erstellt werden, solange ältere Versionen von einer der virtuellen Maschinen im Maschinenkatalog verwendet werden. Führen Sie in diesem Fall einen der folgenden Schritte aus:

- Erhöhen Sie das Limit für die maximale Anzahl von Versionen, die im Maschinenkatalog aufbewahrt werden sollen.
- Aktualisieren Sie einige VMs, die sich auf älteren Versionen befinden, sodass diese älteren Versionen von keiner VM mehr referenziert werden und gelöscht werden können.

### Maschinenkatalog, der nicht auf Maschinenprofilen basiert, in einen auf einem Maschinenprofil basierenden Maschinenkatalog in einer Azure-Umgebung konvertieren

Sie können eine VM, eine Vorlagenspezifikation (Azure) oder eine Startvorlage (AWS) als Maschinenprofileingabe verwenden, um einen Maschinenkatalog, der nicht auf Maschinenprofilen basiert, in

einen auf einem Maschinenprofil basierenden Maschinenkatalog zu konvertieren. Neue virtuelle Maschinen, die dem Katalog hinzugefügt werden, übernehmen Eigenschaftswerte aus dem Maschinenprofil, sofern sie nicht durch eine explizite benutzerdefinierte Eigenschaft überschrieben werden.

> **Hinweis:**
>
> Ein Maschinenkatalog, der auf einem Maschinenprofil basiert, kann nicht in einen Maschinenkatalog geändert werden, der nicht auf einem Maschinenprofil basiert.

Gehen Sie hierzu folgendermaßen vor:

1. Erstellen Sie einen persistenten oder nicht persistenten Maschinenkatalog mit VMs und ohne Maschinenprofil.
2. Öffnen Sie das **PowerShell**-Fenster.
3. Führen Sie den Befehl `Set-ProvScheme` aus, um die Eigenschaftswerte aus dem Maschinenprofil auf die neuen VMs anzuwenden, die dem Maschinenkatalog hinzugefügt werden. Beispiel:

   - Azure:

   ```
   Set-ProvScheme = Set-ProvScheme -ProvisioningSchemeName xxxx
       -MachineProfile XDHyp:\HostingUnits<HostingUnitName>\
       machineprofile.folder<ResourceGroupName><TemplateSpecName
       ><VersionName>
   <!--NeedCopy-->
   ```

   - AWS:

   ```
   Set-ProvScheme = Set-ProvScheme -ProvisioningSchemeName xxxx
       -MachineProfile "XDHyp:\HostingUnits<hosting-unit><launch-
       template>.launchtemplate<launch-template-version>.
       launchtemplateversion"
   <!--NeedCopy-->
   ```

### Identitätsinformationen aktiver Computerkonten reparieren

Sie können die Identitätsinformationen von aktiven Computerkonten mit Identitätsproblemen zurücksetzen. Sie können wählen, ob Sie nur das Maschinenkennwort und die vertrauenswürdigen Schlüssel-IDs oder die gesamte Konfiguration des Identitätsdatenträgers zurücksetzen möchten. Diese Implementierung gilt für persistente und nicht persistente MCS-Maschinenkataloge.

> **Hinweis:**
>
> Derzeit wird das Feature nur für Azure- und VMware-Virtualisierungsumgebungen unterstützt.

### Bedingungen

Um den Identitätsdatenträger erfolgreich zurückzusetzen:

- Schalten Sie die VM aus und versetzen Sie sie in den Wartungsmodus.
- Verwendung Sie nicht den Parameter "-OS"im PowerShell-Befehl.

### Identitätsdatenträger zurücksetzen

Gehen Sie zum Zurücksetzen des Identitätsdatenträgers folgendermaßen vor:

1. Öffnen Sie das **PowerShell**-Fenster.
2. Führen Sie `asnp citrix*` aus, um die Citrix-spezifischen PowerShell-Module zu laden.
3. Setzen Sie die Identitätsinformationen zurück.

   - Um nur das Maschinenkennwort und Vertrauensschlüssel zurückzusetzen, führen Sie die folgenden Befehle in der Reihenfolge ihrer Aufführung aus:

     ```
     1  Repair-AcctIdentity -IdentityAccountName TEST\VM1 -
           PrivilegedUserName TEST\admin1 -PrivilegedUserPassword
           $password -Target IdentityInfo
     2  <!--NeedCopy-->
     ```

     Die Beschreibungen der Befehlsparameter:

     - `IdentityAccountName`: Name des Identitätskontos, das repariert werden muss.
     - `PrivilegedUserName`: Benutzerkonto mit Schreibberechtigung für den Identitätsanbieter (AD oder AzureAD).
     - `PrivilegedUserPassword`: Kennwort für PrivilegedUserName.
     - `Target`: Ziel für die Reparaturaktion. Dies kann IdentityInfo zur Reparatur von Kontokennwort/Vertrauensschlüssel sein und UserCertificate für Benutzerzertifikatattribute von Maschinenidentitäten mit Hybrid-AzureAD-Verbindung.

     ```
     1  Reset-ProvVMDisk -ProvisioningSchemeName <name> -VMname <name
           > -Identity -ResetIdentityInfo
     2  <!--NeedCopy-->
     ```

     Der Parameter `ResetIdentityInfo` setzt Folgendes zurück:

     - Kennwort und Vertrauensschlüssel: wenn die VM einer AD-Domäne angehört
     - Nur Vertrauensschlüssel: wenn die VM keiner AD-Domäne angehört
     - Nur Kennwort: Wenn die VM einer AD-Domäne angehört

   - Um die gesamte Konfiguration des Identitätsdatenträgers zurückzusetzen, führen Sie die folgenden Befehle in der angegebenen Reihenfolge aus:

```
Repair-AcctIdentity -IdentityAccountName TEST\VM1 -
    PrivilegedUserName TEST\admin1 -PrivilegedUserPassword
    $password -Target IdentityInfo
<!--NeedCopy-->
```

```
Reset-ProvVMDisk ProvisioningSchemeName <name> -VMName <name>
     -Identity
<!--NeedCopy-->
```

4. Geben Sie **y** ein, um die Aktion zu bestätigen. Sie können die Bestätigungsaufforderung auch mithilfe des Parameters `-Force` auslassen. Beispiel:

```
Reset-ProvVMDisk -ProvisioningSchemeName <name> -VMName <name> -
    Identity -Force
<!--NeedCopy-->
```

5. Führen Sie den Befehl `Get-ProvVM -ProvisioningSchemeName <name -VMName <name>` aus, um die Einstellung des aktualisierten Identitätsdatenträgers zu überprüfen. Die Attribute des Identitätsdatenträgers (z. B. `IdentityDiskId`) müssen aktualisiert worden sein. `StorageId` und `IdentityDiskIndex` dürfen sich nicht ändern.

### Cachekonfiguration eines Maschinenkatalogs ändern

Nach der Erstellung eines nicht persistenten Katalogs mit aktiviertem MCSIO können Sie mit dem Befehl “Set-ProvScheme”die folgenden Parameter ändern:

- WriteBackCacheMemorySize
- WriteBackCacheDiskSize

Das Feature gilt derzeit für:

- GCP- und Microsoft Azure-Umgebungen sowie
- nicht persistenter Katalog mit aktiviertem MCSIO

#### Anforderungen

Anforderungen zum Ändern der Cachekonfiguration:

- Update auf die neueste VDA-Version (2308 oder höher).
- Aktivieren des Parameters `UseWriteBackCache` für den Maschinenkatalog. Verwendung von `New-ProvScheme`, um einen Maschinenkatalog mit aktiviertem `UseWriteBackCache` zu erstellen. Beispiel:

```
New-ProvScheme -ProvisioningSchemeName $CatalogName -
    HostingUnitUid $HostingUnitUid `
-IdentityPoolUid $acctPool.IdentityPoolUid -CleanOnBoot `
-MasterImageVM $MasterImage `
-ServiceOffering $ServiceOffering `
-NetworkMap $NetworkMap `
-SecurityGroup $SecurityGroup `
-UseWriteBackCache -WriteBackCacheDiskSize 8
<!--NeedCopy-->
```

#### Cachekonfiguration ändern

Führen Sie den Befehl Set-ProvScheme aus. Beispiel:

```
Set-ProvScheme -ProvisioningSchemeName $provScheme.
    ProvisioningSchemeName -WriteBackCacheDisk32 -
    WriteBackCacheMemorySize 128
<!--NeedCopy-->
```

> **Hinweis:**
>
> - Der Wert von `WriteBackCacheDiskSize` muss größer als Null sein, da mindestens 1 GB Cachedatenträgerplatz erforderlich ist.
> - Der Wert von `WriteBackCacheMemorySize` muss kleiner als die Speichergröße des Maschinenkatalogs sein.
> - Diese Änderungen werden nur auf neue VMs anwendet, die dem Katalog hinzugefügt wurden, nachdem die Änderung vorgenommen wurde. Bestehende VMs sind von diesen Änderungen nicht betroffen.

### VDA-Aktualisierungsunterstützung über lokalen Dateifreigabezugriff

Geben Sie den Speicherort des VDA-Installationsprogramms mit PowerShell-Cmdlets an, sodass Sie weniger Netzwerkregeln bereitstellen müssen, damit jeder VDA das neue VDA-Installationsprogramm vom Citrix Managed Azure CDN abrufen kann.

#### PowerShell-Cmdlets

Den Cmdlets **New-VusCatalogSchedule** und **New-VusMachineUpgrade** wurden zwei neue optionale Parameter hinzugefügt, mit denen Sie Installationsprogramme von einer lokalen Dateifreigabe aus verwenden können.

- **VdaWorkstationPackageUri**: um den UNIC-Pfad zum VDA-Installationsprogramm für Arbeitsstationsbetriebssysteme anzugeben

- **VdaServerPackageUri**: um den UNC-Pfad zum VDA-Installationsprogramm für das Serverbetriebssystem anzugeben

**Voraussetzungen**

- VUS Agent-Installationsprogramm, das im Lieferumfang von VDA 2311 enthalten ist
- VDA Upgrade Agent auf Version 7.40.0.35 oder höher (mit dem VDA-Installationsprogramm Version 2311 oder höher)
- Virtual Apps and Desktops Remote PowerShell SDK Version 7.40 oder höher (veröffentlicht am 10. Januar 2024 oder später)

**So legen Sie Dateifreigabeberechtigungen fest**

Die Netzwerkfreigaben, die VDA-Installationspakete enthalten, müssen Lesezugriff für den VDA Upgrade Agent-Dienst haben, der als Lokales System (NT AUTHORITY\SYSTEM-Prinzipal) ausgeführt wird.

- **Freigabeberechtigung für Dateien, die in eine Domäne eingebunden sind**

  Wenn die VDA-Maschine einer Domäne beigetreten ist, verwendet das **lokale Systemkonto** (VUA wird als lokales System ausgeführt) Computeranmeldeinformationen für den Zugriff auf Netzwerkfreigaben.

  Die geringste Berechtigung kann festgelegt werden, indem Domänencomputern **Lesezugriff** gewährt wird.

  1. Wählen Sie Personen in Ihrem Netzwerk aus, für die Sie die Datei freigeben möchten.
  2. Klicken Sie auf **Erweiterte Freigabeeinstellungen** und aktivieren Sie die **Datei- und Druckerfreigabe**.

- **Erlaubnis zur Freigabe von Dateien, die nicht mit einer Domäne verbunden sind**

  Wenn die VDA-Maschine nicht in eine Domäne eingebunden ist, verwendet das **lokale Systemkonto** (VUA wird als lokales System ausgeführt) **ANONYMOUS LOGON,** wenn auf Netzwerkfreigaben zugegriffen wird.

  1. Wählen Sie einen freigegebenen Ordner aus.
  2. Deaktivieren Sie den Kennwortschutz.
     a) Gehen Sie zum Ordner **Eigenschaften**.
     b) Wählen Sie **Netzwerk- und Freigabecenter** aus.
     c) Schalten Sie **Kennwortgeschützte Freigabe** aus.
  3. Klicken Sie auf **Erweiterte Freigabe**, um eine Freigabeberechtigung zu erteilen.

a) Wählen Sie **Berechtigungen**.
b) Erteilen Sie **ANONYMOUS LOGON** eine Freigabe-**Leseberechtigung**.

4. Wählen Sie die Registerkarte **Sicherheit**, um Ordnerberechtigungen zu gewähren
   a) Klicken Sie auf **Bearbeiten**, um dem freigegebenen Ordner Berechtigungen hinzuzufügen.
   b) Wählen Sie den freigegebenen Ordner aus, um **ANONYMOUS LOGON** Ordnerberechtigungen zu gewähren.
5. Klicken Sie auf **Erweitert**, um die **Datei- und Druckerfreigabe** zu aktivieren.
6. Fügen Sie den Namen des freigegebenen Ordners zur **Netzwerkzugriffssicherheitsrichtlinie** hinzu.

> **Hinweis:**
>
> Starten Sie Ihre Maschine neu, damit die Änderung sofort wirksam wird.

**VDA-Updates von einer lokalen Dateifreigabe**

1. Laden Sie das VDA-Installationsprogramm herunter und platzieren Sie es in der freigegebenen Datei.

   > **Hinweis:**
   >
   > Mit Virtual Upgrade Service können Sie zwischen dem Titel Current Release oder LTSR-Track wählen.
   >
   > **Beispiel:** Wenn für den Maschinenkatalog die aktuelle Version 2311 festgelegt ist und die VDA-Version 2305 ist, müssen Sie den VDA auf Version 2311 aktualisieren.

   a) Navigieren Sie zur Seite **Downloads** auf unserer Website.
   b) Wählen Sie **Citrix Virtual Apps and Desktops** als Produkt aus.
   c) Wählen Sie **Citrix Virtual Apps and Desktops 7 2311, alle Editionen**.
   d) Wählen Sie das VDA-Installationsprogramm aus den **Komponenten aus, die sich auf der Produkt-ISO befinden, aber auch separat erweiterbar** sind.

2. Wählen Sie das entsprechende VDA-Installationsprogramm basierend auf dem Katalogtyp aus.

   - Laden Sie das **VDA-Installationsprogramm für Multisitzungs-OS** herunter, wenn der Katalogtyp **Mehrere Sitzungen** ist.
   - Laden Sie das **VDA-Installationsprogramm für Einzelsitzungs-OS** herunter, wenn der Katalogtyp **Einzelsitzung** ist.
   - Laden Sie das **Installationsprogramm des Kernkomponenten-VDA unter Einzelsitzungs-OS-Betriebssystem** herunter, wenn der Katalogtyp **Remote-PC-Zugriff** ist.

> **Hinweis:**
>
> Die Version des Fileshare-Installationsprogramms muss **genau** mit der Version der neuesten Version des Installationsprogramms übereinstimmen, die von VUS in der Cloud veröffentlicht wurde.

### 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.

### So geht es weiter

Informationen zum Verwalten bestimmter Cloudservices-Kataloge finden Sie unter:

- AWS-Katalog verwalten
- XenServer-Katalog verwalten
- Google Cloud Platform -Katalog verwalten
- Microsoft Azure-Katalog verwalten
- Microsoft System Center Virtual Machine Manager-Katalog verwalten
- VMware-Katalog verwalten

## AWS-Katalog verwalten

June 27, 2024

Unter Maschinenkataloge verwalten werden die Assistenten zum Verwalten eines Maschinenkatalogs beschrieben. Die folgenden Informationen beziehen sich speziell auf AWS-Cloudumgebungen.

> **Hinweis:**
>
> Sie müssen einen AWS-Katalog erstellt haben, bevor Sie ihn verwalten können. Siehe AWS-Katalog erstellen.

### Tags entfernen

Wenn Sie einen Katalog oder eine VM erstellen, werden von MCS erstellte Tags für folgende Ressourcen erstellt:

- Virtuelle Maschine
- Stammdatenträger-Volume
- Identitätsdatenträger-Volume
- Netzwerkkarte
- Stammdatenträgerimage (AMI)
- Startvorlage
- Snapshot von AMI oder Stammdatenträger

Sie können VMs und Maschinenkataloge aus der Citrix Datenbank sowie von MCS erstellte Tags entfernen. Optionen:

- Verwenden Sie `Remove-ProvVM` mit dem Parameter `ForgetVM` zum Entfernen von VMs und von MCS erstellten Tags aus einer einzelnen VM oder einer Liste von VMs aus einem Maschinenkatalog.
- `Remove-ProvScheme` mit Parameter `ForgetVM` zum Entfernen eines Maschinenkatalogs aus der Citrix Datenbank und von Ressourcen aus einem Maschinenkatalog.

Dieses Feature ist nur für persistente VMs verfügbar.

Gehen Sie hierzu folgendermaßen vor:

1. Öffnen Sie ein **PowerShell**-Fenster.
2. Führen Sie `asnp citrix*` aus, um die Citrix-spezifischen PowerShell-Module zu laden.
3. Entsperren Sie die VM, bevor Sie die VMs entfernen. Beispiel:

```
Unlock-ProvVM -ProvisioningSchemeName "<name>" -VMID "<id"
<!--NeedCopy-->
```

4. Führen Sie einen der folgenden Befehle aus, um VMs, Maschinenkataloge und von MCS erstellte Tags aus Ressourcen zu entfernen.

   - Führen Sie `Remove-ProvVM` mit `ForgetVM` aus, um VMs aus der Citrix-Datenbank und Tags aus VMs zu entfernen. Beispiel:

```
Remove-ProvVM -ProvisioningSchemeName "<name>" -VMName "<name
    >" -ForgetVM
<!--NeedCopy-->
```

   - Führen Sie `Remove-ProvScheme` aus, um einen Maschinenkatalog aus der Citrix Datenbank und Ressourcen aus einem Maschinenkatalog zu entfernen. Beispiel:

```
Run Remove-ProvScheme -ProvisioningSchemeName "<name>" -
    ForgetVM
<!--NeedCopy-->
```

5. Vergewissern Sie sich, dass die VM aus Delivery Controller, nicht aber dem Hypervisor entfernt wurde.

   a) Führen Sie `Get-ProvVM -ProvisioningSchemeName "<name>"-VMName "<name>"` aus. Es darf nichts zurückgegeben werden.

   b) Rufen Sie die AWS-EC2-Konsole auf. Die VMs müssten angezeigt werden, die Tags sind jetzt jedoch entfernt. Tags aus den folgenden Ressourcen wurden entfernt:

      - Virtuelle Maschine
      - Stammdatenträger-Volume
      - Identitätsdatenträger-Volume
      - Netzwerkkarte

6. Wenn Sie den Maschinenkatalog entfernen, vergewissern Sie sich, dass der Katalog vom Delivery Controller entfernt wurde.

   a) Führen Sie `Get-ProvScheme -ProvisioningSchemeName "forgetvmdemo"` aus. Dies muss einen Fehler zurückgeben.

   b) Vergewissern Sie sich in der AWS-EC2-Konsole, dass die folgenden Ressourcen entfernt wurden.

      - Stammdatenträgerimage (AMI)
      - Startvorlage
      - Snapshot von AMI oder Stammdatenträger

### Von MCS erstellte Ressourcen identifizieren

Nachfolgend werden die Tags aufgeführt, die MCS den Ressourcen hinzufügt. Die Tags werden in der Tabelle als in der Form “Schlüssel”: “Wert”dargestellt.

| Ressourcenname | Tag |
|---|---|
| ID-Datenträger | “Name”: “VMName_IdentityDisk”<br>“XdConfig”: “XdProvisioned=true”<br>“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |
| Image | “XdConfig”: “XdProvisioned=true” |

| Ressourcenname | Tag |
| --- | --- |
| Netzwerkkarte | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”<br>“Description”: “XD NIC”<br>“XdConfig”: “XdProvisioned=true” |
| OS-Datenträger | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”<br>“Name”: “VMName_rootDisk”<br>“XdConfig”: “XdProvisioned=True” |
| Vorbereitungs-VM | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”<br>[Wenn AwsCaptureInstanceProperties = true]<br>“Citrix Resource”: “”<br>[Wenn AwsCaptureInstanceProperties = true und AwsOperationalResourcesTagging = true]<br>“CitrixOperationalResource”: “”<br>“Name”: “Preparation - CatalogName - xxxxxxxxxx”<br>“XdConfig”: “XdProvisioned=true” |
| Veröffentlichter Snapshot | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”<br>[Wenn AwsCaptureInstanceProperties = true]<br>“Citrix Resource”: “”<br>[Wenn AwsCaptureInstanceProperties = true und AwsOperationalResourcesTagging = true]<br>“CitrixOperationalResource”: “”<br>“XdConfig”: “XdProvisioned=true” |
| Vorlage | Wenn kein Snapshot für Volumeworker-AMI, dann “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxxxxxx”<br>[Wenn AwsCaptureInstanceProperties = true]<br>“XdConfig”: “XdProvisioned=true”<br>[Wenn AwsCaptureInstanceProperties = true]<br>“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”<br>[Wenn AwsCaptureInstanceProperties = true]<br>“CitrixResource”: “” |

| Ressourcenname | Tag |
| --- | --- |
| VM im Katalog | [Wenn AwsCaptureInstanceProperties = true und AwsOperationalResourcesTagging = true] “CitrixOperationalResource”: “” “XdConfig”: “XdProvisioned=true” “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” [Wenn AwsCaptureInstanceProperties = true] “CitrixResource”: “” [Wenn AwsCaptureInstanceProperties = true] “aws:ec2launchtemplate:id”:”lt-xxxx” [Wenn AwsCaptureInstanceProperties = true] “aws:ec2launchtemplate:version”: “n” [Wenn AwsCaptureInstanceProperties = true und AwsOperationalResourcesTagging = true] “CitrixOperationalResource”: “” |
| Volumeworker-AMI | “XdConfig”: “XdProvisioned=true” |
| Volumeworker-Bootstrapper | “Name”: “XenDesktop Temp” “XdConfig”: “XdProvisioned=true” “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” [Wenn AwsCaptureInstanceProperties = true und AwsOperationalResourcesTagging = true] “CitrixVolumeWorkerBootstrapper”: “” |
| Volumeworker-Instanz | “Name”: “Citrix.XD.Volumeworker-xxxx-xx-xx-xx-xxxx” “XdConfig”: “XdProvisioned=true” |

## Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Verbindung zu AWS
- Maschinenkataloge erstellen
- AWS-Katalog erstellen
- Maschinenkataloge verwalten

# XenServer-Katalog verwalten

June 27, 2024

Unter Maschinenkataloge verwalten werden die Assistenten zum Verwalten eines Maschinenkatalogs beschrieben. Die folgenden Informationen beziehen sich speziell auf XenServer-Virtualisierungsumgebungen.

> **Hinweis:**
>
> Sie müssen einen XenServer-Katalog erstellt haben, bevor Sie ihn verwalten können. Weitere Informationen finden Sie unter XenServer-Katalog erstellen.

## Von MCS erstellte Ressourcen identifizieren

Nachfolgend werden die Tags aufgeführt, die MCS den Ressourcen hinzufügt. Die Tags werden in der Tabelle als in der Form "Schlüssel": "Wert"dargestellt.

| Ressourcenname | Tag |
|---|---|
| Veröffentlichter Basisdatenträger und zugehörige Kopie in jedem Netzwerk oder lokalen Speicher | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| ID-Datenträger | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| OS-Datenträger | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| Vorbereitungs-VM | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| VM im Katalog | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| WBC-Datenträger | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |

## Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Verbindung zu XenServer
- Maschinenkataloge erstellen
- XenServer-Katalog erstellen

- Maschinenkataloge verwalten

## Google Cloud Platform -Katalog verwalten

June 27, 2024

Unter Maschinenkataloge verwalten werden die Assistenten zum Verwalten eines Maschinenkatalogs beschrieben. Die folgenden Informationen beziehen sich speziell auf Google-Cloudumgebungen.

> **Hinweis:**
>
> Sie müssen einen Google Cloud Platform-Katalog erstellt haben, bevor Sie ihn verwalten können. Weitere Informationen finden Sie unter Google Cloud Platform-Katalog erstellen.

### Verwalten von Maschinenkatalogen

Informationen zum Hinzufügen von Maschinen zu einem Katalog, zum Aktualisieren von Maschinen und zum Rollback eines Updates finden Sie unter Verwalten von Maschinenkatalogen.

### Energieverwaltung

Citrix DaaS ermöglicht die Energieverwaltung von Google Cloud-Maschinen. Mit dem Knoten **Suchen** im linken Bereich finden Sie die Maschine, für die Sie eine Energieverwaltung festlegen möchten. Folgende Energieaktionen stehen zur Verfügung:

- Löschen
- Starten
- Neu starten
- Neustart erzwingen
- Herunterfahren
- Herunterfahren erzwingen
- Zu Bereitstellungsgruppe hinzufügen
- Tags verwalten
- Wartungsmodus einschalten

Sie können die Energieverwaltung für Google Cloud-Maschinen auch mit Autoscale aktivieren. Fügen Sie hierfür die Google Cloud-Maschinen einer Bereitstellungsgruppe hinzu und aktivieren Sie Autoscale für diese Bereitstellungsgruppe. Weitere Hinweise zu Autoscale finden Sie unter Autoscale.

### Bereitgestellte Maschinen mit PowerShell aktualisieren

Mit dem Befehl `Set-ProvScheme` ändern Sie das Provisioningschema. Dies wirkt sich jedoch nicht auf vorhandene Maschinen aus. Mit dem PowerShell-Befehl `Set-ProvVMUpdateTimeWindow` können Sie jetzt das aktuelle Provisioningschema auf eine oder mehrere persistente oder nicht persistente Maschine(n) anwenden. Die derzeit in GCP von diesem Feature unterstützte aktualisierte Eigenschaft ist das Maschinenprofil.

Sie können Folgendes aktualisieren:

- Eine einzelne VM
- Eine Liste bestimmter VMs oder alle VMs, die mit der ID eines Provisioningschemas verknüpft sind.
- Eine Liste bestimmter VMs oder alle VMs, die mit dem Namen eines Provisioningschemas verknüpft sind.

Schrittfolge zum Aktualisieren der vorhandenen VMs:

1. Prüfen Sie die Konfiguration der vorhandenen Maschinen. Beispiel:

```
Get-ProvScheme | select ProvisioningSchemeName,
    ProvisioningSchemeVersion
<!--NeedCopy-->
```

2. Aktualisieren Sie das Provisioningschema. Beispiel:

```
`Set-ProvScheme  – ProvisioningSchemeName "my-catalog"  –
    MachineProfile "XDHyp:\HostingUnits<hosting-unit>\
    machineprofileinstance.vm"
<!--NeedCopy-->
```

3. Überprüfen Sie, ob die aktuelle Eigenschaft der VM mit dem aktuellen Provisioningschema übereinstimmt und ob eine Aktualisierungsaktion auf der VM aussteht. Beispiel:

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
    ProvisioningSchemeVersion
<!--NeedCopy-->
```

   Sie können auch Maschinen einer bestimmten Version finden. Beispiel:

```
Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select
    VMName, ProvisioningSchemeVersion
<!--NeedCopy-->
```

4. Aktualisieren Sie vorhandene Maschinen.

   - Gehen Sie zum Aktualisieren aller vorhandenen Maschinen folgendermaßen vor:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -StartsNow -DurationInMinutes -1
```

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

- Zum Aktualisieren einer Liste bestimmter Maschinen:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes
   -1
<!--NeedCopy-->
```

- Zum Aktualisieren von Maschinen basierend auf der Ausgabe von `Get-ProvVM`:

```
Get-ProvVM -ProvisioningSchemeName "my-catalog" | Set-
   ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
   -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

5. Suchen Sie Maschinen mit einem geplanten Update. Beispiel:

```
Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName
   , ProvisioningSchemeUpdateAfter
<!--NeedCopy-->
```

6. Starten Sie die Maschinen neu. Beim nächsten Einschalten werden Eigenschaftsänderungen auf die vorhandenen Maschinen angewendet. Sie können den aktualisierten Status mit dem folgenden Befehl überprüfen:

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
   ProvisioningSchemeVersion
<!--NeedCopy-->
```

### Datenträgerbezogene benutzerdefinierte Eigenschaften eines Katalogs ändern

Sie können die folgenden datenträgerbezogenen benutzerdefinierten Eigenschaften eines Katalogs und der VMs des Katalogs ändern:

- `PersistOSDisk`
- `PersistWBC`
- `StorageType`
- `IdentityDiskStorageType`
- `WbcDiskStorageType`

> **Hinweis:**
>
> - Die Eigenschaft `StorageType` ist für den OS-Datenträger vorgesehen.
> - Die Eigenschaft `PersistOsDisk` kann nur für nicht persistente Kataloge mit aktiviertem Zurückschreibcache festgelegt werden

Diese Implementierung hilft Ihnen, auch nach der Erstellung eines Katalogs verschiedene Speichertypen für verschiedene Datenträger auszuwählen und so den Preisen für die verschiedenen Speichertypen Rechnung zu tragen.

Verwenden Sie dazu die PowerShell-Befehle `Set-ProvScheme` und `Set-ProvVMUpdateTimeWindow`:

1. Öffnen Sie ein **PowerShell**-Fenster.
2. Führen Sie `asnp citrix*` aus.
3. Führen Sie `Get-ProvVM -VMName <VM name>` aus, um die benutzerdefinierten Eigenschaften abzurufen.
4. Ändern Sie die Zeichenfolge der benutzerdefinierten Eigenschaften:
   a) Kopieren Sie die benutzerdefinierten Eigenschaften in einen Editor und ändern Sie die benutzerdefinierten Eigenschaften.
   b) Fügen Sie im **PowerShell-Fenster** die geänderte Zeichenfolge für "Custom Properties" aus dem Editor ein, und weisen Sie ihr eine Variable zu. Beispiel:

```
$cp =  '<CustomProperties xmlns=http://schemas.citrix.com
   /2014/xd/machinecreation xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance">
<Property xsi:type="StringProperty" Name="CatalogZones" Value
   ="" />
<Property xsi:type="StringProperty" Name="PersistWBC" Value="
   true" />
<Property xsi:type="StringProperty" Name="PersistOSDisk" Value
   ="true" />
<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
   Value="pd-standard" />
<Property xsi:type="StringProperty" Name="StorageType" Value="
   pd-standard" />
</CustomProperties>'
<!--NeedCopy-->
```

5. Aktualisieren Sie den bestehenden Katalog. Beispiel:

```
Set-ProvScheme -ProvisioningSchemeName <yourCatalogName> -
   CustomProperties $cp
<!--NeedCopy-->
```

6. Aktualisieren Sie die vorhandenen VMs. Beispiel:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -
   VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

7. Starten Sie die VMs neu. Beim nächsten Einschalten werden Änderungen benutzerdefinierter Eigenschaften auf die vorhandenen Maschinen angewendet.

### Schutz vor versehentlichem Löschen von Maschinen

Citrix DaaS ermöglicht den Schutz von MCS-Ressourcen in Google Cloud vor versehentlichem Löschen. Konfigurieren Sie die bereitgestellte VM, indem Sie das Flag `deletionProtection` auf TRUE setzen.

Standardmäßig werden mit MCS oder dem Google Cloud-Plug-In bereitgestellte VMs mit aktiviertem InstanceProtection erstellt. Die Implementierung gilt für persistente und nicht persistente Kataloge. Nicht persistente Kataloge werden aktualisiert, wenn die Instanzen anhand der Vorlage neu erstellt werden. Für bestehende persistente Maschinen können Sie das Flag in der Google Cloud-Konsole festlegen. Weitere Informationen zum Festlegen des Flags finden Sie in der Google-Dokumentation. Neue Maschinen, die zu persistenten Katalogen hinzugefügt wurden, werden mit aktiviertem Flag `deletionProtection` erstellt

Der Versuch, eine VM-Instanz, für die das Flag `deletionProtection` festgelegt ist, zu löschen, schlägt fehl. Wenn Sie jedoch die Berechtigung `compute.instances.setDeletionProtection` oder die IAM-Rolle **Compute-Administrator** haben, können Sie das Flag zurücksetzen, damit die Ressource gelöscht werden kann.

### Von MCS erstellte Ressourcen identifizieren

Nachfolgend werden die Tags aufgeführt, die MCS den Ressourcen hinzufügt. Die Tags werden in der Tabelle als in der Form “Schlüssel”: “Wert”dargestellt.

| Ressourcenname | Tag |
|---|---|
| ID-Datenträger | “CitrixResource”: “internal” |
| Image | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”<br>“CitrixResource”: “internal” |
| OS-Datenträger | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”<br>“CitrixResource”: “internal” |
| Vorbereitungs-VM | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”<br>“CitrixResource”: “internal” |
| Veröffentlichter Snapshot | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”<br>“CitrixResource”: “internal” |
| Speicherbucket | “Citrixresource”: “internal” |

| Ressourcenname | Tag |
| --- | --- |
| Vorlage | “CitrixResource”: “internal”<br>“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |
| VM im Katalog | “CitrixResource”: “internal”<br>“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”. Das Plug-In fügt auch dieses Tag für von MCS bereitgestellte VMs hinzu: “citrix-provisioning-scheme-id”: “provSchemeId”. Sie können es verwenden, um in der GCP-Konsole nach Katalog zu filtern. |
| WBC-Datenträger | “CitrixResource”: “internal”<br>CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |

> **Hinweis:**
>
> Eine VM ist im Citrix-Bestand nicht sichtbar, wenn ein **CitrixResource**-Tag hinzugefügt wird, um sie als eine von MCS erstellte Ressource zu identifizieren. Sie können das Tag entfernen oder umbenennen, um sie sichtbar zu machen.

### Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Verbindung zu Google-Cloudumgebungen
- Maschinenkataloge erstellen
- Google Cloud Platform-Katalog erstellen
- Maschinenkataloge verwalten

## Einen HPE Moonshot-Katalog verwalten

June 27, 2024

Unter Maschinenkataloge verwalten werden die Assistenten zum Verwalten eines Maschinenkatalogs beschrieben. Die folgenden Informationen beziehen sich speziell auf HPE Moonshot-Kataloge.

> **Hinweis:**
>
> Sie müssen einen HPE Moonshot-Katalog erstellt haben, bevor Sie ihn verwalten können.

### Energieverwaltung

Mit Citrix Virtual Apps and Desktops können Sie die Energieverwaltung von HPE Moonshot-Computern durchführen. Mit dem Knoten **Suchen** im Navigationsbereich finden Sie die Maschine, für die Sie eine Energieverwaltung festlegen möchten. Folgende Energieaktionen stehen zur Verfügung:

- Starten
- Herunterfahren
- Herunterfahren erzwingen
- Neu starten
- Zurücksetzen

> **Hinweis:**
>
> Die Energieaktionen **Anhalten** und **Fortsetzen** werden nicht unterstützt.

### Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Verbindung zu HPE Moonshot
- Maschinenkataloge erstellen
- HPE Moonshot-Maschinenkatalog erstellen
- Maschinenkataloge verwalten

## Microsoft Azure-Katalog verwalten

June 27, 2024

> **Hinweis:**
>
> Seit Juli 2023 hat Microsoft Azure Active Directory (Azure AD) in Microsoft Entra ID umbenannt. In diesem Dokument bezieht sich jeder Verweis auf Azure Active Directory, Azure AD oder AAD jetzt auf Microsoft Entra ID.

Unter Maschinenkataloge verwalten werden die Assistenten zum Verwalten eines Maschinenkatalogs beschrieben. Die folgenden Informationen beziehen sich speziell auf Microsoft Azure Resource Manager-Cloudumgebungen.

> **Hinweis:**
>
> Sie müssen einen Microsoft Azure-Katalog erstellt haben, bevor Sie ihn verwalten können. Siehe Microsoft Azure-Katalog erstellen.

### Speichertyps beim Herunterfahren einer VM zu einer niedrigeren Ebene ändern

Sie können Speicherkosten sparen, indem Sie den Speichertyp eines verwalteten Datenträgers auf eine niedrigere Ebene umstellen, wenn Sie eine VM herunterfahren. Verwenden Sie dazu die benutzerdefinierte Eigenschaft `StorageTypeAtShutdown`.

Der Speichertyp des Datenträgers ändert sich in eine niedrigere Ebene (wie in der benutzerdefinierten Eigenschaft `StorageTypeAtShutdown` angegeben), wenn Sie die VM herunterfahren. Nach dem Einschalten der VM ändert sich der Speichertyp in den ursprünglichen Speichertyp zurück (wie in der benutzerdefinierten Eigenschaft `StorageType` oder `WBCDiskStorageType` angegeben).

> **Wichtig:**
>
> Der Datenträger ist erst vorhanden, wenn die VM mindestens einmal eingeschaltet wurde. Daher können Sie den Speichertyp nicht ändern, wenn Sie die VM zum ersten Mal einschalten.

#### Anforderungen

- Gilt für einen verwalteten Datenträger. Dies bedeutet, dass Sie die benutzerdefinierte Eigenschaft `UseManagedDisks` auf "true"festlegen.
- Gilt für einen persistenten und nicht persistenten Katalog mit einem persistenten OS-Datenträger. Dies bedeutet, dass Sie die benutzerdefinierte Eigenschaft `persistOsDisk` auf "true"festlegen.
- Gilt für einen nicht persistenten Katalog mit einem persistenten WBC-Datenträger. Dies bedeutet, dass Sie die benutzerdefinierte Eigenschaft `persistWBC` auf "true"festlegen.

#### Einschränkung

- Gemäß Vorgaben von Microsoft können Sie den Datenträgertyp nur zweimal pro Tag ändern. Siehe Microsoft-Dokumentation. Gemäß Citrix erfolgt das `StorageType`-Update immer dann, wenn eine Aktion zum Starten oder Aufheben der Zuordnung für die VM erfolgt. Beschränken Sie daher die Anzahl der Energieaktionen pro VM auf zwei pro Tag. Beispiel: eine Energieaktion morgens zum VM-Start und eine abends, um die Zuordnung der VM aufzuheben.

**Speichertyp auf eine niedrigere Ebene ändern**

Bevor Sie mit den Schritten fortfahren, lesen Sie die Abschnitte Anforderungen und Einschränkungen.

1. Fügen Sie die benutzerdefinierte Eigenschaft `StorageTypeAtShutdown` hinzu, legen Sie den Wert auf Standard_LRS (HDD) fest und erstellen Sie einen Katalog mit `New-ProvScheme`. Informationen zum Erstellen eines Katalogs mit PowerShell finden Sie unter https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

   > **Hinweis:**
   >
   > Wenn `StorageTypeAtShutdown` einen anderen Wert als leer hat oder Standard_LRS (HDD) ist, schlägt der Vorgang fehl.

   Beispiel für das Festlegen benutzerdefinierter Eigenschaften beim Erstellen eines persistenten Katalogs:

```
$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="StorageType" Value="Premium_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="Windows_Client" />
<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />
<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />
<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown" Value="Standard_LRS" />
</CustomProperties>'
<!--NeedCopy-->
```

   Beispiel für das Festlegen benutzerdefinierter Eigenschaften beim Erstellen eines nicht persistenten Katalogs:

```
$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="StorageType" Value="Premium_LRS" />
<Property xsi:type="StringProperty" Name="WbcDiskStorageType" Value="Standard_SSD_LRS" />
```

```
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="Windows_Client" />
<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />
<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />
<Property xsi:type="BooleanProperty" Name="persistWBC" Value=true />
<Property xsi:type="BooleanProperty" Name="persistOsDisk" Value=true />
<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown" Value="Standard_LRS" />
</CustomProperties>'
<!--NeedCopy-->
```

> **Hinweis:**
>
> Wenn Sie ein Maschinenprofil verwenden, hat die benutzerdefinierte Eigenschaft Vorrang vor der in `MachineProfile` definierten Eigenschaft.

2. Fahren Sie die VM herunter und überprüfen Sie den Speichertyp der VM im Azure-Portal. Der Speichertyp des Datenträgers ändert sich in eine niedrigere Ebene, wie in der benutzerdefinierten Eigenschaft `StorageTypeAtShutdown` angegeben.
3. Schalten Sie die VM ein. Der Speichertyp des Datenträgers ändert sich zurück zu dem aufgeführten Speichertyp:
   - Benutzerdefinierte Eigenschaft `StorageType` für OS-Datenträger
   - Benutzerdefinierte Eigenschaft `WBCDiskStorageType` für WBC-Datenträger, nur wenn Sie sie in `CustomProperties` angeben. Andernfalls ändert er sich zurück zum unter `StorageType` angegebenen Speichertyp.

#### `StorageTypeAtShutdown` auf einen vorhandenen Katalog anwenden

Bevor Sie mit den Schritten fortfahren, lesen Sie die Abschnitte Anforderungen und Einschränkungen.

Verwenden Sie `Set-ProvScheme`, um eine VM zu einem vorhandenen Katalog hinzuzufügen. Das Feature gilt für neue VMs, die nach dem Ausführen von `Set-ProvScheme` hinzugefügt wurden. Die vorhandenen Maschinen sind nicht betroffen.

Beispiel für das Festlegen benutzerdefinierter Eigenschaften beim Hinzufügen einer VM zu einem vorhandenen Katalog:

```
$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="StorageType" Value="Premium_LRS" />
<Property xsi:type="StringProperty" Name="WbcDiskStorageType" Value="Standard_SSD_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="Windows_Client" />
<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />
<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />
<Property xsi:type="BooleanProperty" Name="persistWBC" Value=true />
<Property xsi:type="BooleanProperty" Name="persistOsDisk" Value=true />
<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown" Value="Standard_LRS" />
</CustomProperties>'

$ProvScheme = Get-Provscheme -ProvisioningSchemeName $CatalogName

Set-ProvScheme -ProvisioningSchemeName $ProvScheme.ProvisioningSchemeName -CustomProperties $customProperties
<!--NeedCopy-->
```

#### Speichertyp vorhandener VMs beim Herunterfahren in niedrigere Ebene ändern

Bevor Sie mit den Schritten fortfahren, lesen Sie die Abschnitte Anforderungen und Einschränkungen.

Sie können Speicherkosten sparen, indem Sie den Speichertyp vorhandener VMs beim Herunterfahren der VMs in eine niedrigere Ebene ändern. Verwenden Sie dazu die benutzerdefinierte Eigenschaft `StorageTypeAtShutdown`.

Führen Sie folgende Schritte aus, um den Speichertyp vorhandener Maschinen in einem Katalog beim Herunterfahren der VMs in eine niedrigere Ebene zu ändern:

1. Öffnen Sie ein PowerShell-Fenster.
2. Führen Sie `asnp citrix*` aus, um die Citrix-spezifischen PowerShell-Module zu laden.
3. Führen Sie `Get-Provscheme -ProvisioningSchemeName $CatalogName` aus.
4. Ändern Sie die Zeichenfolge der benutzerdefinierten Eigenschaften.

```
$customProperties = '<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown" Value="Standard_LRS" />
</CustomProperties>'
<!--NeedCopy-->
```

5. Aktualisieren Sie das Provisioningschema des vorhandenen Katalogs. Das Update gilt für neue VMs, die nach dem Ausführen von `Set-ProvScheme` hinzugefügt wurden.

```
Set-ProvScheme -ProvisioningSchemeName $CatalogName -
    CustomProperties $customProperties
<!--NeedCopy-->
```

6. Aktualisieren Sie die vorhandenen VMs, um `StorageTypeAtShutdown` zu aktivieren.

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName $CatalogName -
    StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

7. Beim nächsten Einschalten der Maschinen wird die Eigenschaft `StorageTypeAtShutdown` der Maschinen aktualisiert. Der Speichertyp ändert sich beim nächsten Herunterfahren.

8. Führen Sie den folgenden Befehl aus, um den Wert `StorageTypeAtShutdown` für jede VM in einem Katalog anzuzeigen:

```
Get-ProvVM -ProvisioningSchemeName <catalog-name> | foreach {
  $vmName = $_.VMName; $storageTypeAtShutdown = ($_.CustomVmData |
       ConvertFrom-Json).StorageTypeAtShutdown.
      DiskStorageAccountType; return New-Object psobject -Property
      @{
  "VMName" = $vmName; "StorageTypeAtShutdown" =
      $storageTypeAtShutdown  }
   }

<!--NeedCopy-->
```

### Aktualisieren bereitgestellter Maschinen auf das aktuelle Provisioningschema

Mit dem Befehl `Set-ProvScheme` ändern Sie das Provisioningschema. Dies wirkt sich jedoch nicht auf vorhandene Maschinen aus. Mit dem PowerShell-Befehl `Set-ProvVMUpdateTimeWindow` können Sie das aktuelle Provisioningschema auf eine oder mehrere persistente oder nicht persistente Maschine(n) anwenden. Sie können auch ein Zeitfenster für die Konfigurationsupdates der vorhandenen, per MCS bereitgestellten Maschinen festlegen. Während dieses Zeitfensters wird dann bei jedem Einschalten oder Neustart ein geplantes Update des Provisioningschemas auf eine Maschine angewendet. Derzeit können Sie in Azure `ServiceOffering`, `MachineProfile` und die folgenden benutzerdefinierten Eigenschaften aktualisieren:

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`
- `LicenseType`
- `DedicatedHostGroupId`

- `PersistWBC`
- `PersistOsDisk`
- `PersistVm`

> **Hinweis:**
>
> - Sie können nur die benutzerdefinierten Eigenschaften `StorageType`, `WBCDiskStorageType` und `IdentityDiskStorageType` eines Katalogs mit verwaltetem Datenträger in Azure-Umgebungen aktualisieren.
> - Wenn Sie `Set-ProvVMUpdateTimeWindow` zweimal ausführen, wird der neueste Befehl wirksam.

Sie können Folgendes aktualisieren:

- Eine einzelne VM
- Eine Liste bestimmter VMs oder alle VMs, die mit der ID eines Provisioningschemas verknüpft sind.
- Eine Liste bestimmter VMs oder alle VMs, die mit dem Namen eines Provisioningschemas (Maschinenkatalogname) verknüpft sind.

Nachdem Sie die folgenden Änderungen am Provisioningschema vorgenommen haben, wird die VM-Instanz für persistente Kataloge in Azure neu erstellt:

- Ändern Sie `MachineProfile`.
- Entfernen Sie `LicenseType`.
- Entfernen Sie `DedicatedHostGroupId`.

> **Hinweis:**
>
> Der Betriebssystemdatenträger vorhandener Maschinen samt Daten bleibt unverändert, und es wird eine neue VM mit dem Datenträger verbunden.

Bevor Sie die vorhandenen VMs aktualisieren:

1. Prüfen Sie die Konfiguration der vorhandenen Maschinen. Beispiel:

```
Get-ProvScheme | select ProvisioningSchemeName,
    ProvisioningSchemeVersion
<!--NeedCopy-->
```

2. Aktualisieren Sie das Provisioningschema. Beispiel:

   - VM zur Eingabe des Maschinenprofils verwenden:

```
Set-ProvScheme -ProvisioningSchemeName "my-catalog" -
    MachineProfile "XDHyp:\HostingUnits<hosting-unit>\
    machineprofile.folder<resource-group>.resourcegroup<
    virtual-machine>.vm"
```

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

- Vorlagenspezifikation zur Eingabe des Maschinenprofils verwenden:

```
Set-ProvScheme -ProvisioningSchemeName "my-catalog"
-MachineProfile "XDHyp:\HostingUnits<hosting-unit>\
   machineprofile.folder<resource-group>.resourcegroup<
   template-spec>.templatespec<template-spec-version>.
   templatespecversion"
-ServiceOffering "XDHyp:\HostingUnits<hosting-unit>\
   serviceoffering.folder<service-offering>.serviceoffering"
<!--NeedCopy-->
```

- Nur Dienstangebot verwenden:

```
Set-ProvScheme -ProvisioningSchemeName "my-catalog" -
   ServiceOffering "XDHyp:\HostingUnits<hosting-unit>\
   serviceoffering.folder<service-offering>.serviceoffering"
<!--NeedCopy-->
```

3. Überprüfen Sie, ob die aktuelle Eigenschaft der VM mit dem aktuellen Provisioningschema übereinstimmt und ob eine Aktualisierungsaktion auf der VM aussteht. Beispiel:

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
   ProvisioningSchemeVersion
<!--NeedCopy-->
```

Sie können auch Maschinen einer bestimmten Version finden. Beispiel:

```
Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select
   VMName, ProvisioningSchemeVersion
<!--NeedCopy-->
```

Um Updates für bestehende Maschinen anzufordern, die beim nächsten Neustart angewendet werden sollen, gehen Sie wie folgt vor:

1. Führen Sie die folgenden Befehle aus, um bestehende Maschinen zu aktualisieren und die Updates beim nächsten Neustart anwenden zu lassen.

- Aktualisieren Sie alle vorhandenen Maschinen. Beispiel:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

- Aktualisieren Sie eine Liste bestimmter Maschinen. Beispiel:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes
   -1
<!--NeedCopy-->
```

- Aktualisieren Sie Maschinen basierend auf der Ausgabe von Get-ProvVM. Beispiel:

```
Get-ProvVM -ProvisioningSchemeName "my-catalog" | Set-
    ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

> **Hinweis:**
>
> - `StartsNow` gibt an, dass die geplante Startzeit die aktuelle Uhrzeit ist.
> - `DurationInMinutes` mit einer negativen Zahl (z. B. -1) gibt an, dass es im Zeitfenster des Zeitplans keine Obergrenze gibt.

2. Suchen Sie Maschinen mit einem geplanten Update. Beispiel:

```
Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName
    , ProvisioningSchemeUpdateAfter
<!--NeedCopy-->
```

3. Starten Sie die Maschinen neu. Beim nächsten Einschalten werden Eigenschaftsänderungen auf die vorhandenen Maschinen angewendet. Sie können den aktualisierten Status mit dem folgenden Befehl überprüfen. Beispiel:

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
    ProvisioningSchemeVersion
<!--NeedCopy-->
```

Zum Planen des Updates einer VM auf die neuesten Provisioningeinstellungen beim nächsten Start im geplanten Zeitfenster:

1. Führen Sie die folgenden Befehle aus:

   - Update mit der aktuellen Uhrzeit als Startzeit planen:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -VMName vm1 -StartsNow -DurationInMinutes 120
<!--NeedCopy-->
```

   - Update an einem Wochenende planen:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName “ my-
    catalog “ -VMName “ vm1 ” -StartTimeInUTC “ 10/15/2022
    9:00am ” -DurationInMinutes (New – TimeSpan – Days 2).
    TotalMinutes
<!--NeedCopy-->
```

> **Hinweis:**
>
> - `VMName` ist optional. Wenn nicht angegeben, wird das Update für den gesamten Kat-

> alog geplant.
> - Verwenden Sie statt `StartTimeInUTC` den Befehl `StartsNow`, um anzugeben, dass die geplante Startzeit der aktuellen Uhrzeit entspricht.
> - `DurationInMinutes` ist optional. Der Standardwert ist 120 Minuten. Eine negative Zahl (z. B. -1) gibt an, dass es im Zeitfenster des Zeitplans keine Obergrenze gibt.

2. Überprüfen Sie den Updatestatus.

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
   ProvisioningSchemeUpdateUntil, ProvisioningSchemeVersion
<!--NeedCopy-->
```

3. Schalten Sie die VM ein. Wenn Sie die Maschine nach dem geplanten Zeitfenster einschalten, wird das Konfigurationsupdate nicht durchgeführt. Wenn Sie die Maschine innerhalb des geplanten Zeitfensters einschalten,

   - Wenn die Maschine ausgeschaltet ist und
     - Sie die Maschine nicht einschalten, wird das Konfigurationsupdate nicht angewendet.
     - Sie die Maschine einschalten, wird das Konfigurationsupdate angewendet.
   - Wenn die Maschine eingeschaltet ist und
     - Sie die Maschine nicht neu starten, wird das Konfigurationsupdate nicht angewendet.
     - Sie die Maschine neu starten, wird das Konfigurationsupdate angewendet.

Konfigurationsupdate abbrechen:

Sie können ein Konfigurationsupdate auch für eine einzelne VM, mehrere VMs oder einen gesamten Katalog abbrechen. Konfigurationsupdate abbrechen:

1. Führen Sie `Clear-ProvVMUpdateTimeWindow` aus. Beispiel:

   - Das für eine einzelne VM geplante Konfigurationsupdate abbrechen:

```
Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName “ my-
   catalog “ -VMName “ vm1 ”
<!--NeedCopy-->
```

   - Das für mehrere VMs geplante Konfigurationsupdate abbrechen:

```
Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName "my-
   catalog" -VMName "vm1","vm2"
<!--NeedCopy-->
```

> **Hinweis:**
>
> Die VMs müssen aus demselben Katalog stammen.

### Eigenschaften einzelner VMs aktualisieren

Sie können die Eigenschaften einzelner VMs in einem persistenten MCS-Maschinenkatalog mithilfe des PowerShell-Befehls `Set-ProvVM` aktualisieren. Die Updates werden jedoch nicht sofort angewendet. Sie müssen das Zeitfenster zur Anwendung der Updates mit dem PowerShell-Befehl `Set-ProvVMUpdateTimeWindow` festlegen.

Mithilfe dieser Implementierung können Sie einzelne VMs effizient verwalten, ohne den gesamten Maschinenkatalog aktualisieren zu müssen. Derzeit gilt dieses Feature nur für die Azure-Umgebung.

Derzeit können Sie folgende Eigenschaften aktualisieren:

- `CustomProperties`
- `ServiceOffering`
- `MachineProfile`

Mit dem Feature ist Folgendes möglich:

- Eigenschaften einer VM aktualisieren
- Aktualisierte Eigenschaften auf einer VM nach dem Aktualisieren des Maschinenkatalogs beibehalten
- Auf eine VM angewendete Konfigurationsupdates rückgängig machen

Vor dem Aktualisieren der Eigenschaften einer VM:

1. Öffnen Sie ein **PowerShell**-Fenster.
2. Führen Sie `asnp citrix*` aus, um die Citrix-spezifischen PowerShell-Module zu laden.
3. Prüfen Sie die Konfiguration des vorhandenen Maschinenkatalogs. Beispiel:

```
Get-ProvScheme -ProvisioningSchemeName AzureCatalog
<!--NeedCopy-->
```

4. Überprüfen Sie die Konfiguration der VM, die Sie aktualisieren möchten. Beispiel:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```

#### Eigenschaften einer VM aktualisieren

Gehen Sie wie folgt vor, um die Eigenschaften einer VM zu aktualisieren:

1. Schalten Sie die VM aus, auf der Sie die Updates anwenden möchten.

2. Aktualisieren Sie die Eigenschaften der VM. Wenn Sie beispielsweise die benutzerdefinierte Eigenschaft Speichertyp (`StorageType`) der VM aktualisieren möchten, führen Sie Folgendes aus:

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1 -
    CustomProperties "...<Property Name='StorageType' Value='
    Premium_LRS' />..."
<!--NeedCopy-->
```

Sie können die Eigenschaften zweier VMs in einem Maschinenkatalog gleichzeitig aktualisieren. Beispiel:

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1 -
    CustomProperties "...<Property Name='StorageType' Value='
    Premium_LRS' />..."
<!--NeedCopy-->
```

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine2 -
    CustomProperties "...<Property Name='StorageType' Value='
    StandardSSD_LRS' />..."
<!--NeedCopy-->
```

> **Hinweis:**
>
> Die Updates werden nicht sofort angewendet.

3. Rufen Sie die Liste der zur Aktualisierung angegebenen Eigenschaften und die Konfigurationsversion ab. Beispiel:

```
Get-ProvVMConfiguration -ProvisioningSchemeName AzureCatalog -
    VMName machine1
<!--NeedCopy-->
```

Überprüfen Sie den Eigenschaftswert von `Version` und die Eigenschaften, die aktualisiert werden sollen (in diesem Fall `StorageType`).

4. Überprüfen Sie die Konfigurationsversion. Beispiel:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```

Überprüfen Sie den Wert der Eigenschaft `ProvVMConfigurationVersion`. Das Update wurde noch nicht angewendet. Die VM besitzt immer noch die alte Konfiguration.

5. Fordern Sie ein geplantes Update an. Beispiel:

```
 Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -
    StartsNow -DurationInMinutes -1
 <!--NeedCopy-->
```

Weitere Informationen zu geplanten Updates finden Sie unter Aktualisieren bereitgestellter Maschinen auf das aktuelle Provisioningschema.

> **Hinweis:**
>
> Jegliches ausstehende Provisioningschema-Update wird ebenfalls angewendet.

6. Starten Sie die VM neu. Beispiel:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
<!--NeedCopy-->
```

7. Überprüfen Sie die Konfigurationsversion. Beispiel:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```

   Überprüfen Sie den Wert der Eigenschaft `ProvVMConfigurationVersion`. Das Update wurde angewendet. Die VM hat jetzt die neue Konfiguration.

8. Um weitere Konfigurationsupdates auf der VM anzuwenden, schalten Sie die VM aus und wiederholen Sie die Schritte.

### Aktualisierte Eigenschaften auf einer VM nach dem Aktualisieren des Maschinenkatalogs beibehalten

Gehen Sie wie folgt vor, um die aktualisierten Eigenschaften einer VM beizubehalten:

1. Schalten Sie die VM aus, auf der Sie die Updates anwenden möchten.
2. Aktualisieren Sie den Maschinenkatalog. Wenn Sie beispielsweise die VM-Größe (`ServiceOffering`) und den Speichertyp (`StorageType`) ändern möchten, führen Sie Folgendes aus:

```
Set-ProvScheme -ProvisioningSchemeName AzureCatalog -
    ServiceOffering Standard_E4_v3 -CustomProperties "...<Property
    Name='StorageType' Value='StandardSSD_LRS' />..."
<!--NeedCopy-->
```

3. Rufen Sie die Konfigurationsdetails des Maschinenkatalogs ab. Beispiel:

```
Get-ProvScheme -ProvisioningSchemeName AzureCatalog
<!--NeedCopy-->
```

   `ProvisioningSchemeVersion` wird jetzt um eins erhöht. Die VM-Größe und der Speichertyp werden ebenfalls aktualisiert.

4. Aktualisieren Sie die Eigenschaften der VM. Stellen Sie der VM beispielsweise ein Maschinenprofil bereit.

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1 -
    MachineProfile "XDHyp:\HostingUnits<hosting-unit>\
    machineprofile.folder<resource-group>.resourcegroup<template-
    spec>.templatespec<template-spec-version>.templatespecversion"
<!--NeedCopy-->
```

> **Hinweis:**
>
> Die Maschinenprofileingabe hat ein Tag und eine andere VM-Größe (`ServiceOffering` ).

5. Rufen Sie die Liste der Eigenschaften ab, die die VM nach dem Zusammenführen der Konfigurationsupdates auf der VM mit den Maschinenkatalog-Updates haben wird. Beispiel:

```
Get-ProvVMConfigurationResultantSet -ProvisioningSchemeName
    AzureCatalog -VMName machine1
<!--NeedCopy-->
```

> **Hinweis:**
>
> Alle Updates der VM setzen die Updates am Maschinenkatalog außer Kraft.

6. Fordern Sie ein geplantes Update für die VM an. Beispiel:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -
    VMName machine1 -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

7. Starten Sie die VM neu. Beispiel:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
<!--NeedCopy-->
```

   Die VM behält ihre aktualisierte, aus dem Maschinenprofil abgeleitete Größe bei. Die im Maschinenprofil angegebenen Tag-Werte werden ebenfalls auf die VM angewendet. Der Speichertyp wird jedoch aus dem neuesten Provisioningschema abgeleitet.

8. Rufen Sie die Konfigurationsversion der VM ab. Beispiel:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```

   Für `ProvisioningSchemeVersion` und `ProvVMConfigurationVersion` wird jetzt die neueste Version angegeben.

#### Auf eine VM angewendete Konfigurationsupdates rückgängig machen

1. Nachdem Sie die Updates auf eine VM angewendet haben, schalten Sie die VM aus.

2. Führen Sie den folgenden Befehl aus, um die Updates zu entfernen, die auf die VM angewendet wurden. Beispiel:

```
Set-ProvVM -RevertToProvSchemeConfiguration -
    ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```

3. Fordern Sie ein geplantes Update für die VM an. Beispiel:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -
    VMName machine1 -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

4. Starten Sie die VM neu. Beispiel:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
<!--NeedCopy-->
```

5. Überprüfen Sie die Konfigurationsversion der VM. Beispiel:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```

   Der Wert für `ProvVMConfigurationVersion` gibt jetzt die Konfigurationsversion des Maschinenkatalogs wieder.

### Abrufen von Informationen für Azure-VMs, Snapshots, Betriebssystemdatenträger und Katalogimagedefinition

Sie können Informationen für eine Azure-VM anzeigen, einschließlich Betriebssystemdatenträger und -typ, Snapshot und Katalogimagedefinition. Diese Informationen werden für Ressourcen im Masterimage angezeigt, wenn ein Maschinenkatalog zugewiesen wird. Verwenden Sie diese Funktion, um entweder ein Linux- oder ein Windows-Image anzuzeigen und auszuwählen. Eine PowerShell-Eigenschaft, `TemplateIsWindowsTemplate`, wurde dem Parameter `AdditionDatafield` hinzugefügt. Dieses Feld enthält Azure-spezifische Informationen: VM-Typ, Betriebssystemdatenträger, Informationen zum Katalogimage und Informationen zum Betriebssystemtyp. Die Einstellung von `TemplateIsWindowsTemplate` auf **True** zeigt an, dass der Betriebssystemtyp Windows ist; die Einstellung von `TemplateIsWindowsTemplate` auf **False** zeigt an, dass der Betriebssystemtyp Linux ist.

> **Tipp:**
>
> Die von der PowerShell-Eigenschaft `TemplateIsWindowsTemplate` angezeigten Informationen werden von der Azure-API abgeleitet. Gelegentlich kann dieses Feld leer sein. Beispiel: Ein Snapshot von einem Datenträger enthält das Feld `TemplateIsWindowsTemplate` nicht,

> da der Betriebssystemtyp nicht aus einem Snapshot abgerufen werden kann.

Beispiel: Legen Sie den `AdditionData`-Parameter der Azure-VM für den Betriebssystemtyp Windows mit PowerShell auf **True** fest:

```
PS C:\Users\username> (get-item XDHyp:\HostingUnits\mynetwork\image.folder\username-dev-testing-rg.resourcegroup\username-dev-tsvda.vm).AdditionalData
Key Value
ServiceOfferingDescription Standard_B2ms
HardDiskSizeGB 127
ResourceGroupName FENGHUAJ-DEV-TESTING-RG
ServiceOfferingMemory 8192
ServiceOfferingCores 2
TemplateIsWindowsTemplate True
ServiceOfferingWithTemporaryDiskSizeInMb 16384
SupportedMachineGenerations Gen1,Gen2
<!--NeedCopy-->
```

### Von MCS erstellte Ressourcen identifizieren

Nachfolgend werden die Tags aufgeführt, die MCS den Ressourcen hinzufügt. Die Tags werden in der Tabelle als in der Form “Schlüssel”: “Wert”dargestellt.

| Ressourcenname | Tag |
|---|---|
| ID-Datenträger | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal” |
| Image | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal” |
| Netzwerkkarte | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal” |
| OS-Datenträger | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal” |
| Vorbereitungs-VM | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal” |

| Ressourcenname | Tag |
| --- | --- |
| Veröffentlichter Snapshot | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal” |
| Ressourcengruppe | “CitrixResource”: “Internal” CitrixSchemaVersion: 2.0 |
| Speicherkonto | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |
| | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal” |
| VM im Katalog | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal” |
| WBC-Datenträger | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal” |

> **Hinweis:**
>
> Eine VM ist im Citrix-Bestand nicht sichtbar, wenn ein **CitrixResource**-Tag hinzugefügt wird, um sie als eine von MCS erstellte Ressource zu identifizieren. Sie können das Tag entfernen oder umbenennen, um sie sichtbar zu machen.

### Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Verbindung zu Microsoft Azure
- Maschinenkataloge erstellen
- Microsoft Azure-Katalog erstellen
- Maschinenkataloge verwalten

## Microsoft System Center Virtual Machine Manager-Katalog verwalten

June 27, 2024

Unter Maschinenkataloge verwalten werden die Assistenten zum Verwalten eines Maschinenkatalogs beschrieben. Die folgenden Informationen beziehen sich speziell auf Microsoft System Center Virtual Machine Manager (VMM)-Virtualisierungsumgebungen.

> **Hinweis:**
>
> Sie müssen einen VMM-Katalog erstellt haben, bevor Sie ihn verwalten können. Siehe Microsoft System Center Virtual Machine Manager-Katalog erstellen.

### Von MCS erstellte Ressourcen identifizieren

Nachfolgend werden die Tags aufgeführt, die MCS den Ressourcen hinzufügt. Die Tags werden in der Tabelle als in der Form "Schlüssel": "Wert"dargestellt.

| Ressourcenname | Tag |
| --- | --- |
| Vorbereitungs-VM | Tagzeichenfolge: "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"<br>Benutzerdefinierte Eigenschaft: "XdConfig:" XdProvisioned=True" |
| VM im Katalog | Tagzeichenfolge: "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"<br>Benutzerdefinierte Eigenschaft: "XdConfig:" XdProvisioned=True" |

### Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Verbindung zu Microsoft System Center Virtual Machine Manager
- Maschinenkataloge erstellen
- Microsoft System Center Virtual Machine Manager-Katalog erstellen
- Maschinenkataloge verwalten

## VMware-Katalog verwalten

June 27, 2024

Unter Maschinenkataloge verwalten werden die Assistenten zum Verwalten eines Maschinenkatalogs beschrieben. Die folgenden Informationen beziehen sich speziell auf VMware-Virtualisierungsumgebungen.

> **Hinweis:**
>
> Sie müssen einen VMware-Katalog erstellt haben, bevor Sie ihn verwalten können. Siehe VMware-Katalog erstellen.

### Ordner-ID eines Maschinenkatalogs aktualisieren

Sie können die Ordner-ID eines MCS-Maschinenkatalogs aktualisieren, indem Sie `FolderId` in den benutzerdefinierten Eigenschaften des Befehls `Set-ProvScheme` angeben. Die nach dem Aktualisieren der Ordner-ID erstellten VMs werden unter dieser neuen Ordner-ID erstellt. Wenn diese Eigenschaft nicht in `CustomProperties` angegeben ist, werden VMs in dem Ordner erstellt, in dem das Masterimage ist.

Führen Sie folgende Schritte aus, um die Ordner-ID eines Maschinenkatalogs zu aktualisieren.

1. Öffnen Sie einen Webbrowser und geben Sie die URL für den **vSphere Web Client** ein.
2. Geben Sie die Anmeldeinformationen ein und klicken Sie auf **Login**.
3. Erstellen Sie einen VM-Platzierungsordner in **vSphere Web Client**.
4. Öffnen Sie ein PowerShell-Fenster.
5. Führen Sie **asnp citrix*** aus, um die Citrix-spezifischen PowerShell-Module zu laden.
6. Geben Sie `FolderID` in den `CustomProperties` von `Set-ProvScheme` an. In diesem Beispiel ist der Wert für die Ordner-ID `group-v2406`.

```
1 Set-ProvScheme -ProvisioningSchemeUid "50bb319c-2e83-4a37-9ea1-94
    f630687372" -CustomProperties "<CustomProperties xmlns=""http
    ://schemas.citrix.com/2014/xd/machinecreation"" xmlns:xsi=""
    http://www.w3.org/2001/XMLSchema-instance""><Property xsi:type=
    ""StringProperty"" Name=""FolderId"" Value=""group-v2406"" /></
    CustomProperties>"
2 <!--NeedCopy-->
```

7. Fügen Sie dem Maschinenkatalog mit Studio eine VM hinzu.
8. Überprüfen Sie die neue VM im vSphere Web Client. Die neue VM wird unter dem neuen Ordner erstellt.

#### Suchen der Ordner-ID in vSphere

Verwenden Sie den Browser für verwaltete Objekte (MOB) auf einem beliebigen ESXi- oder vCenter Server-System zum Finden der Ordner-ID der VMs.

Der Browser für verwaltete Objekte (MOB), ist eine webbasierte Serveranwendung, die in alle ESX/ESXi- und vCenter Server-Systeme integriert ist. Mit diesem vSphere-Dienstprogramm können Sie detaillierte Informationen zu Objekten wie VMs, Datenspeichern und Ressourcenpools anzeigen.

1. Öffnen Sie einen Webbrowser und geben Sie `http://x.x.x.x/mob` ein, wobei x.x.x.x die IP-Adresse des vCenter Server oder ESX/ESXi-Hosts ist. Beispiel: https://10.60.4.70/mob.
2. Klicken Sie auf der **Startseite** von MOB auf den Wert der Eigenschaft **content**.
3. Klicken Sie auf den Wert von **rootFolder**.
4. Klicken Sie auf den Wert von **childEntity**.
5. Klicken Sie auf den Wert von **vmFolder**.
6. Sie finden die Ordner-ID im Wert von **childEntity**.

## Speichermigration von VMs

Sie können den Datenträgerspeicher vorhandener VMs von einem alten Speicher in einen neuen Speicher verschieben. Während der Migration behält MCS die VM-Funktionen wie Energieverwaltung, Zurücksetzen des OS-Datenträgers usw. bei. Sie können dem Maschinenkatalog auch mithilfe des neuen Datenträgerspeichers neue VMs hinzufügen. Verwenden Sie dazu den PowerShell-Befehl `Move-ProvVMDisk`.

Derzeit können Sie nur vollständige Klone persistenter VMs migrieren.

Der neue Speicher muss die folgenden Bedingungen erfüllen:

- Er muss sich in demselben Cluster des alten Speichers befinden.
- Der Host, auf dem die VM läuft, muss Zugriff auf den alten und den neuen Datenspeicher haben.

Sie können die folgenden Aufgaben erledigen:

- Datenträgerspeicher migrieren
- Alten Speicher verwerfen

### Datenträgerspeicher migrieren

So migrieren Sie den Datenträgerspeicher:

1. Fügen Sie einer vorhandenen Hostingeinheit einen neuen Speicher hinzu. Ändern Sie den alten Speicher auf **Ersetzt**. Hierfür können Sie Web Studio oder PowerShell-Befehle verwenden.
    - Wenn Sie Web Studio verwenden, finden Sie weitere Informationen unter Speicher bearbeiten.
    - Mit PowerShell-Befehlen:

- Führen Sie `Add-Hyphostingunitstorage` aus, um den neuen Speicher zur vorhandenen Hostingeinheit hinzuzufügen.
- Führen Sie `Set-Hyphostingunitstorage` mit **Superseded** auf "True"aus, um das Erstellen neuer virtueller Maschinen im alten Speicher zu deaktivieren.

2. Schalten Sie die virtuellen Maschinen aus und den **Wartungsmodus** ein.
3. Verschieben Sie den Datenträgerspeicher der VMs in den neuen Speicher und aktualisieren Sie die Speicherinformationen. Beispiel:

```
Move-ProvVMDisk -ProvisioningSchemeName "myFullCloneProvScheme" -
    VMName ("VMware-TestVM01", "VMware-TestVM02") -DiskType OS,
    Identity -DestinationStorageId datastore1,datastore1
<!--NeedCopy-->
```

4. Rufen Sie die Aufgaben-ID der Migration ab. Beispiel:

```
,(Get-ProvVM -ProvisioningSchemeName xxxxx) | Move-ProvVMDisk -
    ProvisioningSchemeName xxxxx -DiskType OS,Identity -
    DestinationStorageId datastore1,datastore1
<!--NeedCopy-->
```

5. Überprüfen Sie den Status der Migration.

- `(Get-ProvTask -TaskID xxxxxxxxx).DiskMovedVirtualMachines`: stellt die Liste der VMs mit erfolgreicher Datenträgermigration bereit, einschließlich der VMs, die bereits auf den neuen Speicher migriert wurden.
- `(Get-ProvTask -TaskID xxxxxxxxx).DiskMoveFailedVirtualMachines` : stellt die Liste der virtuellen Maschinen bereit, bei denen die Migration fehlgeschlagen ist.
- `(Get-ProvTask -TaskID xxxxxxxxx).NotStartedVirtualMachines`: stellt die Liste der VMs bereit, deren Migration noch nicht gestartet wurde.
- `Get-ProvVM -ProvisioningSchemeName xxxxx -VMName "VMware-TestVM01`: stellt die aktualisierten VM-Eigenschaften nach der Migration bereit. Überprüfen Sie die Eigenschaften wie `StorageId`, `AssignedImage`, `BootedImage`, `IdentityDiskId`, `IdentityDiskStorage` und `LastBootTime`.

Nach der Migration der Datenträger der von MCS erstellten VMs mit Snapshot wird möglicherweise die Warnung **Konsolidierung ist erforderlich im vSphere Client** angezeigt. So konsolidieren Sie und vermeiden Datenverlust:

1. Erstellen Sie ein VMware-VM-Backup. Übertragen Sie beispielsweise alle VM-Dateien in einen anderen Ordner auf einem Datenspeicher.
2. Wenn die Warnung angezeigt wird, klicken Sie auf **Konsolidieren** und dann auf **OK**, um die Konsolidierung zu bestätigen.

#### Alten Speicher verwerfen

So verwerfen Sie den alten Speicher nach der Datenträgermigration der virtuellen Maschinen:

1. Rufen Sie die Informationen über die Basisdatenträger und die Anzahl der Maschine in jedem Datenträgerspeicher der Hostingeinheit ab. Beispiel:

   ```
   $result=Get-ProvSchemeResourceInStorage -ProvisioningSchemeName
       xxxxx
   $result
   $result.ProvResourceInStorage | Format-List -Property *
   <!--NeedCopy-->
   ```

   Nach einer erfolgreichen Migration entfernt MCS automatisch den veralteten Basisdatenträger und im alten Speicher befinden sich keine Maschinen mehr. Stellen Sie daher nach dem Ausführen des Befehls sicher, dass sich im alten Speicher keine Maschinen und kein Basisdatenträger befinden.

2. Führen Sie `Remove-Hyphostingunitstorage` aus, um den alten Speicher vollständig von der Hostingeinheit zu entfernen. Sie können Web Studio auch verwenden, um den alten Speicher zu entfernen.

### Von MCS erstellte Ressourcen identifizieren

Nachfolgend werden die Tags aufgeführt, die MCS den Ressourcen hinzufügt. Die Tags werden in der Tabelle als in der Form “Schlüssel”: “Wert”dargestellt.

| Ressourcenname | Tag |
|---|---|
| Vorbereitungs-VM | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “XdConfig:”XdProvisioned=True” |
| VM im Katalog | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “XdConfig:”XdProvisioned=True” |

### Weitere Informationen

- Verbindungen und Ressourcen erstellen und verwalten
- Verbindung zu VMware
- Maschinenkataloge erstellen
- VMware-Katalog erstellen

- Maschinenkataloge verwalten

## Energieverwaltung

June 27, 2024

Mit Citrix Virtual Apps and Desktops ist die Energieverwaltung per MCS-bereitgestellte VMs über verschiedene unterstützte Hypervisors und Clouddienste hinweg möglich. Die Energieverwaltung bietet:

- Optimale Benutzererfahrung
- Kostenmanagement und Energieeinsparung

Die verfügbaren Energieaktionen:

- Starten
- Herunterfahren
- Neu starten
- Anhalten
- Fortsetzen
- Neustart erzwingen
- Herunterfahren erzwingen

> **Hinweis:**
>
> - Bei einer nicht persistenten VM führt Abschalten und Wiedereinschalten bzw. Neustarten zum Zurücksetzen des Betriebssystemdatenträgers.
> - Energieaktionen und deren Verhalten variieren je nach Hypervisor und Cloudservice.

In diesem Artikel werden die wichtigsten Energieverwaltungsfunktionen im Zusammenhang mit bestimmten unterstützten Hypervisors behandelt.

- Energieverwaltung für AWS-VMs
- Energieverwaltung für Azure-VMs

## Energieverwaltung für AWS-VMs

June 27, 2024

Informationen zu den erforderlichen Berechtigungen finden Sie unter Erforderliche AWS-Berechtigungen.

### Ruhezustand von Instanzen

Beim Ruhezustand wird der In-Memory-Status der Instanz samt privater und elastischer IP-Adressen gespeichert, sodass Benutzer genau dort weitermachen kann, wo sie aufgehört haben.

Wenn eine Instanz in den Ruhezustand versetzt wird, schreibt sie ihren In-Memory-Status in eine Datei auf dem EBS-Stammvolume und fährt dann herunter. Ein Amazon EBS-Volume ist ein robuster Blockspeicher, den Sie an Ihre Instanzen anschließen können. Nachdem Sie ein Volume an eine Instanz angeschlossen haben, können Sie es wie eine physische Festplatte verwenden. Verschlüsseln Sie das EBS-Stammvolume der Instanz. Die Verschlüsselung gewährleistet einen angemessenen Schutz vertraulicher Daten, wenn sie aus dem Speicher in das EBS-Volume kopiert werden. Informationen zur EBS-Verschlüsselung finden Sie unter Amazon EBS encryption.

Es gelten folgende Einschränkungen für den unterstützten Ruhezustand von Instanzen:

- Instanzenspeicher (RAM) bis maximal 150 GB unterstützt
- UEFI-Startmodus wird nicht unterstützt
- Es werden nur Allzweck-SSD und Bereitgestellte IOPS-SSD als EBS-Volumetypen unterstützt.

#### VMs mit unterstütztem Ruhezustand erstellen

Erstellen von VMs mit unterstütztem Ruhezustand:

1. Erstellen Sie eine Hostverbindung. Siehe Verbindung zu AWS.
2. Starten Sie eine Instanz mit verschlüsseltem EBS-Stamm und aktivierter Eigenschaft **Stop-Hibernate**. Weitere Informationen zum Starten der Instanz, Verschlüsseln des EBS-Stammvolumes und Aktivieren des Ruhezustands finden Sie unter https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/launching-instance.html/. Verwenden Sie diese Instanz als Masterimage, um ein AMI zu erstellen.
3. Bereiten Sie das Masterimage vor:
    a) Installieren Sie einen VDA auf dem Masterimage. Citrix empfiehlt die Installation der neuesten Version, damit die neuesten Features verfügbar sind. Wird kein VDA auf dem Masterimage installiert, schlägt die Katalogerstellung fehl. Weitere Informationen zur Installation eines VDA finden Sie unter Installieren von VDAs.
    b) Fügen Sie das Masterimage der Domäne hinzu, zu der die Anwendungen und Desktops gehören. Vergewissern Sie sich, dass das Masterimage auf dem Host verfügbar ist, auf dem die Maschinen erstellt werden.
4. Erstellen Sie ein AMI aus dieser Instanz. Informationen zum Erstellen eines AMI aus einer Instanz finden Sie unter Create an AMI from an Amazon EC2 Instance.

5. Erstellen Sie mit dem Befehl `New-ProvScheme` einen Maschinenkatalog. Legen Sie die benutzerdefinierte Eigenschaft `AwsCaptureInstanceProperties` auf **True** fest. Informationen zum Aktivieren von AWS-Instanzeigenschaften in der Benutzeroberfläche "Vollständige Konfiguration"finden Sie unter Anwenden von AWS-Instanzeigenschaften und Tagging von Betriebsressourcen in der Benutzeroberfläche "Vollständige Konfiguration".

```
New-ProvScheme  -AdminAddress "xxx" -CleanOnBoot
-CustomProperties "AwsCaptureInstanceProperties,true;"
-HostingUnitName "xxx" -IdentityPoolName $catalog_name -
   InitialBatchSizeHint 1
-MasterImageVM "xyz.template" -NetworkMapping @{
 "0"="XDHyp:\HostingUnits\MyConn\us-east-2a.availabilityzone
    \10.0.0.0``/24 (vpc-0f1771e45671aedcd).network" }

-ProvisioningSchemeName $catalog_name
-RunAsynchronously -Scope @() -SecurityGroup @("xxx") -
   ServiceOffering "xxx"
<!--NeedCopy-->
```

   Hinweise zum Erstellen eines Maschinenkatalogs mithilfe von PowerShell-Befehlen finden Sie unter https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/.

VMs, die in den Ruhezustand versetzt werden können, werden erstellt, wenn Folgendes gilt:

- Sie wählen ein AMI aus, das aus einem Masterimage mit aktivierter Eigenschaft **Stop-Hibernate** erstellt wurde.
- Die Master-VM ist domänengebunden und hat einen installierten VDA.
- Sie wählen die richtige VM-Größe (Dienstangebot), die den Ruhezustand bewältigen kann.

Der Befehl **New-ProvScheme** schlägt fehl und es wird eine Fehlermeldung angezeigt, wenn Folgendes gilt:

- Die Ruhezustandsfunktion ist für die Master-VM aktiviert, das Dienstangebot kann den Ruhezustand jedoch nicht verarbeiten.
- Die Master-VM ist nicht domänengebunden und hat keinen installierten VDA.

#### Ruhezustandsstatus von Dienstangeboten und AMI

Führen Sie die folgenden Befehle aus, um den Ruhezustandsstatus von Dienstangeboten und AMI (Vorlagen) abzurufen:

- `Get-HypConfigurationObjectForItem 'XDHyp:\HostingUnits\MyConn\WIN2016-ADDC-2021.09.10.145334-a1968709-10c4-47d5-9642-21e743159a7b (ami-0e6c5b33a52d2a6b6).template'`
- `Get-HypConfigurationObjectForItem 'XDHyp:\HostingUnits\MyConn\R6i Sixteen Extra Large Instance.serviceoffering'`

#### Dienstangebot eines bestehenden Provisioningschemas mit unterstütztem Ruhezustand aktivieren

1. Führen Sie den Befehl `Set-ProvScheme` aus. Beispiel:

```
Set-ProvScheme -ProvisioningSchemeName <String> -ServiceOffering <
    String>
<!--NeedCopy-->
```

Das System zeigt eine Ausnahmemeldung an, wenn das Dienstangebot nicht kompatibel ist.

#### Update eines Maschinenkatalogs, der den Ruhezustand unterstützt

Wenn Sie versuchen, einen vorhandenen Maschinenkatalog durch einen Maschinenkatalog zu ersetzen, der den Ruhezustand nicht unterstützt, schlägt das Update fehl und es wird eine Fehlermeldung angezeigt.

#### Energieverwaltung von VMs im Ruhezustand

Sie können die folgenden Energieverwaltungsvorgänge auf VMs im Ruhezustand ausführen:

1. Sie können eine ausgeführte VM anhalten.
2. Sie können eine angehaltene VM fortsetzen.
3. Sie können eine angehaltene VM neu starten.

## Energieverwaltung für Azure-VMs

June 27, 2024

Informationen zu den erforderlichen Berechtigungen finden Sie unter Erforderliche Azure-Berechtigungen.

### Bedarfsgesteuertes Provisioning in Azure

Beim bedarfsgesteuerten Provisioning in Azure werden VMs nur erstellt, wenn Citrix Virtual Apps and Desktops nach Abschluss des Provisionings eine Einschaltaktion initiiert.

Wenn Sie Maschinenkataloge mit Maschinenerstellungsdiensten (MCS) in Azure Resource Manager erstellen, bietet das bedarfsgesteuerte Provisioning in Azure folgende Vorteile:

- Geringere Speicherkosten
- Schnellere Katalogerstellung

Wenn Sie einen MCS-Katalog erstellen, werden im Azure-Portal die Netzwerksicherheitsgruppen, Netzwerkschnittstellen, Basisimages und Identitätsdatenträger in den Ressourcengruppen angezeigt.

VMs werden erst dann im Azure-Portal angezeigt, wenn Citrix Virtual Apps and Desktops eine VM-Einschaltaktion startet. Es gibt zwei Arten von Maschinen mit den folgenden Unterschieden:

- Bei gepoolten Maschinen sind OS-Datenträger und Zurückschreibcache nur vorhanden, wenn die VM vorhanden ist. Wenn Sie eine gepoolte Maschine in der Konsole herunterfahren, ist die VM im Azure-Portal nicht sichtbar. Wenn Sie Maschinen routinemäßig herunterfahren (z. B. außerhalb der Arbeitszeit), sparen Sie erhebliche Speicherkosten.
- Bei dedizierten Maschinen wird der Betriebssystemdatenträger beim ersten Einschalten der VM erstellt. Die virtuelle Maschine im Azure-Portal bleibt im Speicher, bis die Maschinenidentität gelöscht wird. Wenn Sie eine dedizierte Maschine in der Konsole herunterfahren, ist die VM weiterhin im Azure-Portal sichtbar.

> **Hinweis:**
>
> Die Unterstützung für Azure-Kataloge, die vor der Funktion zur bedarfsgesteuerten Bereitstellung erstellt wurden (“ältere”Kataloge), ist veraltet. Erstellen Sie daher ältere Azure-Katalog-VMs neu. Die Kataloge werden dann nach Bedarf bereitgestellt, wodurch Speicherkosten gespart werden.

### Bereitgestellte virtuelle Maschine bei Energiezyklen beibehalten

Wählen Sie aus, ob eine bereitgestellte virtuelle Maschine bei Energiezyklen (Neustarts) beibehalten werden soll. Verwenden Sie den PowerShell-Parameter `New-ProvScheme CustomProperties`. Dieser Parameter unterstützt die zusätzliche Eigenschaft `PersistVm`, mit der festgelegt wird, ob eine bereitgestellte virtuelle Maschine bei Energiezyklen beibehalten werden soll. Setzen Sie die Eigenschaft `PersistVm` auf **true**, um eine virtuelle Maschine beim Ausschalten beizubehalten, oder setzen Sie die Eigenschaft auf **false**, um die virtuelle Maschine beim Ausschalten nicht beizubehalten.

> **Hinweis:**
>
> Die Eigenschaft `PersistVm` gilt nur für ein Provisioningschema mit aktivierten Eigenschaften `CleanOnBoot` und `UseWriteBackCache`. Wenn die Eigenschaft `PersistVm` für nicht persistente virtuelle Maschinen nicht festgelegt ist, werden die Maschinen nach dem Ausschalten aus der Azure-Umgebung gelöscht.

Im folgenden Beispiel ist die Eigenschaft `PersistVm` im Parameter `New-ProvScheme CustomProperties` auf **true** gesetzt:

```
<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="StorageType" Value="
    Standard_LRS" />
<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true"
    />
<Property xsi:type="StringProperty" Name="PersistVm" Value="true" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="demo-
    resourcegroup" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="
    Windows_Client" />
</CustomProperties>
<!--NeedCopy-->
```

Im folgenden Beispiel behält der Parameter `New-ProvScheme CustomProperties` den Zurückschreibcache bei, indem `PersistVM` auf **true** gesetzt wird:

```
 New-ProvScheme
 -AzureAdJoinType "None"
 -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=`"StorageType`" Value=`"Standard_LRS`" /><
    Property xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"
    false`" /><Property xsi:type=`"StringProperty`" Name=`"
    PersistOsDisk`" Value=`"true`" /><Property xsi:type=`"
    StringProperty`" Name=`"PersistVm`" Value=`"true`" /><Property xsi:
    type=`"StringProperty`" Name=`"ResourceGroups`" Value=`"demo-
    resourcegroup`" /><Property xsi:type=`"StringProperty`" Name=`"
    LicenseType`" Value=`"Windows_Client`" /></CustomProperties>"
 -HostingUnitName "demo"
 -IdentityPoolName "NonPersistent-MCSIO-PersistVM"
 -MasterImageVM "XDHyp:\HostingUnits\demo\image.folder\scale-test.
    resourcegroup\demo-snapshot.snapshot"
 -NetworkMapping @ {
 "0"="XDHyp:\HostingUnits\demo\virtualprivatecloud.folder\East US.
    region\virtualprivatecloud.folder\ji-test.resourcegroup\jitest-vnet
    .virtualprivatecloud\default.network" }

-ProvisioningSchemeName "NonPersistent-MCSIO-PersistVM"
 -ServiceOffering "XDHyp:\HostingUnits\demo\serviceoffering.folder\
    Standard_B2ms.serviceoffering" -UseWriteBackCache
 -WriteBackCacheDiskSize 127
 -WriteBackCacheMemorySize 256
 <!--NeedCopy-->
```

> **Tipp:**
>
> Die Eigenschaft `PersistVm` legt fest, ob eine bereitgestellte virtuelle Maschine beibehalten werden soll. Die Eigenschaft `PersistOsdisk` legt fest, ob der Betriebssystemdatenträger beibehalten werden soll. Um eine bereitgestellte virtuelle Maschine beizubehalten, müssen Sie zuerst den Betriebssystemdatenträger beibehalten. Löschen Sie den Betriebssystemdatenträger nur, wenn Sie zuvor die virtuelle Maschine löschen. Sie können die Eigenschaft `PersistOsdisk` verwenden, ohne den Parameter `PersistVm` festzulegen.

### Einschaltverhalten beim Fehlschlagen der Änderung des Speichertyps anpassen

Beim Einschalten kann der Speichertyp eines verwalteten Datenträgers aufgrund eines Fehlers in Azure möglicherweise nicht in den gewünschten Typ geändert werden. In diesen Szenarien würde die VM ausgeschaltet bleiben, und Sie würden eine Fehlermeldung erhalten. Sie können die VM dann entweder einschalten (auch wenn der Speicher nicht auf den konfigurierten Typ wiederhergestellt werden kann) oder die VM ausgeschaltet lassen.

- Wenn Sie die benutzerdefinierte Eigenschaft `FailSafeStorageType` als **true** konfigurieren (Standardeinstellung) oder sie in den Befehlen `New-ProvScheme` oder `Set-ProvScheme` nicht angeben:
  - Beim Einschalten wird die VM mit dem falschen Speichertyp eingeschaltet.
  - Beim Herunterfahren bleibt die VM mit dem falschen Speichertyp ausgeschaltet.
- Wenn Sie die benutzerdefinierte Eigenschaft `FailSafeStorageType` in den Befehlen `New-ProvScheme` oder `Set-ProvScheme` als **falsch** konfigurieren:
  - Beim Einschalten bleibt die VM mit dem falschen Speichertyp ausgeschaltet.
  - Beim Herunterfahren bleibt die VM mit dem falschen Speichertyp ausgeschaltet.

Erstellen eines Maschinenkatalogs:

1. Öffnen Sie ein PowerShell-Fenster.
2. Führen Sie `asnp citrix*` aus, um die Citrix-spezifischen PowerShell-Module zu laden.
3. Erstellen Sie einen Identitätspool, falls noch nicht vorhanden.
4. Fügen Sie die benutzerdefinierte Eigenschaft in `New-ProvScheme` hinzu. Beispiel:

```
1 New-ProvScheme -HostingUnitName "Azure-Resources-1" -
     IdentityPoolName "name" -InitialBatchSizeHint 1
2 -MasterImageVM "XDHyp:\HostingUnits\Azure-Resources-1\image.folder
     \abc.resourcegroup\def.snapshot"
3 -NetworkMapping @{
4  "0"="XDHyp:\HostingUnits\Azure-Resources-1\ght.folder\abc.
      resourcegroup\abc-vnet.virtualprivatecloud\default.network" }
```

```
5
6  -ProvisioningSchemeName "name"
7  -ServiceOffering "XDHyp:\HostingUnits\Azure-Resources-1\
       serviceoffering.folder\Standard_DS2_v2.serviceoffering"
8  -CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix
       .com/2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org
       /2001/XMLSchema-instance`">
9  <Property xsi:type=`"StringProperty`" Name=`"StorageType`" Value=`
       "Premium_LRS`" />
10 <Property xsi:type=`"StringProperty`" Name=`"StorageTypeAtShutdown
       `" Value=`"Standard_LRS`" />
11 <Property xsi:type=`"StringProperty`" Name=`"FailSafeStorageType`"
        Value=`"true`" />
12 </CustomProperties>"
13 <!--NeedCopy-->
```

5. Erstellen Sie den Maschinenkatalog. Informationen zum Erstellen eines Katalogs mit dem Remote PowerShell SDK finden Sie unter https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

Aktualisieren Sie einen vorhandenen Maschinenkatalog, sodass er die benutzerdefinierte Eigenschaft `FailSafeStorageType` enthält. Dieses Update wirkt sich nicht auf bestehende VMs aus.

1. Aktualisieren Sie die benutzerdefinierte Eigenschaft im Befehl `Set-ProvScheme`. Beispiel:

```
1    Set-ProvScheme -ProvisioningSchemeName <String> -CustomProperties "
2    <CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
        machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
        instance`">
3    <Property xsi:type=`"StringProperty`" Name=`"StorageType`" Value=`"
        Premium_LRS`" />
4    <Property xsi:type=`"StringProperty`" Name=`"IdentityDiskStorageType
        `" Value=`"Premium_LRS`" />
5    <Property xsi:type=`"StringProperty`" Name=`"FailSafeStorageType`"
        Value=`"false`" />
6    </CustomProperties>"
7    <!--NeedCopy-->
```

Führen Sie den Befehl `Set-ProvVMUpdateTimeWindow` mit den Parametern `-StartsNow` und `-DurationInMinutes -1` aus, um die in Set-ProvScheme vorgenommene Änderung auf die vorhandenen VMs anzuwenden.

1. Führen Sie den Befehl `Set-ProvVMUpdateTimeWindow` mit den Parametern `-StartsNow` und `-DurationInMinutes -1` aus. Beispiel:

```
1  Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -
       VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
2  <!--NeedCopy-->
```

2. Starten Sie die VMs neu.

## Für den Ruhezustand geeignete VMs erstellen

In Azure-Umgebungen können Sie einen MCS-Maschinenkatalog erstellen, der den Ruhezustand unterstützt. Mit diesem Feature können Sie eine VM anhalten und dann wieder mit dem vorherigen Status der VM verbinden, wenn sich ein Benutzer erneut anmeldet.

Die Funktion für den Ruhezustand gilt für Folgendes:

- Einzelsitzungs-OS
- Persistente und nicht persistente VMs
- Statische und zufällige (gepoolte) VDI-Desktops

Sie können dieselbe Sitzung fortsetzen, nachdem Sie eine VM in den Ruhezustand versetzt haben, unabhängig davon, ob der VDI-Desktop statisch oder zufällig ist.

In diesem Abschnitt finden Sie Folgendes:

- Voraussetzungen
- Einschränkungen
- Katalog mit für den Ruhezustand geeigneten Maschinen erstellen und verwalten
- Maschinenkatalog für bestehende Maschinen erstellen, die für den Ruhezustand geeignet sind
- Ruhezustand auf bestehenden, per MCS bereitgestellten VMs aktivieren
- Ruhezustand-Eigenschaft überprüfen
- Energieverwaltung von VMs (manuell und automatisch)

### Voraussetzungen für die Verwendung des Ruhezustands

Führen Sie die folgenden Aufgaben aus, um den Ruhezustand zu verwenden:

- Installieren Sie den Azure VM Agent auf dem Masterimage für Windows und Linux. Die Auslagerungsdatei des Windows-Images kann sich auf dem temporären Datenträger befinden. MCS legt den Speicherort der Auslagerungsdatei auf Laufwerk C: des Basisdatenträgers fest, wenn der Ruhezustand für den Maschinenkatalog aktiviert ist.
- MCS legt die Ruhezustands-Eigenschaft für die generierten Ressourcen automatisch fest. Sie müssen die Eigenschaften der Master-Ressourcen nicht konfigurieren, um den Ruhezustand zu unterstützen.
- Verwenden Sie eine VM-Größe in Ihrem Abonnement, die den Ruhezustand unterstützt.
- Erstellen Sie ein für den Ruhezustand geeignetes Maschinenprofil (VM oder Vorlagenspezifikation), damit VMs die Eignung für den Ruhezustand erben. Informationen zum Erstellen der VM finden Sie unter Erste Schritte mit dem Ruhezustand.

> **Hinweis:**
>
> Gemäß Microsoft können Sie für den Ruhezustand geeignete VMs von einem Betriebssystemdatenträger aus bereitstellen. Das Feature wird derzeit für bestimmte Regionen unterstützt und in Kürze für alle Regionen verfügbar sein. Weitere Informationen finden Sie unter VMs mit aktiviertem Ruhezustand von einem Betriebssystemdatenträger bereitstellen.

Gehen Sie wie folgt vor, um die Vorlagenspezifikation zu erstellen:

1. Öffnen Sie das Azure-Portal. Wählen Sie die VM, deren Konfiguration Sie in der Vorlage verwenden möchten. Wählen Sie im linken Bereich **Vorlage exportieren**.
2. Deaktivieren Sie das Kontrollkästchen **Parameter einschließen**. Kopieren Sie den Kontext und speichern Sie ihn als JSON-Datei (beispielsweise `VMExportTemplate.json`).
3. Vergewissern Sie sich, dass der Parameter `hibernationEnabled` für die Vorlage auf **`true`** steht. Wenn der Parameter nicht auf **`true`** steht, überprüfen Sie die verwendete VM-Konfiguration. Sie können eine unterstützte VM-Größe in der Vorlagendatei angeben. Sie können die VM-Größe aber auch beim Erstellen des Katalogs angeben.
4. Fügen Sie der JSON-Datei `VMExportTemplate.json` die Vorlage für die Netzwerkschnittstellenressource hinzu. Dadurch erhalten Sie eine ARM-Vorlagendatei mit zwei Ressourcen.
5. Wählen Sie **Azure-Portal > Vorlagenspezifikationen > Vorlage importieren > Lokale Vorlagendatei auswählen**, um diese Vorlagendatei als ARM-Vorlagenspezifikation zu importieren.
6. Nach Erstellung der ARM-Vorlagenspezifikation können Sie diese als Maschinenprofil verwenden.

> **Hinweis:**
>
> Die Synchronisierung mit Citrix Studio kann einige Minuten dauern.

Informationen hierzu finden Sie bei Microsoft unter Voraussetzungen für die Verwendung des Ruhezustands.

#### Einschränkungen

- Es werden nur Einzelsitzungs-OS-Maschinenkataloge (persistente und nicht persistente) unterstützt.
- Kurzlebige Betriebsystemdatenträger und MCS-E/A-Features unterstützen den Azure-Ruhezustand nicht.
- Während der automatischen Windows-Updates schlägt der Ruhezustand möglicherweise fehl.

Weitere Informationen finden Sie in der Microsoft-Dokumentation.

### Katalog mit für den Ruhezustand geeigneten Maschinen erstellen und verwalten

Um virtuelle Maschinen mit Eignung für den Ruhezustand zu erstellen, können Sie einen entsprechenden Maschinenkatalog mithilfe einer der folgenden Optionen erstellen:

- Web Studio oder
- PowerShell-Befehle

#### Katalog mit Web Studio erstellen

1. Wählen Sie **Maschinenkatalog erstellen**. Der Assistent zum Erstellen von Katalogen wird geöffnet.
2. Wählen Sie auf der Seite **Maschinentyp** die Option **Einzelsitzungs-OS**.
3. Wählen Sie auf der Seite **Maschinenverwaltung** die Einstellungen wie folgt aus:
   a) Wählen Sie **Maschinen mit Energieverwaltung (z. B. virtuelle Maschinen oder Blade-PCs)**.
   b) Wählen Sie **Citrix Maschinenerstellungsdienste (MCS)**.
4. Wählen Sie auf der Seite **Desktoperfahrung** je nach Bedarf die zufällige oder statische Desktoperfahrung aus.
5. Wählen Sie auf der Seite **Image** ein Masterimage. Aktivieren Sie das Kontrollkästchen **Maschinenprofil verwenden** und wählen Sie ein Maschinenprofil aus, das den Ruhezustand unterstützt. Klicken Sie auf den Tooltip, um zu ermitteln, ob ein Maschinenprofil den Ruhezustand unterstützt.
6. Wählen Sie auf der Seite **Speicher- und Lizenztypen** den für diesen Katalog zu verwendenden Speicher und die Lizenz.
7. Wählen Sie auf der Seite **Virtuelle Maschinen** die Anzahl der VMs, die VM-Größe und die Verfügbarkeitszone.

   > **Hinweis:**
   >
   > Es werden nur Maschinengrößen zur Auswahl angezeigt, die den Ruhezustand unterstützen.

8. Fügen Sie auf der Seite **Netzwerkkarten** die Netzwerkkarten hinzu, die die VMs verwenden sollen.
9. Wählen Sie auf der Seite **Datenträgereinstellungen** den Speichertyp und die Größe des Zurückschreibcache-Datenträgers aus.
10. Wählen Sie auf der Seite **Ressourcengruppe** die Ressourcengruppe für die Bereitstellung von VMs aus.

11. Wählen Sie auf der Seite **Maschinenidentitäten** die Option **Neue Active Directory-Konten erstellen**. Geben Sie dann ein Kontobenennungsschema an.
12. Klicken Sie auf der Seite **Domänenanmeldeinformationen** auf **Anmeldeinformationen eingeben**. Geben Sie Ihre Domänenanmeldeinformationen ein, um die Kontenerstellung in der Active Directory-Zieldomäne durchzuführen.
13. Geben Sie auf der Seite **Zusammenfassung** einen Namen für den Maschinenkatalog ein und klicken Sie auf **Fertigstellen**.

Nach Erstellung des MCS-Maschinenkatalogs suchen Sie den Katalog in der Katalogliste und klicken Sie auf die Registerkarte **Vorlageneigenschaften**. Der Wert des Parameters **Ruhezustand** muss **Unterstützt** lauten.

Wenn Sie einen Maschinenkatalog bearbeiten möchten, beachten Sie die folgenden Einschränkungen:

- Wenn der aktuelle Maschinenkatalog den Ruhezustand unterstützt, ist Folgendes nicht möglich:
  - Ändern der VM-Größe auf eine Größe, die nicht für den Ruhezustand geeignet ist.
  - Ändern des Maschinenprofils auf eines, das nicht für den Ruhezustand geeignet ist.
- Wenn der aktuelle Maschinenkatalog den Ruhezustand nicht unterstützt, ist Folgendes nicht möglich:
  - Derzeit können Sie das Maschinenprofil nicht in Web Studio in ein für den Ruhezustand geeignetes Profil umwandeln. Sie können hierfür jedoch PowerShell-Befehle verwenden. Siehe Ruhezustand für per MCS bereitgestellte Maschinen aktivieren.

**Maschinenkatalog für die Verwaltung bestehender Maschinen erstellen, die für den Ruhezustand geeignet sind** Wenn Sie über virtuelle Maschinen verfügen, die für den Ruhezustand geeignet sind und deren Betrieb anhalten und wieder aufnehmen möchten, erstellen Sie einen Maschinenkatalog, um die VMs für die Energieverwaltung zu importieren.

> **Hinweis:**
>
> Sie können einen Maschinenkatalog erstellen, der sowohl für den Ruhezustand geeignete als auch nicht geeignete VMs enthält. Wenn Sie jedoch die Ruhezustandsfunktionen nutzen möchten, darf der Maschinenkatalog nur VMs enthalten, die für den Ruhezustand geeignet sind.

Um über Web Studio einen Katalog für vorhandene virtuelle Maschinen zu erstellen, die für den Ruhezustand geeignet sind, folgen Sie den angezeigten Anweisungen und achten Sie auf die folgenden wichtigen Einstellungen:

1. Wählen Sie auf der Seite **Maschinenverwaltung** die Option **Maschinen mit Energieverwaltung** und dann **Anderer Dienst oder andere Technologie** als Methode der Maschinenbereitstellung.

2. Fügen Sie auf der Seite **Virtuelle Maschinen** nur die virtuellen Maschinen hinzu (oder importieren Sie Maschinen), die für den Ruhezustand geeignet sind.

**Maschinenkatalog mit PowerShell-Befehlen erstellen** Wenn alle Anforderungen für die Verwendung des Ruhezustands erfüllt sind, können Sie mithilfe des Befehls `New-ProvScheme` einen Maschinenkatalog erstellen, der für den Ruhezustand geeignet ist. Informationen zum Erstellen eines Katalogs mit dem Remote PowerShell SDK finden Sie unter New-ProvScheme.

Bei der Katalogerstellung können Sie mithilfe der folgenden PowerShell-Befehle überprüfen, ob eine VM-Größe und ein Maschinenprofil den Ruhezustand unterstützen:

- Führen Sie für die VM-Größe den folgenden Befehl aus und überprüfen Sie, ob die Eigenschaft `supportsHibernation` auf **True** steht. Beispiel:

```
1  Get-ChildItem -AdminAddress "MyDDC.MyDomain.local" -LiteralPath @
       ("XDHyp:\HostingUnits\ <VirtualNetwork> \serviceoffering.
       folder") | select Name, AdditionalData | ConvertTo-Json
2  <!--NeedCopy-->
```

- Führen Sie für das Maschinenprofil den folgenden Befehl aus und überprüfen Sie, ob die Eigenschaft `supportsHibernation` auf **True** steht. Beispiel:

```
1  Get-ChildItem -AdminAddress "MyDDC.MyDomain.local" -LiteralPath @
       ("XDHyp:\HostingUnits\ <VirtualNetwork> \machineprofile.folder
       \abc.resourcegroup")|select Name, AdditionalData|ConvertTo-
       Json
2  <!--NeedCopy-->
```

Wenn Sie einen Maschinenkatalog bearbeiten möchten, beachten Sie die folgenden Einschränkungen:

- Wenn der aktuelle Maschinenkatalog den Ruhezustand unterstützt, ist Folgendes nicht möglich:
  - Ändern der VM-Größe auf eine Größe, die nicht für den Ruhezustand geeignet ist
  - Ändern des Maschinenprofils auf eines, das nicht für den Ruhezustand geeignet ist
- Wenn der aktuelle Maschinenkatalog den Ruhezustand nicht unterstützt, ist Folgendes nicht möglich:
  - Derzeit können Sie das Maschinenprofil nicht in Web Studio in ein für den Ruhezustand geeignetes Profil umwandeln. Sie können hierfür jedoch PowerShell-Befehle verwenden. Siehe Ruhezustand für per MCS bereitgestellte Maschinen aktivieren.

Informationen zum Ändern der VM-Größe und des Maschinenprofils für einen Katalog mit dem Remote PowerShell SDK finden Sie unter https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Set-ProvScheme/.

### Ruhezustand auf bestehenden, per MCS bereitgestellten VMs aktivieren

Sie können den Azure-Ruhezustand für Folgendes aktivieren:

- Mit MCS bereitgestellte Windows-VMs eines Maschinenkatalogs ohne temporären Datenträger.
- Mit MCS bereitgestellte Linux-VMs eines Maschinenkatalogs mit oder ohne temporären Datenträger.

> **Hinweis:**
>
> - Auf den über MCS bereitgestellten VMs muss ein Azure-VM-Agent installiert sein.
> - Derzeit können Sie das Feature nur mit dem PowerShell-Befehl aktivieren.

Gehen Sie hierzu folgendermaßen vor:

1. Öffnen Sie ein **PowerShell**-Fenster.
2. Führen Sie `asnp citrix*` aus, um Citrix-spezifische PowerShell-Module zu laden.
3. Prüfen Sie die Konfiguration der vorhandenen Maschinen. Beispiel:

```
Get-ProvScheme | select ProvisioningSchemeName,
    ProvisioningSchemeVersion
<!--NeedCopy-->
```

4. Aktivieren Sie den Ruhezustand für den Maschinenkatalog mit dem Befehl `Set-ProvScheme`. Beispiel:

```
Set-ProvScheme -provisioningSchemeName xxxx
-machineprofile <path-to-machineprofile-with-hibernation-enabled>
-serviceoffering "XDHyp:\HostingUnits\msc-dev\serviceoffering.
    folder\Standard_D4as_v5.serviceoffering"
<!--NeedCopy-->
```

5. Fordern Sie ein Update für VMs in einem Maschinenkatalog an.

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeUid xxxx -VMName <
    String[]
<!--NeedCopy-->
```

6. Starten Sie die VMs neu, um Updates auszulösen. Beispiel:

```
New-BrokerHostingPowerAction -machinename "<name>" -Action Restart
<!--NeedCopy-->
```

### Ruhezustand-Eigenschaft überprüfen

Sie können die Ruhezustand-Eigenschaft eines Maschinenkatalogs, einer VM oder einer Brokermaschine mithilfe der folgenden PowerShell-Befehle überprüfen:

- Führen Sie die folgenden PowerShell-Befehle aus, um die Ruhezustand-Eigenschaft eines Provisioningschemas zu überprüfen. Der Parameter `HibernationEnabled` muss auf `True` festgelegt sein.

```
(Get-ProvScheme -provisioningSchemeName <YourSchemeName>).
   VMMetadata -join "" |  ConvertFrom-Json | Select
   HibernationEnabled
<!--NeedCopy-->
```

- Führen Sie die folgenden PowerShell-Befehle aus, um die Ruhezustand-Eigenschaft einer Provisioning-VM zu überprüfen. Der Parameter `SupportsHibernation` muss auf `True` festgelegt sein.

```
(Get-ProvVM -VMName <YourVMName>).CustomVmData | ConvertFrom-Json
    | Select SupportsHibernation
<!--NeedCopy-->
```

- Führen Sie die folgenden PowerShell-Befehle aus, um die Ruhezustand-Eigenschaft einer Brokermaschine zu überprüfen. Die Energieaktionen **Anhalten** und **Fortsetzen** zeigen an, dass der Ruhezustand möglich ist.

```
(Get-BrokerMachine -MachineName <YourMachineName>).
   SupportedPowerActions
<!--NeedCopy-->
```

#### Energieverwaltung von für den Ruhezustand geeigneten VMs

Sie können die folgenden Energieverwaltungsvorgänge auf für den Ruhezustand geeigneten VMs ausführen:

- Sie können eine ausgeführte VM **anhalten**.
- Sie können eine angehaltene VM **fortsetzen**.
- Sie können das Herunterfahren einer VM im Zustand "Angehalten"**erzwingen**.
- Sie können den Neustart einer VM im Zustand "Angehalten"**erzwingen**.

Weitere Informationen:

- Anhalten
- Fortsetzen

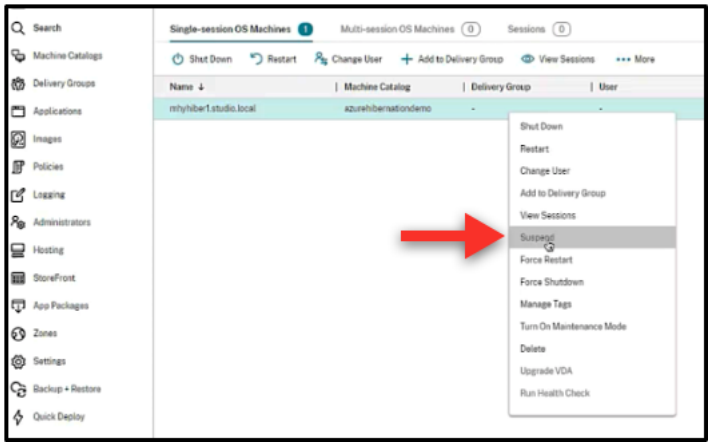
**Anhalten** Sie können eine VM auf eine der folgenden Arten anhalten:

- **Manuell** mit Web Studio
- **Automatisch** mit der Timeout-Richtlinie: Weitere Informationen finden Sie unter Sonstige Einstellungen.

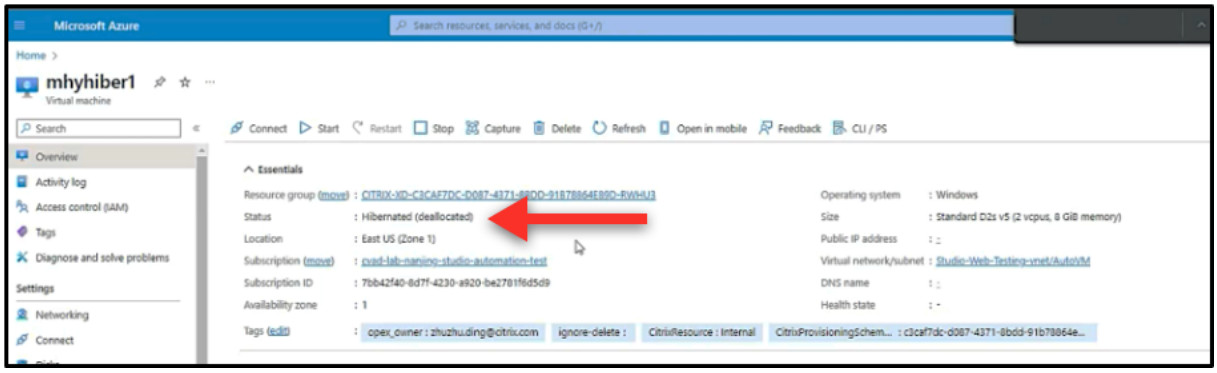
 

Gehen Sie zum manuellen Anhalten einer VM folgendermaßen vor:

1. Klicken Sie mit der rechten Maustaste auf die VM und wählen Sie **Anhalten**. Klicken Sie auf **Ja**, um die Aktion zu bestätigen. Der **Energiezustand** wechselt von **Wird angehalten** zu **Angehalten**.



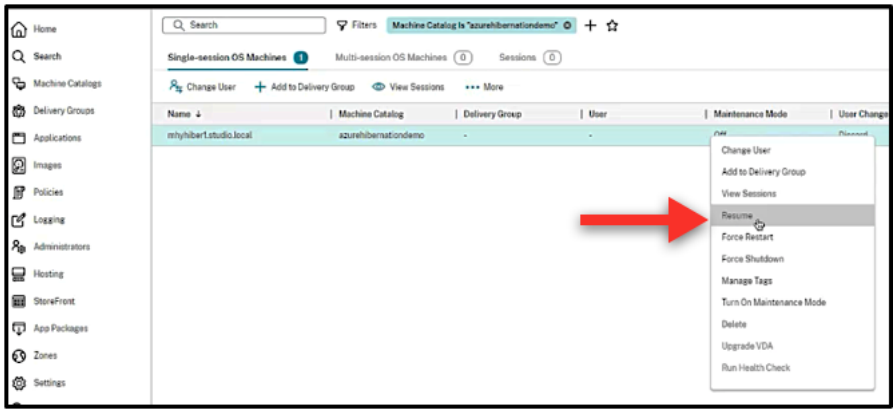

Sie können den Status der VM im Azure-Portal überprüfen.



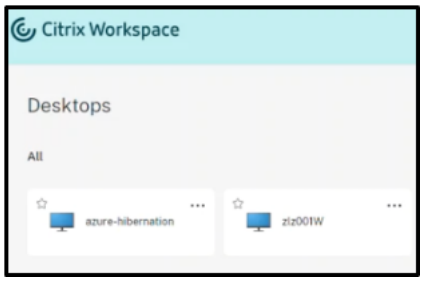

**Fortsetzen** Verwenden Sie eine der folgenden Methoden, um den Betrieb einer VM im Ruhezustand wieder aufzunehmen:

- **Manuell**:
  - Administratoren können die VM mit Web Studio wieder aufnehmen.



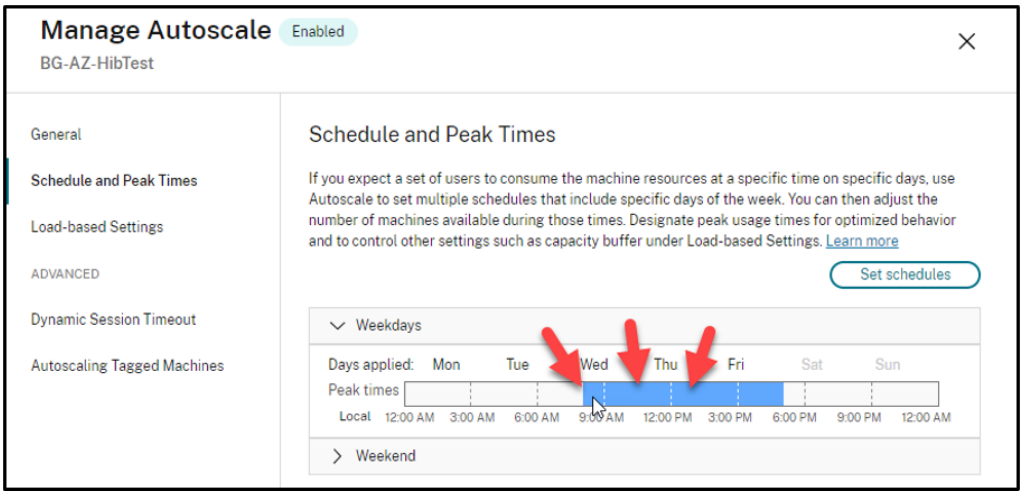

– Endbenutzer können eine VM über das Citrix Workspace-Menü starten, wenn sie auf das Desktopsymbol klicken.




- **Automatisch**:

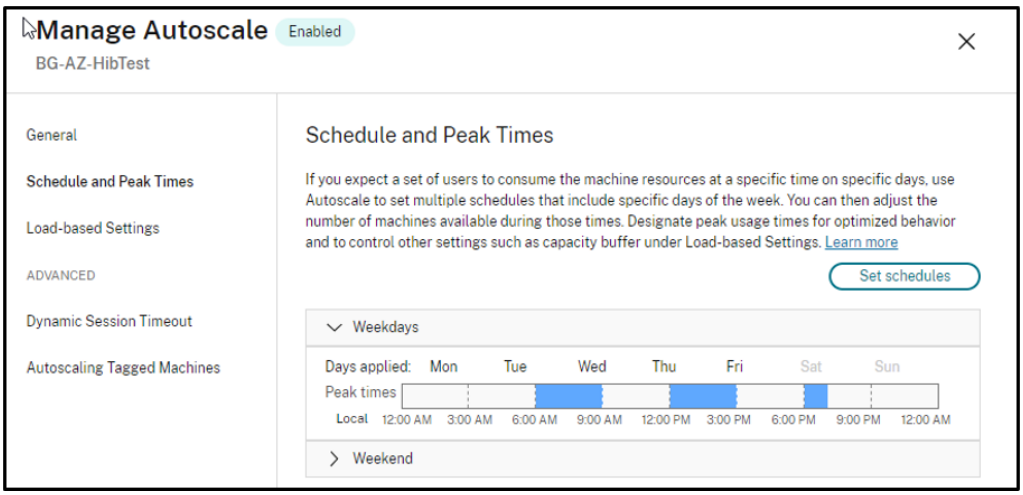
  – Autoscale kann Maschinen im Ruhezustand automatisch einschalten, wenn Sie die Spitzenzeiten richtig konfigurieren. Sie können die Spitzenzeiten in 30-Minuten-Intervallen festlegen, indem Sie auf den Zeitplan klicken. Jeder blaue Rahmen steht für ein Zeitfenster, das als Spitzenzeit markiert ist. Die Spitzenzeiten können aufeinander folgen oder auch nicht.

    * Aufeinanderfolgende Zeitfenster



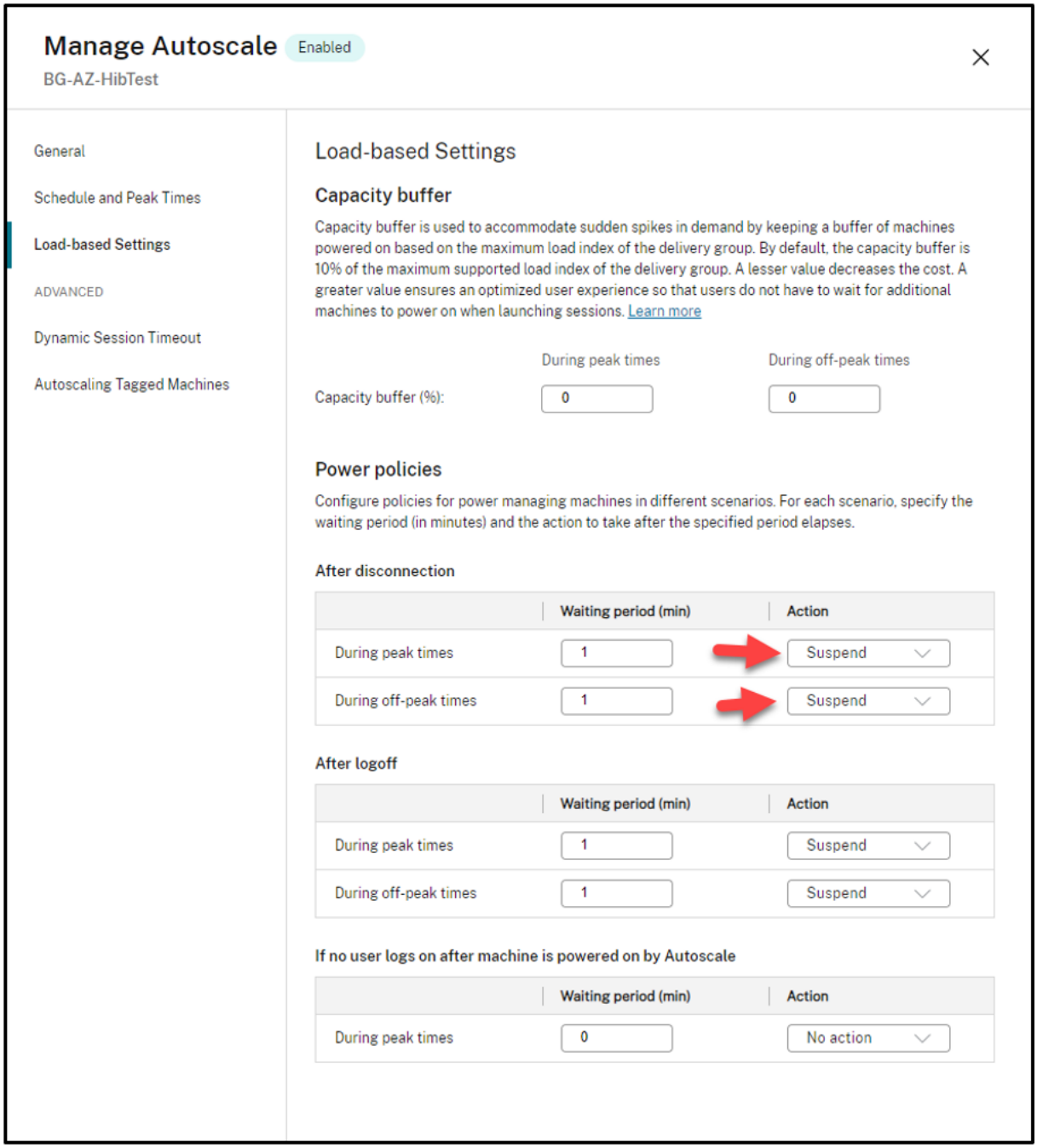

 

* Nicht aufeinanderfolgende Zeitfenster




> **Hinweis:**
>
> Wenn die **Aktion** unter **Autoscale verwalten > Lastbasierte Einstellungen** mit **Anhalten** konfiguriert ist, vergewissern Sie sich, dass alle VMs in der Bereitstellungsgruppe ruhezustandsfähig sind. Andernfalls laufen VMs, die nicht in den Ruhezustand versetzt werden können, weiter.




## Weitere Informationen

Weitere Informationen zum Citrix Azure-Ruhezustand finden Sie in diesem Citrix Tech Zone-Artikel.

# Sicherheitsrichtlinien

June 27, 2024

In diesem Artikel werden die Sicherheitsfeatures für verschiedene unterstützte Cloudservices beschrieben. Dazu gehören:

- Sicherheitsgruppen
- Sicherer Start
- Verschlüsselungsfunktionen

# Sicherheitsgruppen

June 27, 2024

Eine Sicherheitsgruppe ist eine Gruppe von Sicherheitsregeln zum Filtern des Netzwerkdatenverkehrs zwischen Ressourcen in einem virtuellen Netzwerk. Die Sicherheitsregeln erlauben oder verweigern eingehenden und ausgehenden Netzwerkdatenverkehr an und von Ressourcen verschiedener Art. Jede Regel spezifiziert die folgenden Eigenschaften:

- Name: Ein eindeutiger Name innerhalb der Netzwerksicherheitsgruppe
- Priorität: Regeln werden in der Reihenfolge ihrer Priorität verarbeitet, wobei niedrigere Zahlen vor höheren Zahlen verarbeitet werden, da niedrigere Zahlen eine höhere Priorität haben.
- Quelle oder Ziel: Beliebige oder eine einzelne IP-Adresse, ein CIDR-Block (klassenloses domänenübergreifendes Routing, z. B. 10.0.0.0/24), ein Service-Tag oder eine Anwendungssicherheitsgruppe
- Protokoll: Die Protokolle, auf deren Grundlage Sie Regeln für jede Sicherheitsgruppe hinzufügen
- Richtung: Ob die Regel für eingehenden oder ausgehenden Datenverkehr gilt
- Portbereich: Sie können einen einzelnen Port oder einen Bereich von Ports angeben.
- Aktion: Zulassen oder Ablehnen

Weitere Informationen zu unterstützten Hypervisors:

- Sicherheitsgruppen in AWS
- Sicherheitsgruppen in Microsoft Azure
- Sicherheitsgruppen in Google Cloud Platform

### Sicherheitsgruppen in AWS

Sicherheitsgruppen fungieren als virtuelle Firewall und steuern den Datenverkehr für die Instanzen in der VPC. Sie fügen den Sicherheitsgruppen Regeln zur Kommunikation zwischen Instanzen im öffentlichen und im privaten Subnetz hinzu. Sie können die Sicherheitsgruppen außerdem jeder Instanz in der VPC zuordnen. Eingehende Regeln steuern den eingehenden Datenverkehr zu einer Instanz und ausgehende Regeln steuern den ausgehenden Datenverkehr von der Instanz.

Weitere Informationen Netzwerkeinstellung während der Imagevorbereitung finden Sie unter Netzwerkeinstellung während der Imagevorbereitung.

Wenn Sie eine Instanz starten, können Sie eine oder mehrere Sicherheitsgruppen angeben. Informationen zum Konfigurieren von Sicherheitsgruppen finden Sie unter Sicherheitsgruppen konfigurieren.

### Sicherheitsgruppen in Microsoft Azure

Citrix Virtual Apps and Desktops unterstützt Netzwerksicherheitsgruppen in Azure. Von Netzwerksicherheitsgruppen wird erwartet, dass sie Subnetzen zugeordnet sind. Weitere Informationen finden Sie unter Netzwerksicherheitsgruppen.

Weitere Informationen zu bei der Imageerstellung erstellten Netzwerksicherheitsgruppen finden Sie unter Maschinenkatalog unter Verwendung eines Azure Resource Manager-Images erstellen.

### Sicherheitsgruppen in Google Cloud Platform

Bei der Vorbereitung eines Maschinenkatalogs wird ein Maschinenabbild vorbereitet, das als Masterimage-Systemdatenträger für den Katalog dient. Bei diesem Vorgang wird der Datenträger vorübergehend an eine virtuelle Maschine angefügt. Die VM muss in einer isolierten Umgebung ausgeführt werden, die jeglichen eingehenden und ausgehenden Netzwerkdatenverkehr verhindert. Dies wird durch zwei Alles-abweisen-Firewallregeln erreicht. Weitere Informationen finden Sie unter Firewallregeln.

## Sicherer Start

June 27, 2024

Secure Boot soll dafür sorgen, dass nur vertrauenswürdige Software zum Starten des Systems verwendet wird. Die Firmware verfügt über eine Datenbank mit vertrauenswürdigen Zertifikaten und überprüft, ob das zu ladende Image mit einem dieser Zertifikate signiert wurde. Wenn das Image weitere

Images lädt, müssen diese auf die gleiche Weise überprüft werden. vTPM ist eine virtualisierte Softwareinstanz eines herkömmlichen physischen TPM-Moduls. vTPM ermöglicht einen Nachweis durch Messung der gesamten Startkette der VM (UEFI, Betriebssystem, System und Treiber).

Im Folgenden finden Sie weitere Informationen zu unterstützten Cloudservices:

- Secure Boot in Google Cloud Platform
- Secure Boot in Microsoft Azure
- Secure Boot in VMware

### Secure Boot in Google Cloud Platform

Sie können abgeschirmte virtuelle Maschinen auf GCP bereitstellen. Eine abgeschirmte virtuelle Maschine wird durch Sicherheitskontrollen gehärtet, die eine überprüfbare Integrität der Compute Engine-Instanzen über erweiterte Plattformsicherheitsfunktionen wie Sicherer Start, ein virtuelles Trusted Platform Module, UEFI-Firmware und Integritätsüberwachung bieten.

Weitere Informationen zur Verwendung von PowerShell zum Erstellen eines Katalogs mit Shielded VM finden Sie unter Katalog mit Shielded VM mit PowerShell erstellen.

> **Hinweis:**
>
> Wenn Sie Windows 11 auf dem Masterimage installieren, müssen Sie vTPM während der Erstellung des Masterimages aktivieren. Außerdem müssen Sie vTPM auf der Maschinenprofilquelle (VM oder Instanzvorlage) aktivieren. Informationen zum Erstellen von Windows 11-VMs auf dem Einzelmandantenknoten finden Sie unter Windows 11-VMs auf dem Einzelmandantenknoten erstellen.

### Secure Boot in Microsoft Azure

In Azure-Umgebungen können Sie Maschinenkataloge erstellen, für die vertrauenswürdiger Start aktiviert ist. Mit vertrauenswürdigen Starts in Azure lässt sich die Sicherheit von VMs der zweiten Generation weiter verbessern. Der vertrauenswürdige Start schützt vor fortschrittlichen und persistenten Angriffstechniken. Die Grundlage des vertrauenswürdigen Starts bildet Secure Boot für die VM. Der vertrauenswürdige Start verwendet außerdem vTPM für den Remote-Nachweis durch die Cloud. Dies wird für Plattform-Integritätsprüfungen und für vertrauensbasierte Entscheidungen genutzt. Sie können Secure Boot und vTPM individuell aktivieren. Weitere Informationen zum Erstellen eines Maschinenkatalogs mit vertrauenswürdigem Start finden Sie unter Maschinenkataloge mit vertrauenswürdigem Start.

### Secure Boot in VMware

MCS unterstützt das Erstellen eines Maschinenkatalogs mit einer VMware-Vorlage mit angefügtem vTPM als Quelle für die Maschinenprofileingabe. Ist Windows 11 auf dem Masterimage installiert, muss vTPM für das Masterimage aktiviert sein. Daher muss an die VMware-Vorlage, die eine Quelle für das Maschinenprofil ist, vTPM angefügt sein. Weitere Informationen finden Sie unter Erstellen eines Maschinenkatalogs unter Verwendung eines Maschinenprofils.

## Verschlüsselungsfunktionen

June 27, 2024

Verschlüsselungsfunktionen schützen den Inhalt virtueller Maschinen vor Angriffen böswilliger Gäste auf einem freigegebenen VM-Host und vor Angriffen durch die Hypervisor-Steuerungssoftware, die alle virtuellen Maschinen auf dem Host verwaltet.

Im Folgenden finden Sie weitere Informationen zu unterstützten Cloudservices:

- Verschlüsselungsfunktionen in AWS
- Verschlüsselungsfunktionen in Google Cloud Platform
- Verschlüsselungsfunktionen in Microsoft Azure

### Verschlüsselungsfunktionen in AWS

In diesem Abschnitt werden die Verschlüsselungsfunktionen in AWS-Virtualisierungsumgebungen beschrieben.

#### Automatische Verschlüsselung

Sie können die automatische Verschlüsselung neuer Amazon EBS-Volumes und Snapshotkopien aktivieren, die in Ihrem Konto erstellt wurden. Weitere Informationen finden Sie unter Automatische Verschlüsselung.

### Verschlüsselungsfunktionen in Google Cloud Platform

In diesem Abschnitt werden die Verschlüsselungsfunktionen in GCP-Virtualisierungsumgebungen beschrieben.

Wenn Sie mehr Kontrolle über Schlüsseloperationen benötigen, als mit den von Google verwalteten Verschlüsselungsschlüsseln möglich ist, können Sie kundenverwaltete Verschlüsselungsschlüssel verwenden. Bei Verwendung kundenverwalteter Verschlüsselungsschlüssel werden Objekte zum Zeitpunkt der Speicherung in einem Bucket von Cloud Storage verschlüsselt und automatisch entschlüsselt, wenn sie Anforderern zugestellt werden. Weitere Informationen finden Sie unter Vom Kunden verwaltete Verschlüsselungsschlüssel.

Sie können vom Kunden verwaltete Verschlüsselungsschlüssel (Customer Managed Encryption Keys, CMEK) für MCS-Kataloge verwenden. Weitere Informationen finden Sie unter Verwenden vom Kunden verwalteter Verschlüsselungsschlüssel (CMEK).

## Verschlüsselungsfunktionen in Microsoft Azure

In diesem Abschnitt werden die Verschlüsselungsfunktionen in Azure-Virtualisierungsumgebungen beschrieben.

### Azure-serverseitige Verschlüsselung

Die meisten Azure-verwalteten Datenträger sind mit der Azure Storage-Verschlüsselung verschlüsselt, bei eine serverseitige Verschlüsselung (SSE) zum Schutz Ihrer Daten und zur Unterstützung Ihrer Maßnahmen für Sicherheit und Compliance verwendet wird. Citrix Virtual Apps and Desktops unterstützt vom Kunden verwaltete Schlüssel für verwaltete Azure-Datenträger über Azure Key Vault. Weitere Informationen finden Sie unter Azure-serverseitige Verschlüsselung.

### Azure-Datenträgerverschlüsselung auf dem Host

Sie können einen MCS-Maschinenkatalog mit Verschlüsselung auf dem Host erstellen.

Bei diesem Verschlüsselungsverfahren werden Daten nicht über den Azure-Speicher verschlüsselt. Die Daten werden auf dem Hostserver verschlüsselt und dann verschlüsselt durch den Azure-Speicherserver geleitet. Es kommt also zu einer End-to-End-Verschlüsselung der Daten.

Weitere Informationen zum Erstellen eines MCS-Maschinenkatalogs mit Verschlüsselung auf dem Host finden Sie unter Azure-Festplattenverschlüsselung auf dem Host.

### Doppelte Verschlüsselung in Azure

Die doppelte Verschlüsselung besteht aus der plattformseitigen Verschlüsselung (Standard) und der kundenseitig verwalteten Verschlüsselung. Kunden, die ein hohes Sicherheitsniveau erfordern und Risiken bezüglich des Verschlüsselungsalgorithmus, der Implementierung oder kompromittierter

Schlüssel befürchten, können die doppelte Verschlüsselung wählen. Persistente Datenträger für OS und Daten, Snapshots und Images werden sämtlich im Ruhezustand doppelt verschlüsselt. Weitere Informationen finden Sie unter Doppelte Verschlüsselung verwalteter Datenträger.

#### Vertrauliche Azure-VMs

Azure Confidential Computing-VMs stellen sicher, dass Ihr virtueller Desktop im Arbeitsspeicher verschlüsselt und bei der Verwendung geschützt ist.

Sie können MCS verwenden, um einen Katalog mit vertraulichen Azure-VMs zu erstellen. Sie müssen den Maschinenprofil-basierten Workflow verwenden, um einen solchen Katalog zu erstellen. Sie können sowohl die VM- als auch die ARM-Vorlagenspezifikation als Eingabe für das Maschinenprofil verwenden.

Weitere Informationen finden Sie unter Vertrauliche Azure-VMs.

## Bereitstellungsgruppen erstellen

June 27, 2024

> **Hinweis:**
>
> Sie können Ihre Citrix Virtual Apps and Desktops-Bereitstellung mithilfe von zwei Verwaltungskonsolen verwalten: Web Studio (webbasiert) und Citrix Studio (Windows-basiert). Dieser Artikel behandelt nur Web Studio. Informationen zu Citrix Studio finden Sie im entsprechenden Artikel in Citrix Virtual Apps and Desktops 7 2212 oder früher.

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 und 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 ohne Bereitstellungsgruppe erstellt haben, führt Web Studio Sie zum richtigen Startpunkt für die Erstellung einer Bereitstellungsgruppe.
2. Wenn Sie bereits eine Bereitstellungsgruppe erstellt haben und eine weitere erstellen möchten, gehen Sie wie folgt vor:

    a) Wählen Sie **Bereitstellungsgruppen**. Wählen Sie im Aktionsbereich **Bereitstellungsgruppe erstellen**.
    b) Um Bereitstellungsgruppen mit Ordnern zu organisieren, erstellen Sie Ordner im Standardordner **Bereitstellungsgruppen**. Weitere Informationen finden Sie unter Ordner erstellen.
    c) Wählen Sie den Ordner aus, in dem Sie die Gruppe erstellen möchten, und klicken Sie auf **Bereitstellungsgruppe erstellen**. Der Assistent zum Erstellen von Gruppen wird geöffnet.

3. Der Assistent wird mit der **Einführungsseite** gestartet, die Sie für zukünftige Starts des Assistenten deaktivieren können.
4. Der Assistent führt Sie dann 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 Katalog kann in mehreren Bereitstellungsgruppen angegeben werden. Eine Maschine kann nur in einer Bereitstellungsgruppe verwendet werden.
- Eine Bereitstellungsgruppe kann Maschinen aus mehreren Maschinenkatalogen verwenden, diese Kataloge müssen allerdings Maschinen desselben Typs enthalten (Multisitzungs-OS- oder Einzelsitzungs-OS-Maschinen 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 auf allen Maschinen die aktuelle VDA-Version installieren oder auf diese aktualisieren. Aktualisieren Sie Kataloge und Bereitstellungsgruppen nach Bedarf. 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. Wenn eine der Maschinen beispielsweise einen VDA der Version 7.1 hat und die anderen die aktuelle VDA-Version haben, 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.

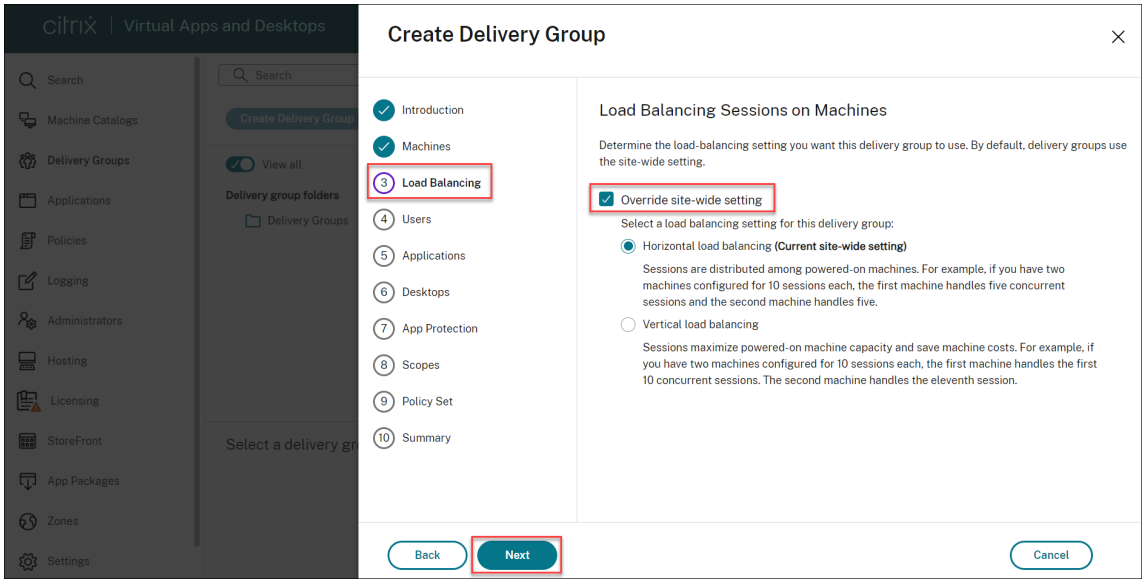
- Jede Maschine in einem Remote-PC-Zugriff-Katalog wird automatisch einer Bereitstellungsgruppe zugewiesen. Wenn Sie eine Remote-PC-Zugriff-Site erstellen, werden automatisch ein Maschinenkatalog unter dem Namen "Remote-PC-Zugriff-Maschinen"und eine Bereitstellungsgruppe unter dem Namen "Remote-PC-Zugriff-Desktops"erstellt.
- 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 Remote-PC-Zugriff-Katalog kompatibel
  - AppDisk-bezogene Überprüfung

### Schritt 2: Lastausgleich

Gehen Sie wie folgt vor, um die Lastausgleich-Einstellungen beim Erstellen einer Bereitstellungsgruppe zu konfigurieren:

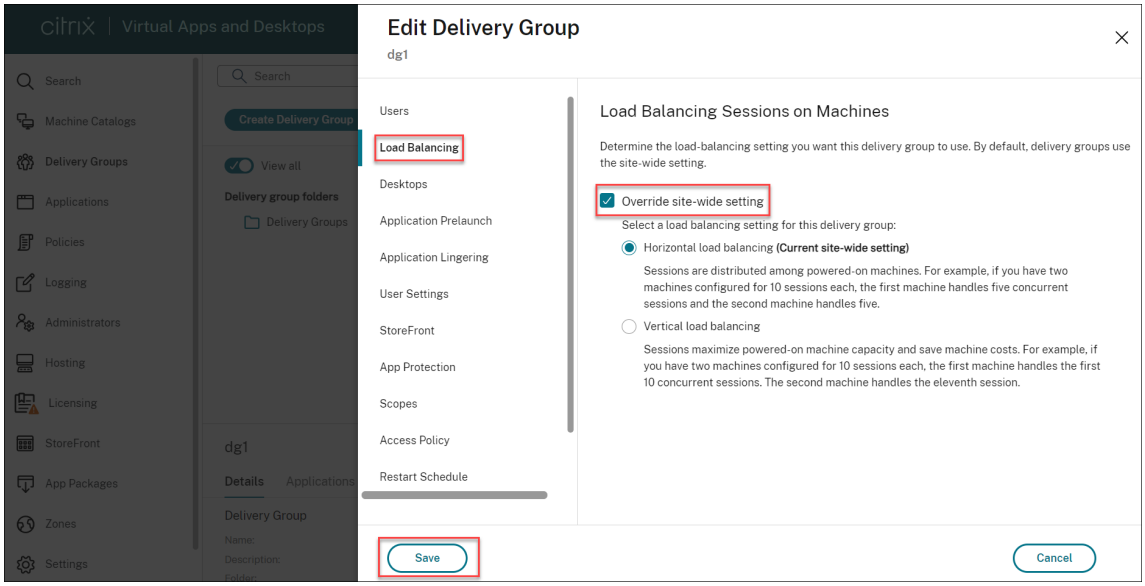
1. Melden Sie sich bei Web Studio an.
2. Klicken Sie in der linken Navigationsleiste auf **Bereitstellungsgruppen**.
3. Klicken Sie auf der Seite **Bereitstellungsgruppen** auf **Bereitstellungsgruppe erstellen**.
4. Klicken Sie im **Assistenten zum Erstellen einer Bereitstellungsgruppe** auf **Weiter**. Der Assistent **Maschinen** wird geöffnet.
5. Wählen Sie im Assistenten **Maschinen** einen erforderlichen Maschinenkatalog und klicken Sie auf **Weiter**. Der Assistent **Lastausgleich** wird geöffnet.
6. Aktivieren Sie im Assistenten **Lastausgleich** das Kontrollkästchen zum **Überschreiben der siteweiten Einstellung**.
7. Wählen Sie je nach Bedarf **Horizontaler Lastenausgleich** oder **Vertikaler Lastenausgleich** und klicken Sie auf **Weiter**.



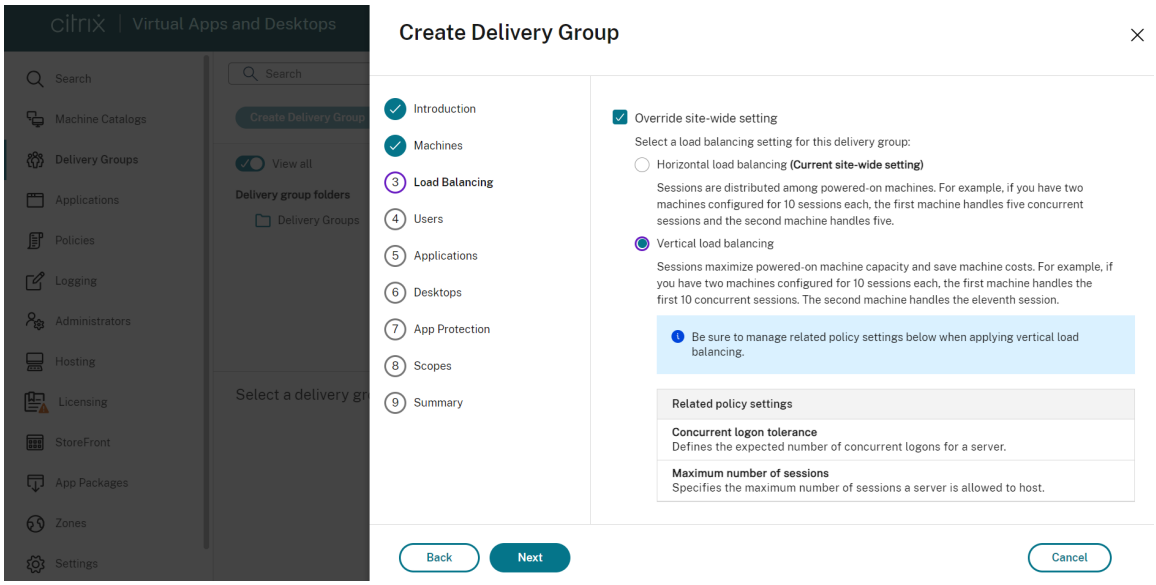

Gehen Sie wie folgt vor, um die Lastausgleich-Einstellungen beim Bearbeiten einer Bereitstellungsgruppe zu konfigurieren:

1. Melden Sie sich bei Web Studio an.
2. Klicken Sie im linken Bereich auf **Bereitstellungsgruppen**.
3. Wählen Sie eine **Bereitstellungsgruppe** aus der Liste aus und klicken Sie auf **Bearbeiten**. Der Assistent zum **Bearbeiten von Bereitstellungsgruppen** wird geöffnet.
4. Klicken Sie auf der Seite **Bereitstellungsgruppe bearbeiten** auf **Lastausgleich**.
5. Aktivieren Sie das Kontrollkästchen zum **Überschreiben der siteweiten Einstellung**.
6. Wählen Sie je nach Bedarf **Horizontaler Lastenausgleich** oder **Vertikaler Lastenausgleich** und klicken Sie auf **Speichern**.



> **Hinweis:**
>
> Bei Auswahl des vertikalen Lastenausgleichs achten Sie darauf, dass die Richtlinien für den **Toleranzwert für gleichzeitige Anmeldungen** und die **Sitzungshöchstanzahl** entsprechend konfiguriert sind.




Weitere Informationen zum Lastausgleich auf Site- und Bereitstellungsgruppenebene finden Sie unter Lastausgleich bei Maschinen

### Schritt 3: Bereitstellungstyp

Diese Seite wird nur angezeigt, wenn Sie einen Maschinenkatalog mit statischen (zugewiesen) Einzelsitzungs-OS-Maschinen auswählen.

Wählen Sie auf der Seite **Bereitstellungstyp** entweder **Anwendungen** oder **Desktops**. Sie können nicht beide aktivieren.

Wenn Sie Maschinen aus einem Katalog mit Multisitzungs-OS-Maschinen oder einem Katalog mit nach dem Zufallsprinzip zugewiesenen (gepoolten) Einzelsitzungs-OS-Maschinen ausgewählt haben, wird als Bereitstellungstyp “Anwendungen und Desktops”angenommen. Sie können Anwendungen, Desktops oder beides bereitstellen.

### 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 Web Studio konfiguriert wird. In der Standardeinstellung gelten die Anwendungsanspruch-Richtlinienregeln 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. Wenn Sie beispielsweise die Verwendung von Anwendung A für eine bestimmte Abteilung konfigurieren möchten, ohne Zugriff für andere Gruppen unnötig einzuschränken, gehen Sie folgendermaßen vor:

- Verwenden der Standardanwendungsanspruch-Richtlinienregel, die für alle Benutzer gilt
- Konfigurieren Sie die Benutzerliste der Bereitstellungsgruppe so, dass alle Benutzer der Organisation die Anwendungen der Bereitstellungsgruppe verwenden können.
- (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 Einzelsitzungs-OS-Maschinen können Sie eine Liste der Benutzer später unter Bearbeiten der Bereitstellungsgruppe importieren.
- **Nicht authentifiziert (anonym):** Bei Bereitstellungsgruppen mit Maschinen mit Multisitzungs-OS 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 im Ordner Anwendungen 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 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 Web 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:** Anwendungen auf einem VDA in der Bereitstellungsgruppe oder an einem anderen Ort in Ihrem Netzwerk. Wenn Sie diese Quelle wählen, wird eine neue Seite geöffnet, auf der Sie mit folgenden Schritten eine Anwendung festlegen können, die Sie hinzufügen möchten:
  - Geben Sie den Pfad zur ausführbaren Datei, das Arbeitsverzeichnis, optionale Befehlszeilenargumente und Anzeigenamen für Administratoren und Benutzer ein.
  - Wählen Sie eine Anwendung von einem VDA in der Bereitstellungsgruppe aus. Klicken Sie dazu auf **Durchsuchen**, geben Sie Ihre Anmeldeinformationen für den VDA-Zugriff ein, warten Sie, bis Sie mit dem VDA verbunden sind, und wählen Sie eine Anwendung auf dem VDA aus. Die Eigenschaften der ausgewählten Anwendung werden automatisch in die Felder auf der Seite eingefügt.
- **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. Fügen Sie die Anwendungen hinzu und klicken Sie 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-Anwendungen bereitstellen.

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.
- Verwenden Sie die Optionsfelder, um einen Desktop zu starten oder eine Maschine beim Starten des Desktops zuzuweisen. 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 in Web Studio angezeigt wird.

Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertigstellen**.

## Bereitstellungsgruppen verwalten

June 27, 2024

> **Hinweis:**
>
> Sie können Ihre Citrix Virtual Apps and Desktops-Bereitstellung mithilfe von zwei Verwaltungskonsolen verwalten: Web Studio (webbasiert) und Citrix Studio (Windows-basiert). Dieser Artikel behandelt nur Web Studio. Informationen zu Citrix Studio finden Sie im entsprechenden Artikel in Citrix Virtual Apps and Desktops 7 2212 oder früher.

### 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.

Verfahrenskategorien: 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

- Gruppendetails anzeigen
- Bereitstellungsmethode ändern
- StoreFront-Adressen ändern
- Funktionsebene ändern
- Remote-PC-Zugriff-Bereitstellungsgruppen verwalten
- Bereitstellungsgruppen mit Ordnern organisieren
- App Protection verwalten

### Gruppendetails anzeigen

1. Verwenden Sie die Suchfunktion, um eine bestimmte Bereitstellungsgruppe zu finden. Anweisungen finden Sie unter Nach Instanzen suchen.
2. Wählen Sie aus den Suchergebnissen nach Bedarf eine Gruppe aus.
3. In der folgenden Tabelle finden Sie Beschreibungen der Gruppenspalten.
4. Klicken Sie im unteren Detailbereich auf eine Registerkarte, um weitere Informationen zu dieser Gruppe zu erhalten.

| Spalte | Beschreibung |
| --- | --- |
| Bereitstellungsgruppe | Der Gruppenname und der Sitzungstyp. Zu den Sitzungstypen gehören Einzelsitzungs-OS und Multisitzungs-OS. |
| Bereitstellen | Der Typ der Ressourcen, die von dieser Gruppe bereitgestellt werden. Zu den möglichen Werten gehören Anwendungen, Desktops sowie Anwendungen und Desktops. “Statische Maschinenzuweisung”wird angezeigt, wenn die Bereitstellungsgruppe aus dedizierten Maschinen besteht. |
| Sitzung wird verwendet | Die Anzahl der eingerichteten Maschinen und die Anzahl der Maschinen, die sich im Zustand “Getrennt”befinden. |
| Zugewiesene Anzahl | Die Anzahl der Maschinen im Katalog, die einer Bereitstellungsgruppe zugewiesen sind. |

| Spalte | Beschreibung |
| --- | --- |
| Ordner | Die Position der Gruppe in der **Bereitstellungsgruppenstruktur**. Hier wird der Name des Ordners angezeigt, in dem sich die Gruppe befindet (einschließlich des abschließenden umgekehrten Schrägstrichs), oder −, wenn sich die Gruppe auf der Stammebene befindet. |

### 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 linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und klicken Sie in der Aktionsleiste auf **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 **Speichern**, um die Konfigurationsänderungen anzuwenden und das Fenster zu schließen.

### StoreFront-Adressen ändern

1. Wählen Sie im linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und klicken Sie in der Aktionsleiste auf **Bearbeiten**.
3. Wählen Sie auf der Seite **StoreFront** die StoreFront-URLs aus oder fügen Sie sie hinzu. Diese URLs werden von der auf jeder Maschine in der Bereitstellungsgruppe installierten Citrix Workspace-App-Instanz verwendet.
4. Klicken Sie auf **Anwenden**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt. Alternativ klicken Sie auf **Speichern**, um die Konfigurationsänderungen anzuwenden und das Fenster zu schließen.

Sie können die StoreFront-Serveradresse auch durch Auswahl von **StoreFront** im linken Bereich festlegen.

### Funktionsebene ändern

Nach dem Upgrade der VDAs auf Maschinen einer Bereitstellungsgruppe sowie auf den Maschinen in den von ihr verwendeten Maschinenkatalogen ändern Sie die Funktionsebene für die Bereitstellungsgruppe.

Vorbereitungen:

- 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 nicht verfügbar. Weitere Informationen finden Sie in der Upgrade-Dokumentation.

Bereitstellungsgruppen aktualisieren:

1. Wählen Sie im linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und klicken Sie in der Aktionsleiste auf **Upgrade von Bereitstellungsgruppe durchführen**. Die Aktion **Funktionsebene ändern** wird nur angezeigt, wenn aktualisierte VDAs erkannt werden.

In der Anzeige sehen Sie, für welche Maschinen die Funktionsebene ggf. nicht geändert werden kann, und warum dies nicht möglich ist. Sie können die Änderung dann abbrechen, das Problem auf der Maschine beheben und die Änderung erneut ausführen.

Nach Abschluss der Änderung können Sie die Maschinen in ihren vorherigen Zustand zurückversetzen. Wählen Sie die Bereitstellungsgruppe und dann in der Aktionsleiste **Änderung der Funktionsebene rückgängig machen**.

### Remote-PC-Zugriff-Bereitstellungsgruppen verwalten

Wenn eine Maschine eines Remote-PC-Zugriff-Maschinenkatalogs nicht 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 die Bereitstellungsgruppe einer Maschine 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. Dem Maschinenkatalog später hinzugefügte Maschinenkonten oder Organisationseinheiten können in der Bereitstellungsgruppe hinzugefügt werden. Die Zuordnung kann deaktiviert oder aktiviert werden.

Hinzufügen oder Entfernen der Zuordnung eines Remote-PC-Zugriff-Maschinenkatalogs zu einer Bereitstellungsgruppe

1. Wählen Sie im linken Bereich **Bereitstellungsgruppen**.
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**.

#### Bereitstellungsgruppen mit Ordnern organisieren

Sie können Ordner erstellen, um den Zugriff auf Bereitstellungsgruppen zu vereinfachen.

**Erforderliche Rollen** Standardmäßig benötigen Sie zum Erstellen und Verwalten von Bereitstellungsgruppenordnern die folgende integrierte Rolle: Cloudadministrator, Volladministrator oder Bereitstellungsgruppenadministrator. Bei Bedarf können Sie Rollen für das Erstellen und Verwalten von Bereitstellungsgruppenordnern anpassen. Weitere Informationen finden Sie unter Erforderliche Berechtigungen.

**Bereitstellungsgruppenordner erstellen** Planen Sie zunächst, wie Sie Ihre Bereitstellungsgruppen organisieren wollen. Beachten Sie Folgendes:

- Sie können Ordner bis zu fünf Ebenen tief verschachteln (mit Ausnahme des Standardstammordners).
- Ein Ordner kann Bereitstellungsgruppen und Unterordner enthalten.
- Alle Knoten (wie etwa **Maschinenkataloge**, **Anwendungen** und **Bereitstellungsgruppen**) teilen sich eine Ordnerstruktur im Back-End. Um Namenskonflikte mit anderen Knoten beim Umbenennen oder Verschieben von Ordnern zu vermeiden, empfehlen wir, Ordnern der ersten Ebene in verschiedenen Knoten unterschiedliche Namen zu geben.

Gehen Sie wie folgt vor, um einen Bereitstellungsgruppenordner zu erstellen:

1. Wählen Sie im linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie in der Ordnerhierarchie einen Ordner aus und klicken Sie dann in der **Aktionsleiste** auf **Ordner erstellen**.

3. Geben Sie einen Namen für den neuen Ordner ein und klicken Sie dann auf **Fertig**.

> **Tipp:**
>
> Wenn Sie einen Ordner an einem falschen Speicherort erstellen, können Sie ihn an den korrekten Speicherort ziehen.

#### Bereitstellungsgruppe verschieben

Sie können eine Bereitstellungsgruppe zwischen Ordnern verschieben. Verfahren:

1. Wählen Sie im linken Bereich **Bereitstellungsgruppen**.
2. Zeigen Sie Gruppen nach Ordner sortiert an. Sie können auch die Option **Alle anzeigen** über der Ordnerhierarchie aktivieren, um alle Bereitstellungsgruppen gleichzeitig anzuzeigen.
3. Klicken Sie mit der rechten Maustaste auf eine Gruppe und wählen Sie **Bereitstellungsgruppe verschieben**.
4. Wählen Sie den Ordner aus, in den Sie die Gruppe verschieben möchten, und klicken Sie auf **Fertig**.

> **Tipp:**
>
> Sie können eine Gruppe in einen Ordner ziehen.

#### Bereitstellungsgruppenordner verwalten

Sie können Bereitstellungsgruppenordner löschen, umbenennen und verschieben.

Beachten Sie, dass Sie einen Ordner nur dann löschen können, wenn er und seine Unterordner keine Bereitstellungsgruppen enthalten.

Gehen Sie wie folgt vor, um einen Ordner zu verwalten:

1. Wählen Sie im linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie in der Ordnerhierarchie einen Ordner aus und wählen Sie dann eine gewünschte Aktion in der **Aktionsleiste** aus:
   - Wählen Sie zum Umbenennen des Ordners **Ordner umbenennen** aus.
   - Wählen Sie zum Löschen des Ordners **Ordner löschen** aus.
   - Wählen Sie zum Verschieben des Ordners **Ordner verschieben** aus.
3. Folgen Sie den Anweisungen auf dem Bildschirm, um die restlichen Schritte auszuführen.

**Erforderliche Berechtigungen** In der folgenden Tabelle sind die Berechtigungen aufgeführt, die zum Ausführen von Aktionen für Bereitstellungsgruppenordner erforderlich sind.

| Aktion | Erforderliche Berechtigungen |
|---|---|
| Bereitstellungsgruppenordner erstellen | Bereitstellungsgruppenordner erstellen |
| Bereitstellungsgruppenordner löschen | Bereitstellungsgruppenordner entfernen |
| Bereitstellungsgruppenordner verschieben | Bereitstellungsgruppenordner verschieben |
| Bereitstellungsgruppenordner umbenennen | Bereitstellungsgruppenordner bearbeiten |
| Bereitstellungsgruppen in Ordner verschieben | Bereitstellungsgruppenordner und Bereitstellungsgruppeneigenschaften bearbeiten |

#### App Protection verwalten

Die folgenden Informationen ergänzen den App-Schutz. Beachten Sie die folgenden Details:

- Sie müssen über einen gültigen Anspruch auf App Protection verfügen. Wenden Sie sich an Ihren Citrix Vertriebsmitarbeiter, um das App Protection-Feature zu erwerben.
- App Protection erfordert XML-Vertrauen. Um XML-Vertrauen zu aktivieren, gehen Sie zu **Einstellungen > XML-Vertrauen aktivieren**.
- Screenshotschutz:
  - Unter Windows und macOS ist nur das Fenster mit dem geschützten Inhalt leer. App Protection ist aktiv, wenn ein geschütztes Fenster nicht minimiert ist.
  - Unter Linux ist der gesamte Screenshot leer. App Protection ist aktiv, unabhängig davon, ob ein geschütztes Fenster minimiert ist.

Führen Sie folgende Schritte aus, um eine App Protection-Methode für eine Bereitstellungsgruppe auszuwählen:

1. Wählen Sie im linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und dann in der Aktionsleiste **Bearbeiten**.
3. Auf der Seite **App Protection** können Sie **Keyloggingschutz** und **Screenshotschutz**aktivieren.

### Benutzer

- Benutzereinstellungen ändern
- Benutzer hinzufügen oder entfernen

**Benutzereinstellungen für eine Bereitstellungsgruppe ändern**

Der Name dieser Seite lautet **Benutzereinstellungen** oder **Grundeinstellungen**.

1. Wählen Sie im linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und klicken Sie in der Aktionsleiste auf **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 **Speichern**, 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. **Hinweis:**Durch das Ändern der Zeitzone für eine Bereitstellungsgruppe kann ein Neustart der darin enthaltenen Maschinen ausgelöst werden. Um Probleme zu vermeiden, ändern Sie die Zeitzoneneinstellungen außerhalb der Produktionszeiten. |
| 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 linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und klicken Sie in der Aktionsleiste auf **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 **Speichern**, 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 zwei durch ein Komma getrennte Spaltenüberschriften enthalten. Die erste Überschrift muss `Machine Account` lauten, die zweite `User Names`. (Sie können zusätzliche Überschriften hinzufügen, diese werden jedoch nicht unterstützt.) Nachfolgende Zeilen in der Datei enthalten durch Kommas getrennte Daten. Die Einträge unter `Machine Account` können Computer-SIDs, FQDN oder Domänen-/Computernamenpaare sein.

Importieren oder Exportieren von Benutzerinformationen

1. Wählen Sie im linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und klicken Sie in der Aktionsleiste auf **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 **Speichern**, um die Konfigurationsänderungen anzuwenden und das Fenster zu schließen.

## Maschinen

- Maschinenbenutzerzuweisung ändern
- Ändern der maximalen Anzahl Maschinen pro Benutzer
- Maschine aktualisieren
- Tagbeschränkungen für einen Desktop hinzufügen, ändern oder entfernen
- Maschine entfernen
- Einschränken des Zugriffs auf Maschinen
- Benutzerverbindung mit Maschinen unterbinden (Wartungsmodus)
- Maschinen herunterfahren und neu starten
- Neustartzeitpläne für Maschinen erstellen und verwalten
- Lastverwaltete Maschinen
- Energieverwaltete 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 linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und klicken Sie in der Aktionsleiste auf **Bearbeiten**.
3. Geben Sie die neuen Benutzer auf der Seite **Desktops** bzw. **Desktopzuweisungsregeln** an (Seitentitel abhängig vom Typ des Maschinenkatalogs).
4. Klicken Sie auf **Anwenden**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt. Alternativ klicken Sie auf **Speichern**, um die Konfigurationsänderungen anzuwenden und das Fenster zu schließen.

### Ändern der maximalen Anzahl Maschinen pro Benutzer in einer Bereitstellungsgruppe

1. Wählen Sie im linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und klicken Sie in der Aktionsleiste auf **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 **Speichern**, um die Konfigurationsänderungen anzuwenden und das Fenster zu schließen.

### Aktualisieren einer Maschine in einer Bereitstellungsgruppe

1. Wählen Sie im linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Gruppe und klicken Sie in der Aktionsleiste auf **Maschinen anzeigen**.
3. Wählen Sie eine Maschine und klicken Sie in der Aktionsleiste auf **Maschinen aktualisieren**.

Zum Auswählen eines anderen Images wählen Sie **Image** 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

### Tagbeschränkungen für einen Desktop hinzufügen, ändern oder entfernen

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 linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und klicken Sie in der Aktionsleiste auf **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 **Speichern**, 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 linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Gruppe und klicken Sie in der Aktionsleiste auf **Maschinen anzeigen**.
3. Vergewissern Sie sich, dass die Maschine heruntergefahren ist.
4. Wählen Sie die Maschine aus und klicken Sie auf in der Aktionsleiste 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:** Erstellen Sie einen Geltungsbereich, in dem Administratoren auf alle Anwendungen zugreifen können, und einen zweiten Geltungsbereich, der nur den Zugriff auf spezifische Anwendungen zulässt, und weisen Sie diese Geltungsbereiche zu. 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 linken Bereich **Bereitstellungsgruppen**.
  2. Wählen Sie eine Bereitstellungsgruppe und klicken Sie in der Aktionsleiste auf **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 **Speichern**, 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.

  Beispiel: Ein Lehrlabor in einem unternehmensinternen Teilnetz, das den Zugriff vom Labor auf eine bestimmte Bereitstellungsgruppe verhindert. Unabhängig davon, wer die Maschinen im Labor verwendet, verwenden Sie den Befehl `Set-BrokerAccessPolicy -Name VPDesktops_Direct -ExcludedClientIPFilterEnabled $True -`.

  Verwenden Sie das Sternchen (*) als Platzhalter für alle Tags, die mit dem gleichen Richtlinienausdruck beginnen. 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 linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Gruppe aus.
3. Zum Aktivieren des Wartungsmodus für alle Maschinen in der Bereitstellungsgruppe klicken Sie in der Aktionsleiste auf **Wartungsmodus einschalten**.

   Zum Aktivieren des Wartungsmodus für einzelne Maschinen klicken Sie in der Aktionsleiste auf **Maschinen anzeigen**. Wählen Sie eine Maschine aus und klicken Sie in der Aktionsleiste 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** in der Aktionsleiste.

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 nicht auf **Keine Verbindung mit diesem Computer zulassen** festgelegt. Der **Anmeldemodus der Remotehostkonfiguration** wurde auf **Neue Verbindungen zulassen, doch neue Anmeldungen verhindern** oder **Neue Verbindungen zulassen, doch Neuanmeldungen bis zum Neustart des Servers verweigern** festgelegt.

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 linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Gruppe und klicken Sie in der Aktionsleiste auf **Maschinen anzeigen**.
3. Wählen Sie die Maschine und klicken Sie in der Aktionsleiste auf einen der folgenden Einträge:

   - **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

> **Hinweis:**
>
> - Wenn ein Neustartzeitplan auf eine Bereitstellungsgruppe mit aktiviertem Autoscale angewendet wird, werden die enthaltenen Maschinen ausgeschaltet und von Autoscale neu eingeschaltet.
> - Wenn Neustartzeitpläne auf zufällige Maschinen mit Einzelsitzungs-OS angewendet werden, werden diese Maschinen ausgeschaltet und nicht neu gestartet, um Kosten zu sparen. Wir empfehlen die Verwendung von Autoscale zum Einschalten von Maschinen.
> - Durch das Ändern der Zeitzone für eine Bereitstellungsgruppe kann ein Neustart der darin enthaltenen Maschinen ausgelöst werden. Um Probleme zu vermeiden, ändern Sie die Zeitzoneneinstellungen außerhalb der Produktionszeiten.

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 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.

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 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 linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und klicken Sie in der Aktionsleiste auf **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

**Hinzufügen (Anwenden) von Tags** Wenn Sie einen Neustartzeitplan mit einer Tagbeschränkung konfigurieren, vergewissern Sie sich, dass das Tag den Maschinen hinzugefügt wird, auf die der Zeit-

plan 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 linken Bereich **Bereitstellungsgruppen**.
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 in der Aktionsleiste 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 linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und klicken Sie in der Aktionsleiste auf **Bearbeiten**.
3. Klicken Sie auf der Seite **Neustartzeitplan** auf **Hinzufügen**.
4. Führen Sie auf der Seite **Neustartzeitplan** folgende Schritte aus:

    - Aktivieren Sie **Ja**, um den Zeitplan zu aktivieren. Wählen Sie **Nein**, um den Zeitplan zu deaktivieren.
    - Geben Sie einen Namen und eine Beschreibung für den Zeitplan ein.
    - Wenden Sie für **Auf Tag beschränken** eine Tagbeschränkung an.
    - Wählen Sie für **Maschinen im Wartungsmodus einschließen** aus, ob solche Maschinen in dem Zeitplan enthalten sein sollen. Informationen zur Verwendung von PowerShell finden Sie unter Geplante Neustarts für Maschinen im Wartungsmodus.
    - Legen Sie unter **Neustartintervall** fest, wie oft der Neustart durchgeführt werden soll: täglich, wöchentlich, monatlich oder einmal. Wenn Sie **Wöchentlich** oder **Monatlich** auswählen, können Sie einen oder mehrere Tage festlegen.
    - Geben Sie für **Wiederholung alle** an, wie oft der Zeitplan ausgeführt werden soll.
    - Geben Sie für **Startdatum** ein Startdatum für den Zeitplan an.
    - Wählen Sie unter **Neustart beginnen um** eine Uhrzeit für den Neustart im 24-Stunden-Format aus.

- Option **Neustartdauer**:
  - Wenn Sie keinen natürlichen Neustart wünschen, wählen Sie **Alle Maschinen gleichzeitig neu starten** oder **Alle Maschinen innerhalb von …Minuten neu starten**.
  - Wenn Sie einen natürlichen Neustart wünschen, wählen Sie **Alle Maschinen nach dem Draining der Sitzungen neu starten**.

    Beim Inkrafttreten eines für den natürlichen Neustart konfigurierten Neustartzeitplans geschieht Folgendes:

    * Alle inaktiven Maschinen, die zur Bereitstellungsgruppe gehören, werden sofort neu gestartet.
    * Jede Maschine in einer Bereitstellungsgruppe mit einer oder mehreren aktiven Sitzungen wird neu gestartet, wenn alle Sitzungen abgemeldet sind.

    > **Hinweis:**
    >
    > Sie können diese Option für energieverwaltete und nicht energieverwaltete Maschinen verwenden.

- Wählen Sie unter **Benachrichtigung an Benutzer senden** aus, ob auf den betroffenen Maschinen eine Meldung angezeigt werden soll, bevor der Neustart beginnt. Standardmäßig 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 einen Countdown bis zum Neustart enthalten soll, verwenden Sie die Variable **%m%**. Sofern Sie keinen gleichzeitigen Neustart aller Maschinen festgelegt haben, wird die Meldung auf jeder Maschine zu der richtigen Zeit angezeigt.

5. Klicken Sie auf **Fertig**, um die Konfigurationsänderungen anzuwenden und das Fenster **Neustartzeitplan hinzufügen** zu schließen.
6. Klicken Sie auf **Anwenden**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt. Alternativ klicken Sie auf **Speichern**, um die Konfigurationsänderungen anzuwenden und das Fenster zu schließen.

**Neustart nach Draining** Die Neustartdauer kann auch festgelegt werden, wenn Sie mit PowerShell einen Maschinenneustart planen bzw. ändern (`New-BrokerRebootSchedulev2` oder `Set-BrokerRebootSchedulev2`).

Wenn Sie das Feature "Neustart nach Draining"mit dem Parameter -UseNaturalReboot <Boolean> definieren, werden alle Maschinen nach dem Draining aller Sitzungen neu gestartet. Bei Erreichen der Neustartzeit werden Maschinen in den Drainingzustand versetzt und neu gestartet, sobald alle Sitzungen abgemeldet sind.

Das Feature wird für Bereitstellungsgruppen mit Einzelsitzungs- und Multisitzungs-Maschinen unterstützt. Sie können diese Option für energieverwaltete und nicht energieverwaltete Maschinen verwenden.

In einer On-Premises-Umgebung wird dieses Feature nur bei Verwendung von PowerShell unterstützt. Das Feature ist in Web Studio nicht verfügbar.

#### Bearbeiten, Entfernen, Aktivieren und Deaktivieren von Neustartzeitplänen

1. Wählen Sie im linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und klicken Sie in der Aktionsleiste auf **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) geplant. Ein Ausfall der Standortdatenbank tritt eine Stunde vor Beginn des geplanten Neustarts (um 2:00 Uhr) auf. Der Ausfall dauert sechs Stunden (bis 08:00 Uhr). Der Neustartzeitplan beginnt, wenn die Verbindung zwischen dem Delivery Controller und der Standortdatenbank wiederhergestellt ist. Der VDA-Neustart beginnt nun fünf Stunden nach dem ursprünglichen Zeitplan und somit während der Produktion.

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 oder hat er einen Null-Wert, 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 Web Studio konfigurieren.

#### Geplante Neustarts für Maschinen im Wartungsmodus

> **Hinweis:**
>
> Dieses Feature ist nur über PowerShell verfügbar. Die Option `IgnoreMaintenanceMode` wird ab Citrix Virtual Apps and Desktops 7 2006 unterstützt.

Wenn Sie angeben möchten, ob sich ein Neustartzeitplan auf Maschinen auswirkt, die sich im Wartungsmodus befinden, verwenden Sie die Option `IgnoreMaintenanceMode` mit `BrokerRebootScheduleV2`-Cmdlets.

Das folgende Cmdlet erstellt beispielsweise einen Zeitplan, der Maschinen neu startet, die im Wartungsmodus sind (zusätzlich zu Maschinen, die nicht im Wartungsmodus sind).

```
New-Brokerrebootschedulev2 rebootSchedule1 -DesktopGroupName <myDesktopGroup
> -IgnoreMaintenanceMode $true
```

Mit dem folgenden Cmdlet wird ein vorhandener Neustartzeitplan geändert.

```
Set-Brokerrebootschedulev2 rebootSchedule1 -IgnoreMaintenanceMode
$true
```

Weitere Informationen finden Sie in der Hilfe zum Cmdlet. Dieses Feature ist nur über PowerShell verfügbar.

#### Lastverwaltete 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 nicht verfügbar ist.

  Sie können den Lastindex in Director (Überwachung), über die Suche in Web 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.

#### Energieverwaltete 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.

  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 linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und klicken Sie in der Aktionsleiste 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 **Speichern**, 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 mussten VDI-Maschinen beim Übergang in einen Zeitraum, in dem eine Aktion (Trennaktion = **Anhalten** oder **Herunterfahren**) erforderlich war, eingeschaltet bleiben. 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"

Weitere Informationen zur Trennaktion der Energierichtlinie 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*) fest, wodurch das vorherige Verhalten aktiviert wird. 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.

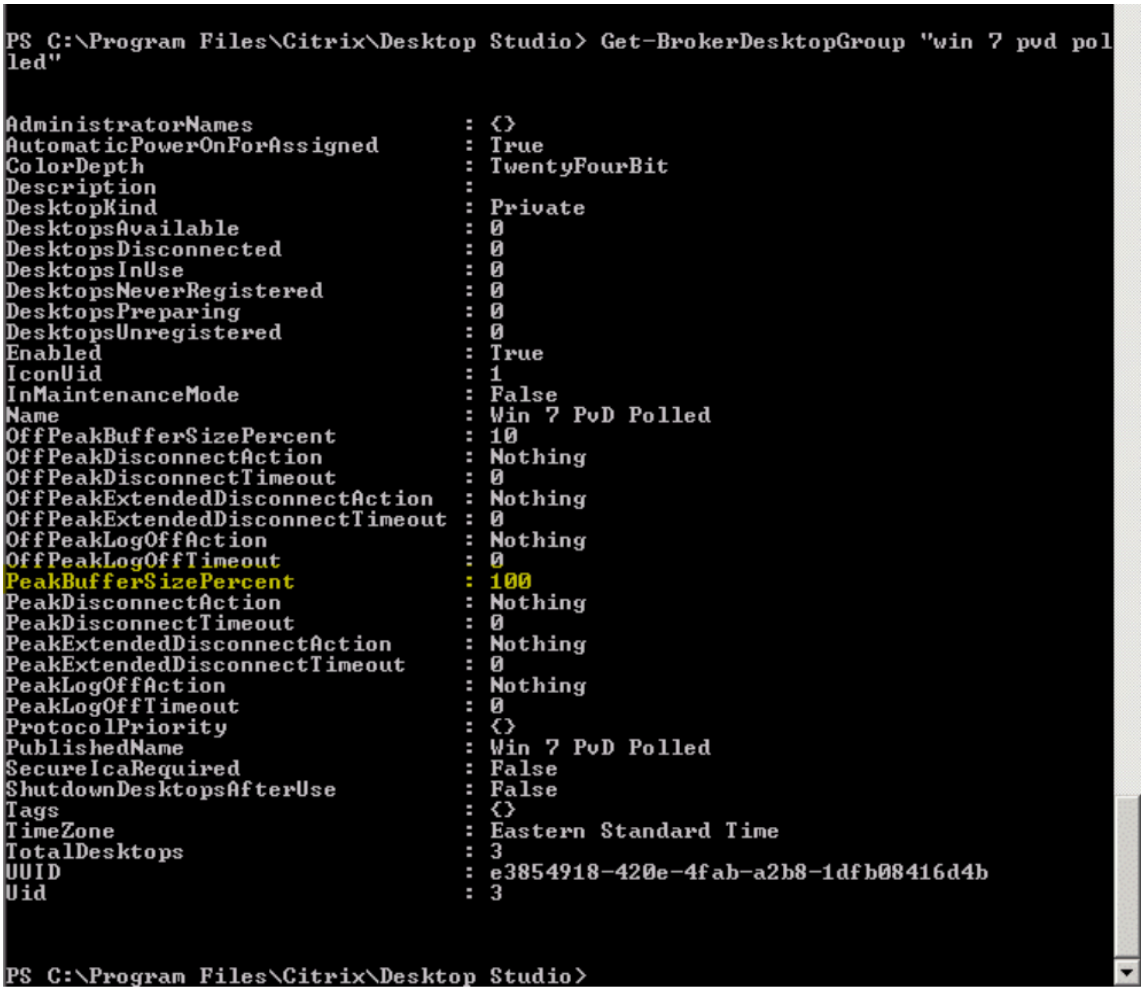
   ```
   asnp Citrix*

   # 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
- Wiederverbinden von Sitzungen nach der Trennung von einer Maschine im Wartungsmodus
- Sitzungsroaming konfigurieren

### Abmelden oder Trennen einer Sitzung

1. Wählen Sie im linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und dann in der Aktionsleiste **Maschinen anzeigen**.
3. Wählen Sie im mittleren Bereich die Maschine, wählen Sie in der Aktionsleiste 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 von einer Sitzung wählen Sie in der Aktionsleiste 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 in der Aktionsleiste 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 linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und dann in der Aktionsleiste **Maschinen anzeigen**.
3. Wählen Sie im mittleren Bereich die Maschine, an die Sie eine Nachricht senden möchten.
4. Wählen Sie in der Aktionsleiste die Option **Sitzungen anzeigen**.
5. Wählen Sie im mittleren Bereich alle Sitzungen aus und wählen Sie in der Aktionsleiste 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.

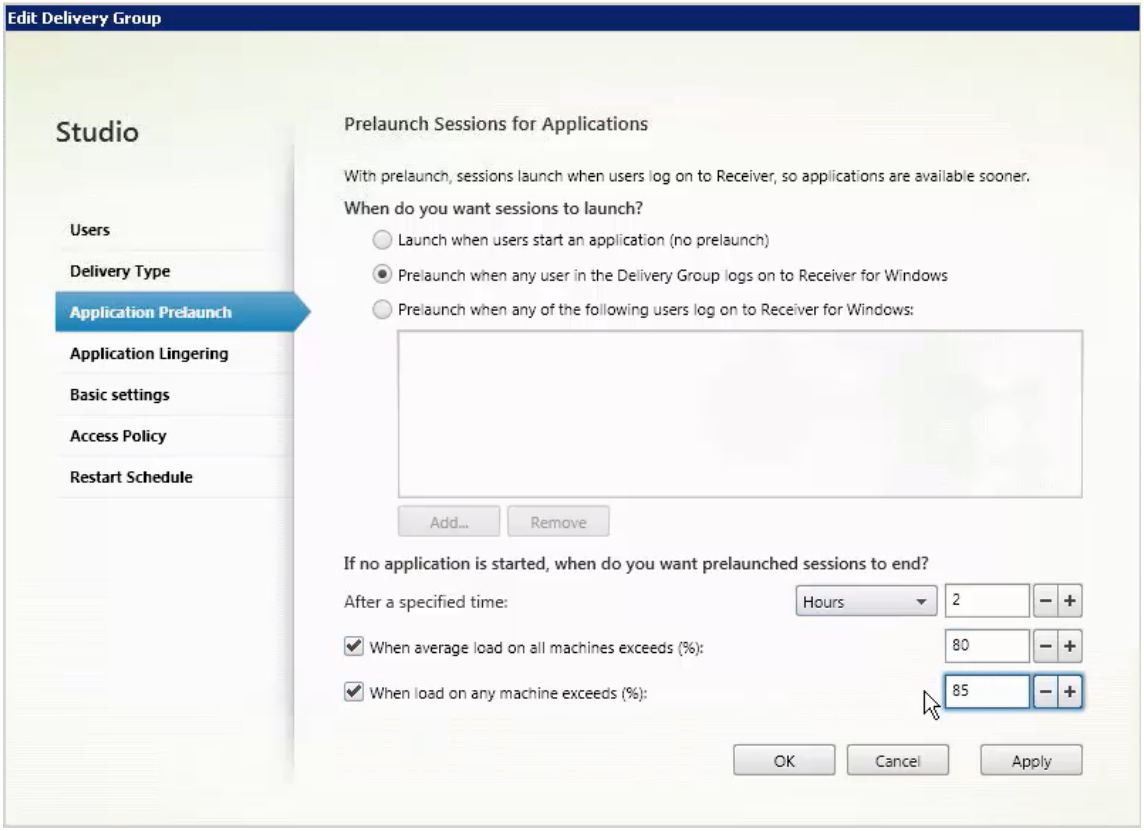
  Sie können zwei Schwellenwerte konfigurieren: die durchschnittliche Last aller Server der Bereitstellungsgruppe und die höchste Last eines Servers in der Bereitstellungsgruppe (beides in Prozent). Wird ein Schwellenwert überschritten, werden jeweils die Sitzungen beendet, die sich am längsten im Zustand “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 eine Bereitstellungsgruppe und klicken Sie in der Aktionsleiste auf **Bereitstellungsgruppe bearbeiten**.
2. 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.




3. 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.

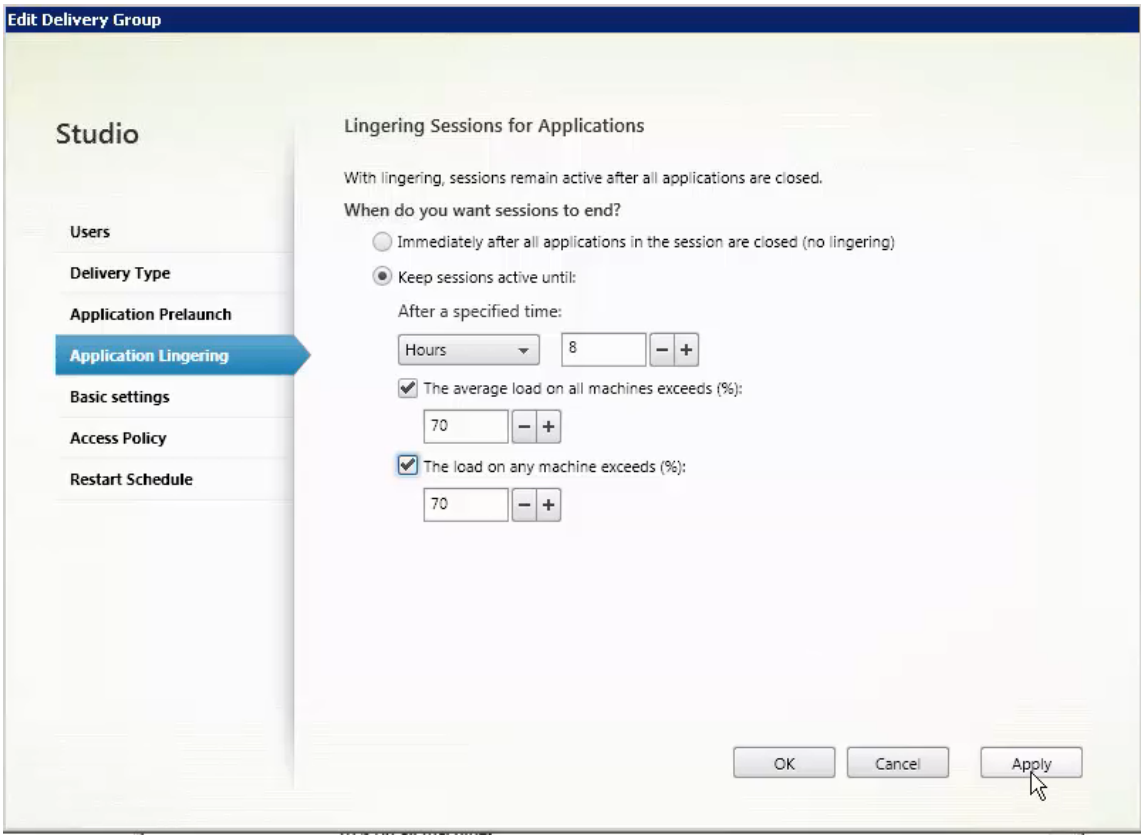
    Eine vorab gestartete Sitzung bleibt also bis zum Eintreten eines der folgenden Ereignisse aktiv: ein Benutzer startet eine Anwendung, das vorgegebene Zeitintervall läuft ab oder der angegebene Lastschwellenwert wird überschritten.

**Aktivieren des Sitzungsfortbestehens**

1. Wählen Sie im linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und klicken Sie in der Aktionsleiste 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.

**Wiederverbinden von Sitzungen nach der Trennung von einer Maschine im Wartungsmodus**

> **HINWEIS:**
>
> Dieses Feature ist nur über PowerShell verfügbar.

Legen Sie fest, ob Sitzungen, die von Maschinen im Wartungsmodus getrennt wurden, sich erneut mit Maschinen in der Bereitstellungsgruppe verbinden dürfen.

Vor Version 2106 war das Wiederverbinden von Sitzungen, die von Maschinen im Wartungsmodus getrennt wurden, auf gepoolten Einzelsitzungsdesktops nicht zulässig. Ab Version 2106 kann eine konfigurierte Bereitstellungsgruppe das Wiederverbinden (unabhängig vom Sitzungstyp) nach der Trennung von einer Maschine im Wartungsmodus zulassen oder verhindern.

Beim Erstellen oder Bearbeiten einer Bereitstellungsgruppe (`New-BrokerDesktopGroup`, `Set-BrokerDesktopGroup`) können Sie mit dem Parameter `-AllowReconnectInMaintenanceMode <boolean>` das Wiederherstellen der Verbindung zu einer Maschine im Wartungsmodus zulassen oder verhindern.

- Wenn der Wert auf "true"festgelegt ist, können Sitzungen sich erneut mit Maschinen in der Gruppe verbinden.
- Wenn der Wert auf "false"festgelegt ist, können Sitzungen die Verbindung zu Maschinen in der Gruppe nicht wiederherstellen.

Standardwerte:

- Einzelsitzung: Deaktiviert
- Multisitzung: Aktiviert

#### Sitzungsroaming konfigurieren

Das Sitzungsroaming ist standardmäßig für Bereitstellungsgruppen aktiviert. Sitzungen wechseln 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 gleichzeitig auf beiden Geräten zur Verfügung. Sie können die Anwendungen auf mehreren Geräten anzeigen. Die Anwendungen folgen dem Benutzer unabhängig von dem Gerät und davon, ob aktuelle Sitzungen vorhanden sind. Oft folgen auch Drucker und andere Ressourcen, die einer Anwendung zugewiesen sind. Alternativ können Sie auch PowerShell verwenden. Weitere Informationen finden Sie unter Sitzungsroaming.

**Sitzungsroaming für Anwendungen konfigurieren** Führen Sie folgende Schritte aus, um das Sitzungsroaming für Anwendungen zu konfigurieren:

1. Wählen Sie links in der Konsole **Bereitstellungsgruppen**.

2. Wählen Sie eine Bereitstellungsgruppe und dann in der Aktionsleiste **Bereitstellungsgruppe bearbeiten**.
3. Aktivieren Sie auf der Seite **Benutzer** das Kontrollkästchen **Sitzungen wechseln mit Benutzern, wenn sie Geräte wechseln**, um das Sitzungsroaming zu aktivieren.

    - Wenn diese Option aktiviert ist, wird auf beiden Geräten die gleiche Sitzung verwendet und angezeigt, wenn ein Benutzer eine Anwendungssitzung startet und dann mit einem anderen Gerät weiterarbeitet. Wenn die Option deaktiviert ist, wechselt die Sitzung nicht mehr zu anderen Geräten.

4. Wählen Sie **OK**, um die Konfigurationsänderungen anzuwenden und das Fenster zu schließen.

**Sitzungsroaming für Desktops konfigurieren** Führen Sie folgende Schritte aus, um das Sitzungsroaming für einen Desktop zu konfigurieren:

1. Wählen Sie links in der Konsole **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und dann in der Aktionsleiste **Bearbeiten**.
3. Wählen Sie auf der Seite **Desktops** den Desktop und wählen Sie dann **Bearbeiten**.
4. Aktivieren Sie das Kontrollkästchen **Sitzungsroaming**, um das Sitzungsroaming zu ermöglichen.

- Wenn diese Option aktiviert ist, wird die gleiche Sitzung verwendet und die Anwendungen stehen auf beiden Geräten zur Verfügung, wenn ein Benutzer eine Sitzung startet und dann mit einem anderen Gerät weiterarbeitet. Wenn die Option deaktiviert ist, wechselt die Sitzung nicht mehr zu anderen Geräten.

Wählen Sie **OK**, um die Konfigurationsänderungen anzuwenden und das Fenster zu schließen.

## 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 können, 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**.

## Anwendungsgruppen erstellen

June 27, 2024

> **Hinweis:**
>
> Sie können Ihre Citrix Virtual Apps and Desktops-Bereitstellung mithilfe von zwei Verwaltungskonsolen verwalten: Web Studio (webbasiert) und Citrix Studio (Windows-basiert). Dieser Artikel behandelt nur Web Studio. Informationen zu Citrix Studio finden Sie im entsprechenden Artikel in Citrix Virtual Apps and Desktops 7 2212 oder früher.

### Einführung

Über Anwendungsgruppen können Sie Anwendungssammlungen verwalten. Erstellen Sie Anwendungsgruppen für Anwendungen, die in verschiedenen Bereitstellungsgruppen verwendet werden. Oder Sie erstellen Anwendungen, die von einer Benutzerteilgruppe innerhalb einer Bereitstellungsgruppe verwendet. Anwendungsgruppen sind optional. Sie bieten eine Alternative zum Hinzufügen derselben Anwendungen zu mehreren Bereitstellungsgruppen. Sie können Bereitstellungsgruppen mehreren Anwendungsgruppen und eine Anwendungsgruppe mehreren Bereitstellungsgruppen zuordnen.

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).

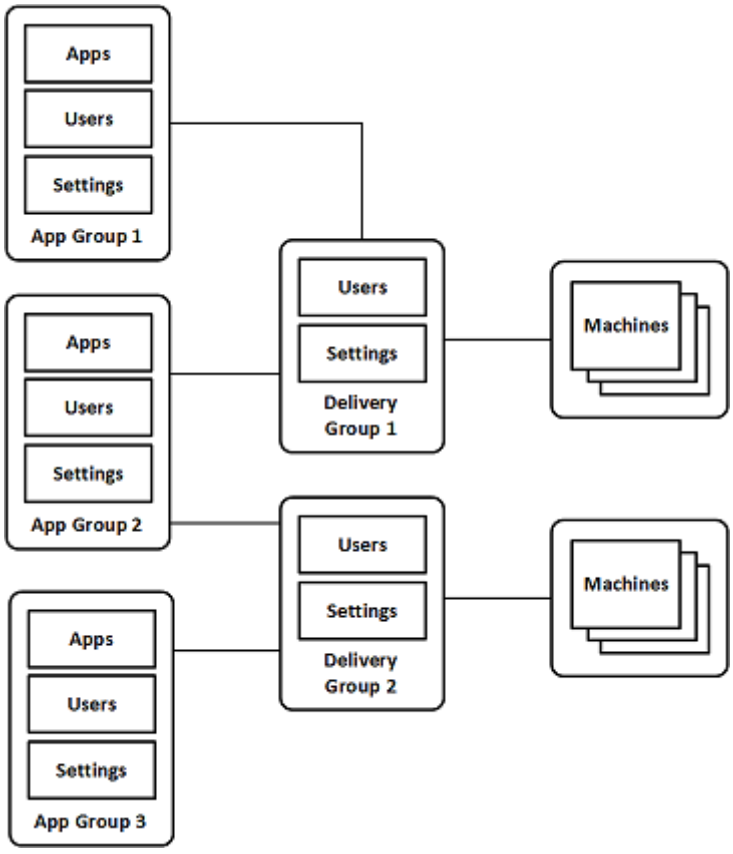
 

- Die Sitzungsfreigabe zwischen den Anwendungsgruppen kann Ressourcen sparen. In anderen Fällen ist das Deaktivieren der Sitzungsfreigabe zwischen Anwendungsgruppen möglicherweise nützlich.
- Mit der Tagbeschränkung können Sie Anwendungen aus einer Anwendungsgruppe nur auf einigen Maschinen in den ausgewählten 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 wer-

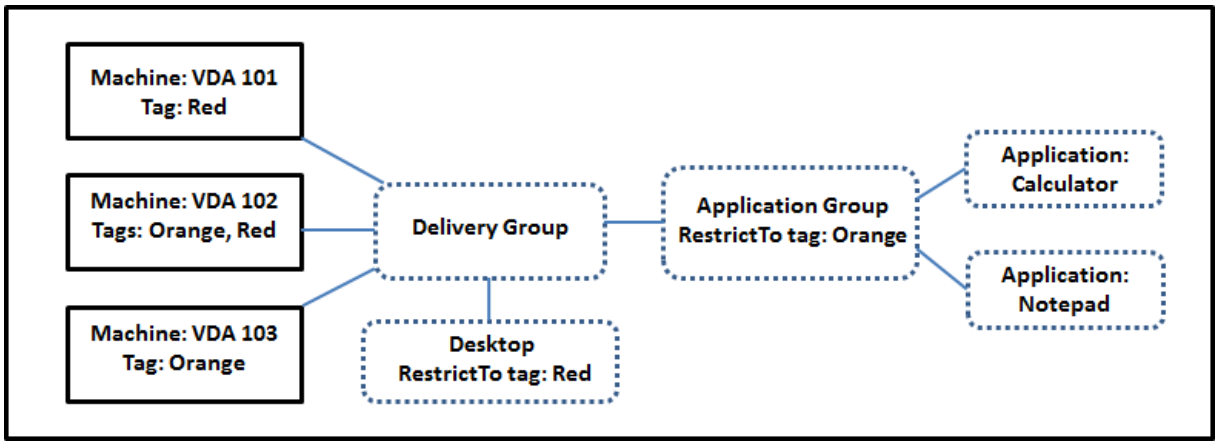
den. (Obwohl dies nicht ausgezeichnet ist, sind die Maschinen in Maschinenkatalogen.)

Anwendungsgruppe 1 ist Bereitstellungsgruppe 1 zugeordnet. Der Zugriff auf die Anwendungen in Anwendungsgruppe 1 erfolgt durch die Benutzer in Anwendungsgruppe 1. Diese Gruppen werden nur angezeigt, wenn sie auch in der Benutzerliste für Bereitstellungsgruppe 1 sind. Diese Konfiguration folgt der Leitlinie, dass die Benutzerliste einer Anwendungsgruppe eine Teilgruppe (d. h. Einschränkung) der Benutzerlisten der zugeordneten Bereitstellungsgruppen ist. 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 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 wird in Anwendungsgruppe 2 eine Priorität zugewiesen, welche die Reihenfolge vorgibt, in der die Bereitstellungsgruppen beim Starten einer Anwendung geprüft werden. Für Bereitstellungsgruppen mit der gleichen Priorität findet ein Lastausgleich statt. Der Zugriff auf die Anwendungen in Anwendungsgruppe 2 erfolgt durch die Benutzer in Anwendungsgruppe 2. Diese müssen jedoch auch in den Benutzerlisten für Bereitstellungsgruppe 1 und Bereitstellungsgruppe 2 erscheinen.

**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. Die enthaltenen Anwendungen werden nur auf Maschinen in dieser Bereitstellungsgruppe mit dem Tag “Orange”, VDA 102 und 103, gestartet.

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. Dieser Prozess 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 Artikel geht es um das Zuordnen von Anwendungen zu mehreren Anwendungsgruppen. Das Hinzufügen von Instanzen der Anwendung aus einer verfügbaren Quelle ist etwas anderes. 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 weitere Sitzungen und ermöglicht die Verwendung von Anwendungsfeatures, wie Kopieren und Einfügen, welche die Zwischenablage erfordern. In manchen Situationen können Sie die Sitzungsfreigabe 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:**

  Eine Konfiguration mit Anwendungen mit schlechter Interoperabilität mit anderen, auf denselben Maschinen installierten Anwendungen. Ein Beispiel wären zwei Versionen einer Software oder zwei Versionen eines Webbrowsers. Sie möchten nicht, dass ein Benutzer beide Versionen in derselben Sitzung startet.

  Erstellen Sie 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. Sie können gleichzeitig andere Anwendungen ausführen, jedoch nicht in der gleichen Sitzung. Wenn ein Benutzer eine der in mehreren Versionen vorliegenden Anwendungen 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 bestehenden Sitzungen auf der Maschine über die Sitzungsfreigabe gestartet.

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.

Die Anwendungssitzungsfreigabe wird beim Erstellen von Anwendungsgruppen standardmäßig aktiviert. Diese Einstellung 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. Melden Sie sich bei Web Studio an.
2. Wählen Sie im linken Bereich **Anwendungen** und dann die Registerkarte **Anwendungsgruppen**.
3. Um Anwendungsgruppen mithilfe von Ordnern zu organisieren, erstellen Sie die Ordner im Stammordner **Anwendungsgruppen**.
4. Wählen Sie den Ordner aus, in dem Sie die Gruppe erstellen möchten, und klicken Sie auf **Anwendungsgruppe erstellen**. Der Assistent zum Erstellen von Gruppen wird gestartet und es erscheint eine **Einführungsseite**. Sie können die Seite bei zukünftigen Starts des Assistenten ausblenden.

5. Konfigurieren Sie im Assistenten die Einstellungen auf den unten beschriebenen Seiten. Wenn Sie mit einer Seite fertig sind, wählen Sie jeweils **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 die Anwendungsbenutzer in der Anwendungsgruppe an. Geben Sie entweder alle Benutzer und Gruppen in den Bereitstellungsgruppen an, die Sie auf der vorherigen Seite ausgewählt haben, oder wählen Sie bestimmte Benutzer bzw. Benutzergruppen aus den Bereitstellungsgruppen aus. Wenn Sie die Benutzer einschränken, haben nur die in der Bereitstellungsgruppe und der Anwendungsgruppe angegebenen Benutzer Zugriff auf die Anwendungen in der Gruppe. 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 im Ordner **Anwendungen** abgelegt. Sie können einen anderen Ordner angeben. Wenn Sie eine Anwendung hinzufügen und es dort 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 Web 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 das Dropdownmenü **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 **App-V**-Server oder **Anwendungsbibliothek** auswählen. Aktivieren Sie dort die Kontrollkästchen der gewünschten Anwendungen und klicken Sie auf **OK**. Weitere Informationen finden Sie unter App-V-Anwendungen bereitstellen. 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 im Dropdownmenü **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 **Fertigstellen**.

# Anwendungsgruppen verwalten

June 27, 2024

> **Hinweis:**
>
> Sie können Ihre Citrix Virtual Apps and Desktops-Bereitstellung mithilfe von zwei Verwaltungskonsolen verwalten: Web Studio (webbasiert) und Citrix Studio (Windows-basiert). Dieser Artikel behandelt nur Web Studio. Informationen zu Citrix Studio finden Sie im entsprechenden Artikel in Citrix Virtual Apps and Desktops 7 2212 oder früher.

## 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 explizit 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. Diese Konfiguration können Sie bei der Erstellung der Gruppe nicht ändern.

1. Wählen Sie im linken Bereich **Anwendungen** und dann die Registerkarte **Anwendungsgruppen**.
2. Wählen Sie eine Anwendungsgruppe und dann in der Aktionsleiste **Anwendungsgruppe bearbeiten**.
3. Aktivieren oder deaktivieren Sie auf der Seite **Einstellungen** das Kontrollkästchen **Anwendungsgruppe aktivieren**.
4. Klicken Sie auf **Anwenden**, damit das Fenster geöffnet bleibt, oder klicken Sie auf **Speichern**, 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. Diese Konfiguration können Sie bei der Erstellung der Gruppe nicht ändern. Weitere Informationen finden Sie unter Sitzungsfreigabe zwischen Anwendungsgruppen.

1. Wählen Sie im linken Bereich **Anwendungen** und dann die Registerkarte **Anwendungsgruppen**.
2. Wählen Sie eine Anwendungsgruppe und dann in der Aktionsleiste **Anwendungsgruppe bearbeiten**.
3. Aktivieren oder deaktivieren Sie auf der Seite **Einstellungen** das Kontrollkästchen **Sitzungsfreigabe zwischen Anwendungsgruppen aktiviert**.
4. Klicken Sie auf **Anwenden**, damit das Fenster geöffnet bleibt, oder klicken Sie auf **Speichern**, 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 ist dies vorteilhaft. 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.

Verwenden Sie das PowerShell-SDK, um die Anwendungssitzungsfreigabe für alle Anwendungen in einer Anwendungsgruppe zu deaktivieren oder eine Gruppe mit deaktivierter Sitzungsfreigabe erstellen.

#### PowerShell-Cmdlet-Beispiele

Verwenden Sie zum Deaktivieren der Sitzungsfreigabe die Broker PowerShell-Cmdlets `New-BrokerApplicationGroup` oder `Set-BrokerApplicationGroup` und legen Sie den Parameter `SessionSharingEnabled` auf `False` und den Parameter `SingleAppPerSession` auf `True` fest.

- 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 linken Bereich **Anwendungen** und dann die Registerkarte **Anwendungsgruppen**.
2. Wählen Sie eine Anwendungsgruppe und dann in der Aktionsleiste **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 linken Bereich **Anwendungen** und dann die Registerkarte **Anwendungsgruppen**.
2. Wählen Sie eine Anwendungsgruppe und dann in der Aktionsleiste **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 **Speichern**, 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 linken Bereich **Anwendungen** und dann die Registerkarte **Anwendungsgruppen**.
2. Wählen Sie eine Anwendungsgruppe und dann in der Aktionsleiste **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 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 **Speichern**, 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 linken Bereich **Anwendungen** und dann die Registerkarte **Anwendungsgruppen**.
2. Wählen Sie eine Anwendungsgruppe und dann in der Aktionsleiste **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 **Speichern**, damit die Änderungen angewendet werden und das Fenster geschlossen wird.

### Hinzufügen, Ändern oder Entfernen eines Anwendungssymbols in einer Anwendungsgruppe

Führen Sie die folgenden Schritte aus, um ein Anwendungssymbol hinzuzufügen, zu ändern oder zu entfernen.

1. Wählen Sie im linken Bereich **Anwendungen**.
2. Wählen Sie auf der Registerkarte **Anwendungen** eine Anwendung und dann **Eigenschaften**.

   Um Änderungen auf Anwendungsgruppenebene vorzunehmen, navigieren Sie zur Registerkarte **Anwendungsgruppen**, wählen Sie eine Anwendung in einer Gruppe aus und wählen Sie **Eigenschaften**.
3. Wählen Sie die Seite **Bereitstellung** und dann **Ändern**. Das Fenster **Symbol auswählen** wird angezeigt.
4. Führen Sie im Fenster **Symbol auswählen** einen der folgenden Schritte aus:

   - Um ein Symbol hinzuzufügen, wählen Sie **Hinzufügen** und navigieren dann zum Symbol.
   - Um ein Symbol zu entfernen, wählen Sie es aus und wählen dann **Entfernen**.
   - Um ein Symbol zu ändern, wählen Sie es für die Anwendung aus.

   > **Wichtig:**
   >
   > - Sie können kein Symbol hinzufügen, das größer als 200 KB ist.
   > - Sie können nur ICON-Dateien hinzufügen.
   > - Sie können keine integrierten Symbole entfernen.
   > - Sie können kein Symbol einer aktuell verwendeten Anwendung entfernen.
5. Wählen Sie **Speichern**, um die Konfigurationsänderungen anzuwenden und das Fenster zu schließen.

### 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 linken Bereich **Anwendungen** und dann die Registerkarte **Anwendungsgruppen**.
2. Wählen Sie eine Anwendungsgruppe und dann in der Aktionsleiste **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 **Speichern**, 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 linken Bereich **Anwendungen** und dann die Registerkarte **Anwendungsgruppen**.
2. Wählen Sie eine Anwendungsgruppe und dann in der Aktionsleiste **Anwendungsgruppe bearbeiten**.
3. Wählen Sie die Seite **Geltungsbereiche**. Aktivieren oder deaktivieren Sie das Kontrollkästchen neben den Geltungsbereichen, die Sie ändern möchten.
4. Wählen Sie **Anwenden**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt, oder wählen Sie **Speichern**, 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 linken Bereich **Anwendungen** und dann die Registerkarte **Anwendungsgruppen**.
2. Wählen Sie eine Anwendungsgruppe und dann in der Aktionsleiste **Gruppe löschen**.
3. Bestätigen Sie die Löschung, wenn Sie dazu aufgefordert werden.

### Anwendungsgruppen mit Ordnern organisieren

Sie können Ordner erstellen, um den Zugriff auf Anwendungsgruppen zu vereinfachen.

### Erforderliche Rollen

Standardmäßig können Sie Anwendungsgruppenordner erstellen und verwalten, wenn Sie eine der folgenden integrierten Rollen haben:

- Cloudadministrator
- Volladministrator
- Administrator der Anwendungsgruppe

Sie können benutzerdefinierte Rollen erstellen, um Verwaltungsaktionen an andere Benutzer zu delegieren. In der folgenden Tabelle sind die für jede Aktion erforderlichen Berechtigungen aufgeführt.

| Aktion | Erforderliche Berechtigungen |
|---|---|
| Anwendungsgruppenordner erstellen | Anwendungsgruppenordner erstellen |
| Anwendungsgruppenordner löschen | Anwendungsgruppenordner entfernen |
| Anwendungsgruppenordner verschieben | Anwendungsgruppenordner verschieben |
| Anwendungsgruppenordner umbenennen | Anwendungsgruppenordner bearbeiten |
| Anwendungsgruppen in Ordner verschieben | Anwendungsgruppenordner bearbeiten, Anwendungsgruppeneigenschaften bearbeiten |

Weitere Informationen finden Sie unter Erstellen und Verwalten von Rollen.

### Ordner erstellen und verwalten

Sie können Anwendungsgruppenordner mit der Aktionsleiste oder dem Rechtsklickmenü erstellen und verwalten. Darüber hinaus können Sie eine Anwendungsgruppe oder einen Ordner an die gewünschte Stelle in der Ordnerstruktur ziehen.

Nützliche Info:

- Sie können Ordner bis zu fünf Ebenen tief verschachteln (mit Ausnahme des Standardstammordners).
- Ein Ordner kann Anwendungsgruppen und Unterordner enthalten. Sie können einen Ordner nur dann löschen, wenn er und seine Unterordner keine Anwendungsgruppen enthalten.
- Alle Knoten (z. B. Maschinenkataloge, Bereitstellungsgruppen, Anwendungen und Anwendungsgruppen) nutzen dieselbe Ordnerstruktur im Back-End. Um Namenskonflikte mit anderen Ressourcenordnern beim Umbenennen oder Verschieben von Ordnern zu vermeiden, empfehlen wir, Ordner der ersten Ebene in verschiedenen Ordnerstrukturen unterschiedlich zu benennen.

# Remote-PC-Zugriff

June 27, 2024

> **Hinweis:**
>
> Sie können Ihre Citrix Virtual Apps and Desktops-Bereitstellung mithilfe von zwei Verwaltungskonsolen verwalten: Web Studio (webbasiert) und Citrix Studio (Windows-basiert). Dieser Artikel behandelt nur Web Studio. Informationen zu Citrix Studio finden Sie im entsprechenden Artikel in Citrix Virtual Apps and Desktops 7 2212 oder früher.

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. Standardmäßig weisen wir der nächsten nicht zugewiesenen Maschine automatisch mehrere Benutzer zu. Um die automatische Zuweisung auf einen einzelnen Benutzer zu beschränken, melden Sie sich bei Web Studio an, gehen Sie zu **Einstellungen** und deaktivieren Sie die Einstellung **Automatische Zuweisung mehrerer Benutzer für Remote-PC-Zugriff aktivieren**.

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 DaaS (ehemals 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.

> **Hinweis:**
>
> Beim Definieren des Remote-PC-Zugriffs müssen Sie die Anzahl der physischen Monitore beachten, die mit der GPU auf dem Remote PC verbunden und derzeit konfiguriert/betriebsbereit sind. Selbst wenn ein Monitor nicht in der Citrix-Sitzung verwendet wird, wird er bei der Anzahl der maximal von der GPU unterstützten Monitore mitgezählt, wenn er vom Grafikprozessor erkannt wird.

### Überlegungen zum Maschinenkatalog

Die Art des erforderlichen Maschinenkatalogs hängt vom Anwendungsfall ab:

- Maschinenkatalog für Remote-PC-Zugriff
  - Dedizierte Windows-PCs
  - Dedizierte Windows-Mehrbenutzer-PCs Dieser Anwendungsfall gilt für physische PCs im Büro, auf die mehrere Benutzer in verschiedenen Schichten remote zugreifen können.
  - Gepoolte Windows-PCs. Dieser Anwendungsfall betrifft physische PCs, auf die mehrere beliebige Benutzer zugreifen können (z. B. in Computerräumen).
- Einzelsitzungs-OS-Maschinenkatalog
  - Statisch - Dedizierte Linux-PCs
  - Zufällig —gepoolte 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 automatische Benutzerzuweisung ist für Linux-Maschinen nicht verfügbar.
- Wenn Benutzer bereits lokal an ihren PCs angemeldet sind, schlagen Versuche, die PCs über StoreFront zu starten, fehl.
- Energiesparoptionen sind für Linux-Maschinen nicht verfügbar.

### 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.
  - Dual-Boot-Maschinen.
- 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 und Windows 11 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/physicalmachine` verwenden. Dadurch wird das gleiche Ergebnis erzielt, wie mit dem VDA-Kerninstallationsprogramm.

     > **Hinweis:**
     >
     > Verwenden Sie für die RemotePC-Installation das Argument `/physicalmachine` mit `/remotepc`, damit der VDA sich in bestimmten Benutzerszenarien wie erwartet verhält.

   - 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 Management 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. Erstellen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

### Deaktivieren von automatischen Zuweisungen mehrerer Benutzer

Fügen Sie auf jedem Delivery Controller folgende Registrierungseinstellung hinzu:

`HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer`

- Name: AllowMultipleRemotePCAssignments
- Typ: DWORD
- Wert: 0

### Energiesparmodus (mindestens Version 7.16)

Damit eine Maschine mit Remote-PC-Zugriff in den Energiesparmodus wechseln kann, fügen Sie dem VDA folgende Registrierungseinstellung hinzu und starten die Maschine dann neu. Nach dem Neustart gelten die Energiespareinstellungen des Betriebssystems. Nach Ablauf der konfigurierten Leerlaufzeit wechselt die Maschine dann in den Energiesparmodus. Wenn die Maschine wieder reaktiviert wird, registriert sie sich erneut beim Delivery Controller.

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Name: DisableRemotePCSleepPreventer

- Typ: DWORD
- Wert: 1

### Sitzungsverwaltung

Standardmäßig wird eine Remotesitzung des Benutzers automatisch getrennt, wenn ein lokaler Benutzer eine Sitzung auf dieser Maschine (durch Drücken von Strg + Alt + Entf) initiiert. Fügen Sie den folgenden Registrierungseintrag auf dem Büro-PC hinzu und starten Sie dann die Maschine neu, um diese automatische Aktion zu verhindern.

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- Name: SasNotification
- Typ: DWORD
- Wert: 1

Standardmäßig erhält der Remotebenutzer Vorzug vor dem lokalen Benutzer, wenn die Verbindungsmeldung nicht innerhalb des Timeouts quittiert wird. Verwenden Sie die folgende Einstellung, um das Verhalten zu konfigurieren:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- Name: RpcaMode
- Typ: DWORD
- Data:
  - 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.

### Protokollierung der Sitzungsverwaltung

Remote-PC-Zugriff kann jetzt Zugriffsversuche auf PCs mit einer aktiven ICA-Sitzung protokollieren. Damit können Sie Ihre Umgebung auf unerwünschte oder unerwartete Aktivitäten überwachen und entsprechende Ereignisse beim Untersuchen von Sie Incidents überprüfen.

Die Protokollierung erfolgt per Windows-Ereignisanzeige in **Anwendungen und Dienste > Citrix > HostCore > ICA-Dienst > Admin**.

Es werden drei Ereignisse bei Verwendung von Remote-PC-Zugriff protokolliert.

#### Strg+Alt+Entf

Dieses Ereignis tritt auf, wenn der lokale Benutzer Strg+Alt+Entf auf der Konsolentastatur mit einer aktiven Remotesitzung drückt.

#### Ereignisdetails

- Protokollname: Anwendungen und Dienste
- Ereignis-ID: 43, 44, 45
- Quelle: ICA-Dienst

**Ereignis-ID 43** Diese Ereignis-ID wird angezeigt, wenn der Registrierungswert “SasNotification” fehlt oder 0 ist.

- Meldung:

```
1          Ctrl+Alt+Del has been pressed on the endpoint.
2          The session management behavior is set to automatically
              disconnect the remote session.
```

**Ereignis-ID 44** Diese Ereignis-ID wird angezeigt, wenn die Registrierungswerte “SasNotification” und “RpcaMode”1 sind oder wenn der Registrierungswert “RpcaMode”fehlt.

- Meldung:

```
1          Ctrl+Alt+Del has been pressed on the endpoint.
2          The session management behavior is set to notify the
               remote user. The user preference is set to remote user
               .
```

**Ereignis-ID 45** Diese Ereignis-ID wird angezeigt, wenn der Registrierungswert "SasNotification"1 und der Registrierungswert "RpcaMode"2 ist.

- Meldung:

```
1          Ctrl+Alt+Del has been pressed on the endpoint.
2          The session management behavior is set to notify the
               remote user.
3          The user preference is set to local user.
```

#### Trennen der Remotesitzung

Dieses Ereignis tritt auf, wenn die Remotesitzung getrennt wurde. Dies kann aus verschiedenen Gründen geschehen.

#### Ereignisdetails

- Protokollname: Anwendungen und Dienste
- Ereignis-ID: 46, 47, 48
- Quelle: ICA-Dienst

**Ereignis-ID 46** Diese Ereignis-ID wird angezeigt, wenn die Remotesitzung getrennt wurde und der Registrierungswert "SasNotification"fehlt oder 0 ist.

- Meldung:

```
1          The remote session for <remoteUserName> has been
               disconnected.
```

**Ereignis-ID 47** Diese Ereignis-ID wird angezeigt, wenn der Remotebenutzer dem Trennen der Sitzung zustimmt und die Registrierungswerte "SasNotification"und "RpcaMode"1 sind oder wenn der Registrierungswert "RpcaMode"2 ist oder fehlt.

- Meldung:

```
The remote session for <remoteUserName> has been
    disconnected because the user accepted the request to
    disconnect the session.
```

**Ereignis-ID 48** Diese Ereignis-ID wird angezeigt, wenn der Remotebenutzer die Anforderung zum Trennen nicht innerhalb des Timeouts ablehnt und der Registrierungswert "SasNotification"1 und der Registrierungswert "RpcaMode"2 ist.

- Meldung:

```
The remote session for <remoteUserName> has been
    disconnected because the user did not decline the
    disconnection request within the configured timeout
    period (<timeout period>).
```

**Strg+Alt+Entf zweimal gedrückt** Dieses Ereignis tritt auf, wenn Strg+Alt+Entf innerhalb von 10 Sekunden zweimal gedrückt wird.

#### Ereignisdetails

- Protokollname: Anwendungen und Dienste
- Ereignis-ID: 49
- Quelle: ICA-Dienst

**Ereignis-ID 49** Diese Ereignis-ID wird angezeigt, wenn Strg+Alt+Entf innerhalb von 10 Sekunden zweimal gedrückt wird.

- Meldung:

```
The remote session for <remoteUserName> has been forcibly
    disconnected.
```

### Wake-On-LAN

Remote-PC-Zugriff unterstützt Wake-On-LAN, sodass physische PCs remote eingeschaltet werden können. Dieses Feature ermöglicht es Benutzern, ihre Büro-PCs ausgeschaltet zu lassen, wenn diese nicht verwendet werden, um Energiekosten zu sparen. Außerdem ist ein Remotezugriff möglich, wenn Maschinen unabsichtlich ausgeschaltet wurden.

Mit dem Wake-On-LAN-Feature werden die Magic Packets auf Befehl des Delivery Controllers direkt vom VDA, der auf dem PC ausgeführt wird, an das Subnetz gesendet, in dem sich der PC befindet.

Dadurch kann das Feature ohne Abhängigkeiten von zusätzlichen Infrastrukturkomponenten oder Drittanbieterlösungen für die Bereitstellung von Magic Packets funktionieren.

Das Wake-On-LAN-Feature unterscheidet sich vom älteren SCCM-basierten Wake-On-LAN-Feature. Weitere Informationen zu SCCM-basiertem Wake-on-LAN finden Sie unter Wake-On-LAN –SCCM-integriert.

### Systemanforderungen

Folgende Systemanforderungen gelten für die Verwendung des Wake-On-LAN-Feature:

- Steuerungsebene:
  - Citrix DaaS
  - Citrix Virtual Apps and Desktops 2009 oder höher
- Physische PCs:
  - VDA Version 2009 oder höher
  - Windows 10 oder Windows 11. Weitere Informationen zur Unterstützbarkeit finden Sie unter VDA-Systemanforderungen.
  - Wake-On-LAN aktiviert in BIOS/UEFI
  - Wake-On-LAN aktiviert in den Eigenschaften des Netzwerkadapters innerhalb der Windows-Konfiguration

### Konfigurieren von Wake-On-LAN

Wenn Sie On-Premises-Citrix Virtual Apps and Desktops verwenden, wird die Konfiguration mit integriertem Wake-On-LAN nur bei Verwendung von PowerShell unterstützt.

Konfigurieren von Wake-On-LAN:

1. Erstellen Sie den Maschinenkatalog für den Remote-PC-Zugriff (falls noch nicht vorhanden).
2. Erstellen Sie die Wake-On-LAN-Hostverbindung (falls noch nicht vorhanden).

   > **Hinweis:**
   >
   > Wenn Sie über eine Hostverbindung vom Typ “Microsoft Configuration Manager Wake-On-LAN”verfügen, erstellen Sie eine neue Hostverbindung, um das Wake-On-LAN-Feature zu verwenden.

3. Rufen Sie den eindeutigen Bezeichner der Wake-On-LAN-Hostverbindung ab.
4. Ordnen Sie die Wake-On-LAN-Hostverbindung einem Maschinenkatalog zu.

Erstellen der Wake-On-LAN-Hostverbindung:

```
# Load Citrix SnapIns
Add-PSSnapIn -Name "*citrix*"

# Provide the name of the Wake on LAN host connection
[string]$connectionName = "Remote PC Access Wake on LAN"

# Create the hypervisor connection
$hypHc = New-Item -Path xdhyp:\Connections `
                -Name $connectionName `
                -HypervisorAddress "N/A" `
                -UserName "woluser" `
                -Password "wolpwd" `
                -ConnectionType Custom `
                -PluginId VdaWOLMachineManagerFactory `
                -CustomProperties "<CustomProperties></CustomProperties
                   >" `
                -Persist

$bhc = New-BrokerHypervisorConnection -HypHypervisorConnectionUid
   $hypHc.HypervisorConnectionUid

# Wait for the connection to be ready before trying to use it
while (-not $bhc.IsReady)
{

    Start-Sleep -s 5
    $bhc = Get-BrokerHypervisorConnection -HypHypervisorConnectionUid
       $hypHc.HypervisorConnectionUid
 }

<!--NeedCopy-->
```

Wenn die Hostverbindung bereit ist, führen Sie die folgenden Befehle aus, um den eindeutigen Bezeichner der Hostverbindung abzurufen:

```
$bhc = Get-BrokerHypervisorConnection -Name "<WoL Connection Name>"
$hypUid = $bhc.Uid
<!--NeedCopy-->
```

Nachdem Sie den eindeutigen Bezeichner der Verbindung abgerufen haben, führen Sie die folgenden Befehle aus, um die Verbindung dem Remote-PC-Zugriff-Maschinenkatalog zuzuordnen:

```
Get-BrokerCatalog -Name "<Catalog Name>" | Set-BrokerCatalog -
   RemotePCHypervisorConnectionUid $hypUid
<!--NeedCopy-->
```

#### Designüberlegungen

Wenn Sie planen, Wake-On-LAN mit Remote-PC-Zugriff zu verwenden, sollten Sie Folgendes beachten:

- Mehrere Maschinenkataloge können dieselbe Wake-On-LAN-Hostverbindung verwenden.
- Damit ein PC einen anderen PC reaktivieren kann, müssen beide PCs sich im gleichen Subnetz befinden und dieselbe Wake-On-LAN-Hostverbindung verwenden. Die PCs können sich im gleichen oder in unterschiedlichen Maschinenkatalogen befinden.
- Hostverbindungen werden bestimmten Zonen zugewiesen. Wenn Ihre Bereitstellung mehr als eine Zone enthält, benötigen Sie in jeder Zone eine Wake-On-LAN-Hostverbindung. Gleiches gilt für Maschinenkataloge.
- Magic Packets werden mit der globalen Broadcast-Adresse 255.255.255.255 übertragen. Stellen Sie sicher, dass diese Adresse nicht blockiert ist.
- Um Maschinen in einem Subnetz zu reaktivieren, muss in diesem Subnetz (für jede Wake-On-LAN-Verbindung) mindestens ein PC aktiviert sein.

#### Operative Überlegungen

Berücksichtigen Sie Folgendes bei der Verwendung des Wake-On-LAN-Features:

- Der VDA muss sich mindestens einmal registrieren, bevor der PC über die integrierte Wake-On-LAN-Funktion reaktiviert werden kann.
- Wake-on-LAN kann nur zum Reaktivieren von PCs verwendet werden. Andere Energieaktionen wie Neustart oder Herunterfahren werden nicht unterstützt.
- Nachdem die Wake-On-LAN-Verbindung erstellt wurde, ist sie in Web Studio sichtbar. Die Eigenschaften können allerdings nicht in Web Studio bearbeitet werden, wenn On-Premises-Citrix Virtual Apps and Desktops verwendet wird.
- Es gibt zwei Situationen, in denen ein Magic Packet gesendet wird:
  1. Ein Benutzer versucht, eine Sitzung auf dem PC zu starten und der VDA ist nicht registriert.
  2. Ein Administrator sendet manuell einen Einschaltbefehl über Web Studio oder PowerShell.
- Da der Delivery Controller den Energiezustand eines PCs nicht kennt, wird in Web Studio unter "Energiezustand"**Nicht unterstützt** angezeigt. Der Delivery Controller ermittelt anhand des VDAs -Registrierungsstatus, ob ein PC ein- oder ausgeschaltet ist.

### Wake-On-LAN —SCCM-integriert

SCCM-integriertes Wake-On-LAN ist eine Wake-On-LAN-Alternative für Remote-PC-Zugriff, die nur mit on-premises Citrix Virtual Apps and Desktops verfügbar ist.

### Systemanforderungen

Folgende Systemanforderungen gelten für die Verwendung des SCCM-integrierten Wake-On-LAN-Feature:

- Citrix Virtual Apps and Desktops 1912 oder höher
- Physische PCs:
  - VDA: Version 1912 oder höher
  - Windows 10. Weitere Informationen zur Unterstützbarkeit finden Sie unter VDA-Systemanforderungen.
  - Wake-On-LAN aktiviert in BIOS/UEFI
  - Wake-On-LAN aktiviert in den Eigenschaften des Netzwerkadapters innerhalb der Windows-Konfiguration
- System Center Configuration Manager (SCCM) 2012 R2 oder höher

### Konfigurieren von SCCM-integriertem Wake-On-LAN

Folgende Voraussetzungen müssen erfüllt sein:

1. 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).
2. 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.
3. Zur Unterstützung von Magic Packet konfigurieren Sie Netzwerkrouter und Firewalls so, dass Magic Packets entweder per subnetzgesteuertem Broadcast oder Unicast gesendet werden können.
4. Konfigurieren Sie Wake-On-LAN in den BIOS/UEFI-Einstellungen aller PCs.
5. Stellen Sie den VDA auf den physischen PCs bereit (falls dies noch nicht erfolgt ist).

Nachdem alle Voraussetzungen erfüllt sind, führen Sie die folgenden Schritte aus, damit der Delivery Controller mit SCCM kommunizieren kann:

1. Erstellen Sie eine Hostverbindung für SCCM. Weitere Informationen finden Sie unter Verbindungen und Ressourcen.
   - Wählen Sie als Verbindungstyp **Microsoft Configuration Manager Wake on LAN**.

- Die eingegebenen Anmeldeinformationen müssen auf die Sammlungen im Geltungsbereich zugreifen können und die Rolle **Remotetoolsverantwortlicher** haben.

2. Wählen Sie die Verbindung in Web Studio aus, wählen Sie **Verbindung bearbeiten** und klicken Sie auf **Erweitert**.
3. Wählen Sie die entsprechende Option für Wake-On-LAN:

   - Bei Verwendung eines Aktivierungsproxys wählen Sie die erste Option: **Microsoft System Center Configuration Manager-Aktivierungsproxy**.
   - Bei Verwendung von Magic Packets wählen Sie die zweite Option: **Vom Delivery Controller übermittelte Wake-On-LAN-Pakete.**.
     - Wählen Sie die entsprechende Übertragungsmethode: **Subnetzgerichtete Broadcasts** oder **Unicast**.

Nach dem Erstellen der Hostverbindung ordnen Sie die Verbindung einem Remote-PC-Zugriff-Katalog zu:

- Um einen neuen Remote-PC-Zugriff-Katalog zu erstellen, wählen Sie im Assistenten für die Katalogerstellung auf der Seite **Betriebssystem** den Katalogtyp **Remote-PC-Zugriff** und dann die entsprechende Verbindung aus der Dropdown-Liste aus.
- Hinzufügen von Wake-On-LAN zu einem vorhandenen Remote-PC-Zugriff-Katalog:

  1. Wechseln Sie in Web Studio zum Knoten **Maschinenkataloge**, wählen Sie den Maschinenkatalog aus und wählen Sie dann **Maschinenkatalog bearbeiten**.
  2. Wählen Sie die Registerkarte **Energieverwaltung** und wählen Sie **Ja**, um die Energieverwaltung für den Maschinenkatalog zu aktivieren.
  3. Wählen Sie die entsprechende Verbindung aus der Dropdown-Liste aus und klicken Sie auf **OK**.

## 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.

## Inhalte veröffentlichen

June 27, 2024

> **Hinweis:**
>
> Sie können Ihre Citrix Virtual Apps and Desktops-Bereitstellung mithilfe von zwei Verwaltungskonsolen verwalten: Web Studio (webbasiert) und Citrix Studio (Windows-basiert). Dieser Artikel behandelt nur Web Studio. Informationen zu Citrix Studio finden Sie im entsprechenden Artikel in Citrix Virtual Apps and Desktops 7 2212 oder früher.

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. Sie können auch festlegen, ob der Inhalt über lokale oder veröffentlichte Anwendungen geöffnet werden soll.

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 Web Studio können Sie keinen Inhalt veröffentlichen. Allerdings können Sie mit Web 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 auf `PublishedContent` festgelegt werden.

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 Bereitstellungen mit Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) 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 Multisitzungs-OS-Maschine 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 DaaS 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.

```
$rtfUNC = "\GMSXJ-EDGE0.xd.local\PublishedResources\PublishedRTF.rtf"
$rtfAppName = "PublishedRTF"

New-BrokerApplication –ApplicationType PublishedContent
–CommandLineExecutable $rtfUNC -Name $rtfAppName
-DesktopGroup $dg.Uid

$docxUNC = "\GMSXJ-EDGE0.xd.local\PublishedResources\PublishedDOCX.docx
    "
$docxAppName = "PublishedDOCX"

New-BrokerApplication –ApplicationType PublishedContent
–CommandLineExecutable $docxUNC -Name $docxAppName
-DesktopGroup $dg.Uid
<!--NeedCopy-->
```

Überprüfen des Vorgangs

- Aktualisieren Sie Ihr StoreFront-Fenster, um die neu veröffentlichten Dokumente anzuzeigen.
- Klicken Sie auf die Anwendungen **PublishedRTF** und **PublishedDOCX**. Beide Dokumente werden in einer lokal ausgeführten WordPad-Instanz geöffnet.

### Anzeigen und Bearbeiten von Anwendungen mit veröffentlichtem Inhalt

Sie verwalten veröffentlichte Inhalte genauso wie andere Anwendungstypen.

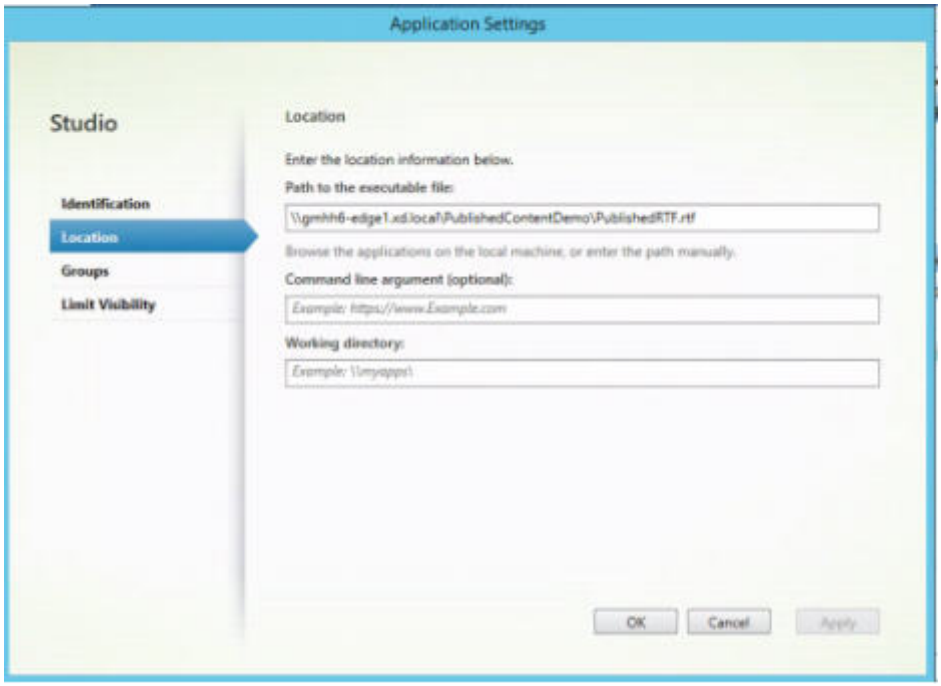
Führen Sie folgende Schritte aus, um `PublishedContent`-Anwendungen anzuzeigen und zu bearbeiten:

1. Melden Sie sich bei Web Studio an und wählen Sie im linken Bereich **Anwendungen**.
2. Wählen Sie auf der Registerkarte **Anwendungen** eine PublishedContent-Anwendung und dann **Eigenschaften**.

Anwendungseigenschaften (z. B. Benutzersichtbarkeit, Gruppenzuordnung und Verknüpfung) gelten für die veröffentlichten Inhalte. Befehlszeilenargumente und Arbeitsverzeichnis können Sie auf der Seite **Speicherort** jedoch nicht ändern.

3. Zum Ändern der Ressource ändern Sie das Feld **Pfad zur ausführbaren Datei** auf dieser Seite.

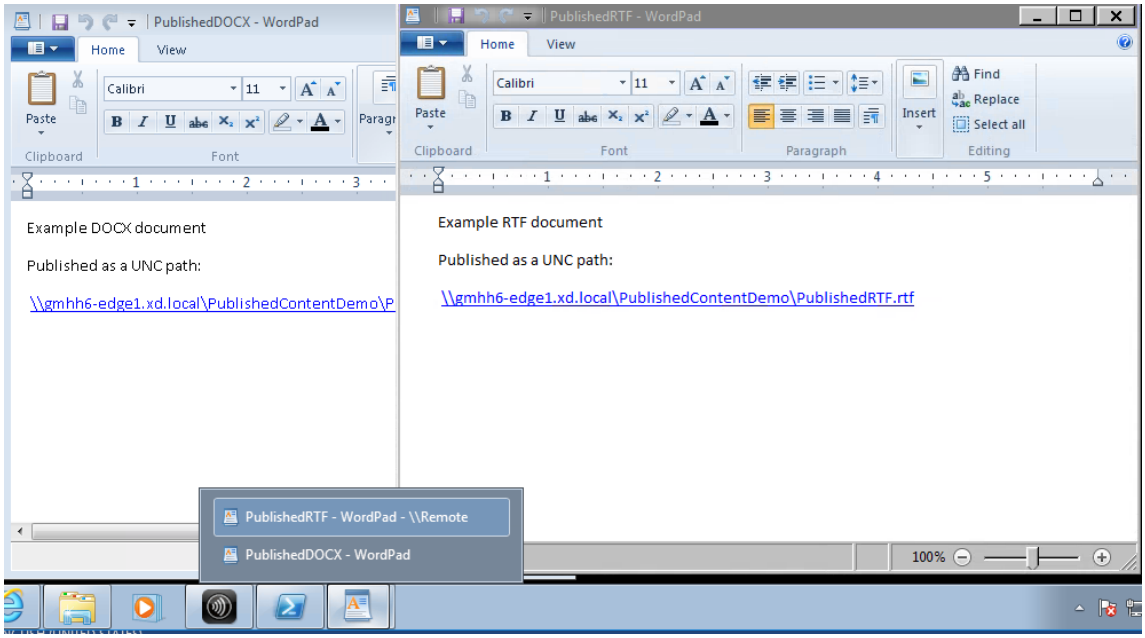



4. Führen Sie folgende Schritte aus, um eine `PublishedContent`-Anwendung mit einer veröffentlichten Anwendung (und nicht mit einer lokalen Anwendung) zu öffnen:

   In diesem Beispiel wird der veröffentlichten WordPad-Anwendung die Dateitypzuordnung für RTF-Dateien zugewiesen.

   a) Aktivieren Sie den Wartungsmodus für die Bereitstellungsgruppe.
   b) Bearbeiten Sie die Eigenschaft **Dateitypzuordnung**.
   c) Deaktivieren Sie den Wartungsmodus, wenn Sie fertig sind.
   d) 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

- Maschinenkataloge erstellen
- Bereitstellungsgruppen erstellen
- Ändern von App-Eigenschaften

## Server-VDI

June 27, 2024

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 aus der Cloud anbieten. Diese Desktops entsprechen dem Microsoft Services Provider License Agreement (SPLA).

Support:

- In Bereitstellungen mit Citrix Virtual Apps and Desktops und Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) wird eine Server-VDI unter Windows Server 2022, Windows Server 2019 und Windows Server 2016 unterstützt.

- Alle Server-VDI-Bereitstellungen unterstützen Benutzerpersonalisierungslayer.
- Damit die Server-VDI mit TWAIN-Geräten wie etwa Scannern funktioniert, muss das Windows-Feature Desktopdarstellung installiert werden.
- Die folgenden Features können nicht mit der Server-VDI verwendet werden:
  - Gehostete Anwendungen
  - Lokaler App-Zugriff
  - Direkte (nicht vermittelte) Desktopverbindungen
  - Remote-PC-Zugriff

### 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\Terminal Server
     ```

     ```
     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 DaaS-Bereitstellungen:
     - `VDAWorkstationSetup.exe /quiet /servervdi`

   Weitere Optionen:

- Verwenden Sie `/controllers`, um Delivery Controller oder Cloud Connectors anzugeben.
- Öffnen Sie mit `/enable_hdx_ports` Ports in der Firewall, wenn diese nicht manuell konfiguriert wird.
- Verwenden Sie `/mastermcsimage` oder `/masterimage`, wenn Sie den VDA auf einem Image installieren, und verwenden Sie MCS zum Erstellen von Server-VMs von diesem Image.
- 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 einer Multisitzungsmaschine installiert ist.

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 Cloud Connectors angegeben haben, holen Sie das anschließend nach. Informationen hierzu finden Sie unter VDA-Registrierung.

## Benutzerpersonalisierungslayer

June 27, 2024

> **Hinweis:**
>
> Sie können Ihre Citrix Virtual Apps and Desktops-Bereitstellung mithilfe von zwei Verwaltungskonsolen verwalten: Web Studio (webbasiert) und Citrix Studio (Windows-basiert). Dieser Artikel behandelt nur Web Studio. Informationen zu Citrix Studio finden Sie im entsprechenden Artikel in Citrix Virtual Apps and Desktops 7 2212 oder früher.

Der Benutzerpersonalisierungslayer ist ein Feature für Citrix Virtual Apps and Desktops, das die Funktionen nicht persistenter Maschinenkataloge erweitert, um die Daten der Benutzer und lokal installierte Anwendungen über Sitzungen hinweg zu erhalten. Wie PvD unterstützt der auf Citrix App Layering-Technologie basierende Benutzerpersonalisierungslayer Citrix Provisioning und Maschinenerstellungsdiensten (MCS) in einem nicht persistenten Maschinenkatalog.

Die Komponenten des Benutzerpersonalisierungslayers werden zusammen mit dem Virtual Delivery Agent im Masterimage installiert. Lokal von Benutzern installierte Anwendungen werden in einer VHD-Datei gespeichert. Die auf dem Image bereitgestellte virtuelle Festplatte fungiert als persönliche virtuelle Festplatte des Benutzers.

> **Wichtig:**
>
> Sie können Benutzerpersonalisierungslayer in Citrix Virtual Apps and Desktops oder in einer App Layering-Imagevorlage aktivierte App Layering-Benutzerlayer bereitstellen (nicht beides). Installieren Sie das Benutzerpersonalisierungslayer-Feature nicht auf einem Layer innerhalb von App Layering.

Das Feature ersetzt PvD (persönliche vDisk) und bietet Benutzern in einer nicht persistenten, gepoolten Desktopumgebung eine persistente Workspace-Benutzeroberfläche.

Um die Funktion für die Benutzerpersonalisierungslayer bereitzustellen, installieren und konfigurieren Sie sie mit den im Artikel beschriebenen Schritten.

## 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 (GPO) 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 installiert, wechselt die App in seinen Benutzerlayer. Wenn der Benutzer dann einen lokalen Benutzer oder eine lokale Gruppe hinzufügt oder bearbeitet, bleiben diese Änderungen nicht über die Sitzung hinaus bestehen.

> **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 oder höher
- Citrix Provisioning, Version 1909 oder höher
- Windows-Dateifreigabe (SMB) oder Azure Files mit aktivierter AD-Authentifizierung on premises

Sie können das Feature Benutzerpersonalisierungslayer unter den folgenden Windows-Versionen bereitstellen, sofern das Betriebssystem als Einzelsitzung bereitgestellt wird. Es wird nur ein Benutzer in einer Sitzung unterstützt.

- Windows 11 Enterprise x64
- Windows 10 Enterprise x64, Version 1607 oder höher
- Windows Server 2016 (unterstützt Azure Files)
- Windows Server 2019 (unterstützt Azure Files)
- Windows Server 2022 (unterstützt Azure Files)

Citrix Virtual Apps and Desktops 7 unterstützt Azure Files mit Benutzerpersonalisierunglayern unter Windows Server 2022, Windows Server 2019, Windows Server 2016 und Windows 10-Client.

> **Hinweis:**
>
> Wenn Sie ein Serverbetriebssystem verwenden, wird nur Server-VDI unterstützt. Weitere Informationen finden Sie im Artikel Server-VDI.
>
> Ein Benutzerpersonalisierungslayer unterstützt nur einen Benutzer pro Maschine und die Maschine muss neu starten, um die Datenträger zurückzusetzen. Sie können den Benutzerpersonalisierungslayer nur mit Einzelsitzungs-Server-OS nicht aber mit Multisitzungs-Server-OS verwenden. Der Benutzerpersonalisierungslayer wird nur für nicht persistente Desktops unterstützt.

Deinstallieren Sie den Benutzerpersonalisierungslayer, falls das Feature installiert ist. Starten Sie das Masterimage neu, bevor Sie das neueste Release installieren.

### Einrichten der Dateifreigabe

Für Benutzerpersonalisierungslayer ist Windows SMB-Speicher (Server Message Block) erforderlich. Zum Erstellen einer Windows-Dateifreigabe folgen Sie dem bei Ihrem Windows-Betriebssystem üblichen Verfahren.

Weitere Informationen zum Verwenden von Azure-Dateien mit Azure-basierten Katalogen finden Sie unter Einrichten des Azure Files-Speichers für Benutzerpersonalisierungslayer.

### Empfehlungen

Beachten Sie die Empfehlungen in diesem Abschnitt, um den Benutzerpersonalisierungslayer fehlerfrei bereitzustellen.

#### Microsoft System Center Configuration Manager

Wenn Sie den Benutzerpersonalisierungslayer mit SCCM verwenden, sollten Sie die Microsoft-Richtlinien zur Image-Vorbereitung in einer VDI-Umgebung beachten. Weitere Informationen finden Sie in diesem Microsoft TechNet-Artikel .

#### Benutzerlayergröße

Ein Benutzerlayer ist ein Datenträger mit schlanker Speicherzuweisung, der erweitert wird, wenn Speicherplatz auf dem Datenträger verwendet wird. Die zulässige Standardgröße für einen Benutzerlayer beträgt 10 GB (empfohlenes Minimum).

> **Hinweis:**
>
> Wird der Wert bei der Installation auf Null (0) festgelegt, dann wird der Standardwert von 10 GB für den Benutzerlayer verwendet.

Wenn Sie die Benutzerlayergröße ändern möchten, können Sie einen anderen Wert für die Richtlinie **Größe von Benutzerlayer** eingeben. Weitere Informationen finden Sie unter **Schritt 5: Erstellen benutzerdefinierter Richtlinien für die Bereitstellungsgruppe** unter **Optional: Klicken Sie neben “Größe von Benutzerlayer in GB”auf “Auswählen”:**

#### Tools zum Außerkraftsetzen der Benutzerlayergröße (optional)

Sie können die Benutzerlayergröße außer Kraft setzen, indem Sie mit einem Windows-Tool ein Kontingent für die Benutzerlayer-Dateifreigabe festlegen.

Verwenden Sie eines der folgenden Microsoft-Kontingenttools, um ein festes Kontingent für die Benutzerlayer-Dateifreigabe **Users** festzulegen:

- Ressourcen-Manager für Dateiserver (FSRM)
- Kontingentmanager

> **Hinweis:**
>
> Das Erhöhen des Kontingents wirkt sich auf neue Benutzerlayer aus und erweitert vorhandene Layer. Das Verringern des Kontingents wirkt sich nur auf neue Benutzerlayer aus. Vorhandene Benutzerlayer werden nie verkleinert.

## Bereitstellen eines Benutzerpersonalisierungslayers

Beim Bereitstellen der Benutzerpersonalisierung definieren Sie die Richtlinien in Web Studio. Anschließend weisen Sie die Richtlinien der Bereitstellungsgruppe zu, die dem Maschinenkatalog zugewiesen ist, für den das Feature bereitgestellt wird.

Wenn kein Benutzerpersonalisierungslayer auf dem Masterimage konfiguriert ist, bleiben die Dienste inaktiv und beeinträchtigen die Erstellungsaktivitäten nicht.

Wenn Sie die Richtlinien im Masterimage festlegen, versuchen die Dienste, einen Benutzerlayer im Masterimage auszuführen und bereitzustellen. Dabei treten beim Masterimage unerwartetes Verhalten und Instabilität auf.

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.

> **Hinweis:**
>
> Nachdem Sie Windows 10 auf dem Image aktualisiert haben, dauert das erste Anmelden länger als gewöhnlich. Der Benutzerlayer muss für die neue Version von Windows 10 aktualisiert werden, wodurch sich die Anmeldezeit verlängert.

### Schritt 1: Überprüfen der Verfügbarkeit einer Citrix Virtual Apps and Desktops-Umgebung

Vergewissern Sie sich, 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.

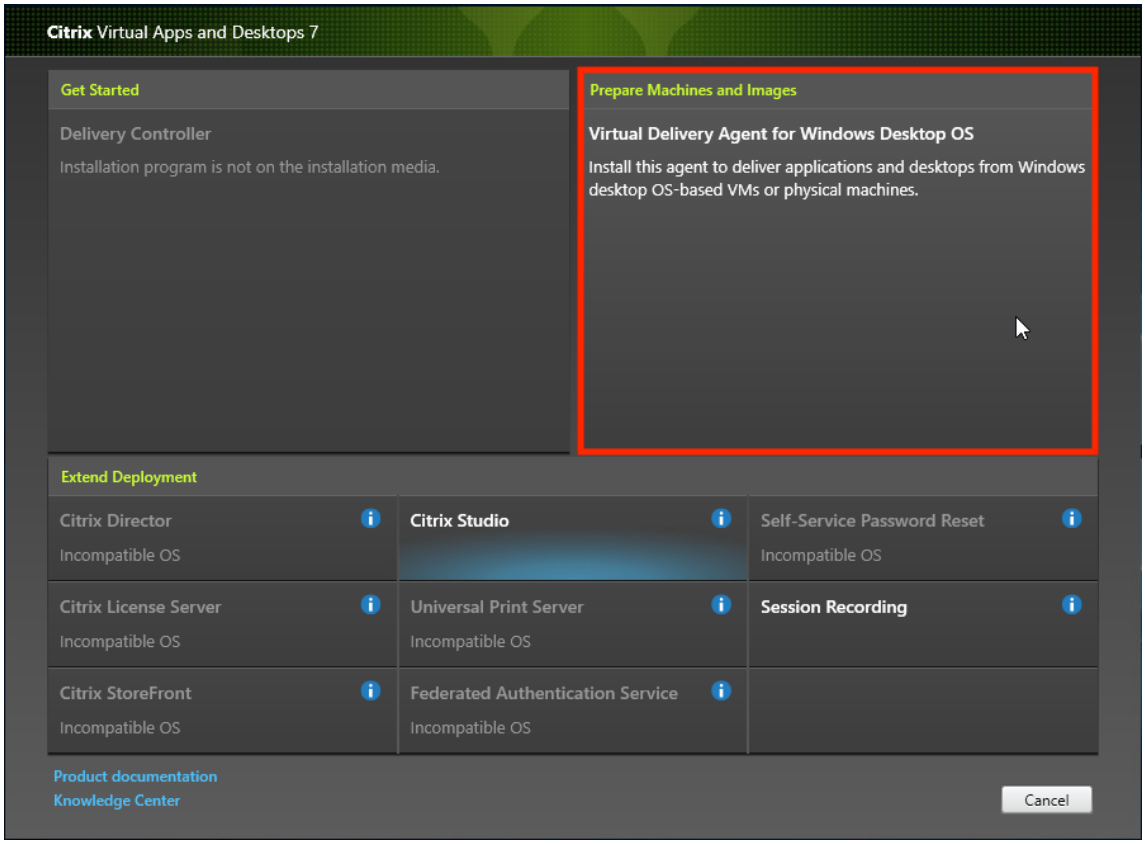
 

### Schritt 2: Vorbereiten Ihres Masterimages

Zum Vorbereiten des Masterimages führen Sie folgende Schritte aus:

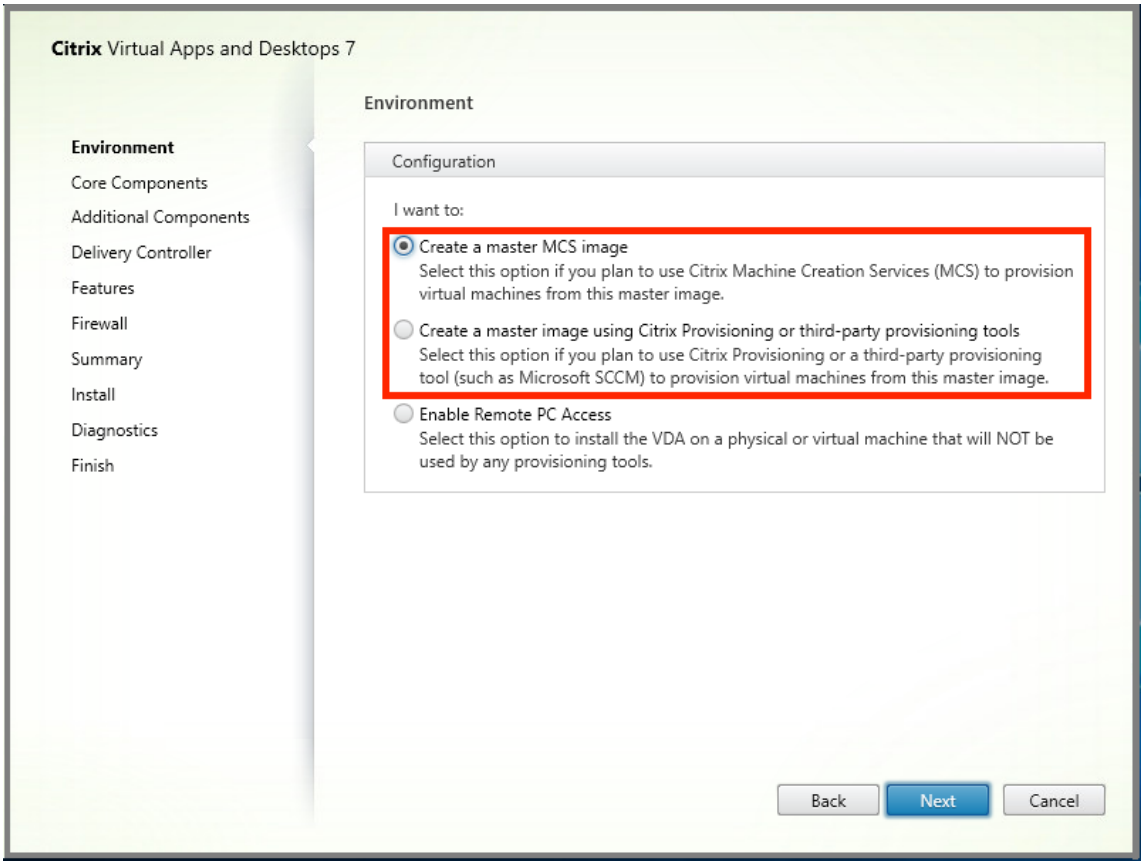
1. Suchen Sie das Masterimage. Installieren Sie die Unternehmensanwendungen Ihrer Organisation und alle übrigen Apps, die für Benutzer von Nutzen sein könnten.
2. Wenn Sie die Server-VDI bereitstellen, führen Sie die unter Server-VDI aufgeführten Schritte aus. Schließen Sie die optionale Komponente **Benutzerpersonalisierungslayer** ein. Einzelheiten finden Sie unter Befehlszeilenoptionen zur VDA-Installation.
3. Wenn Sie Windows 10 verwenden, installieren Sie Virtual Delivery Agent (VDA) 1912 oder höher. 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**.

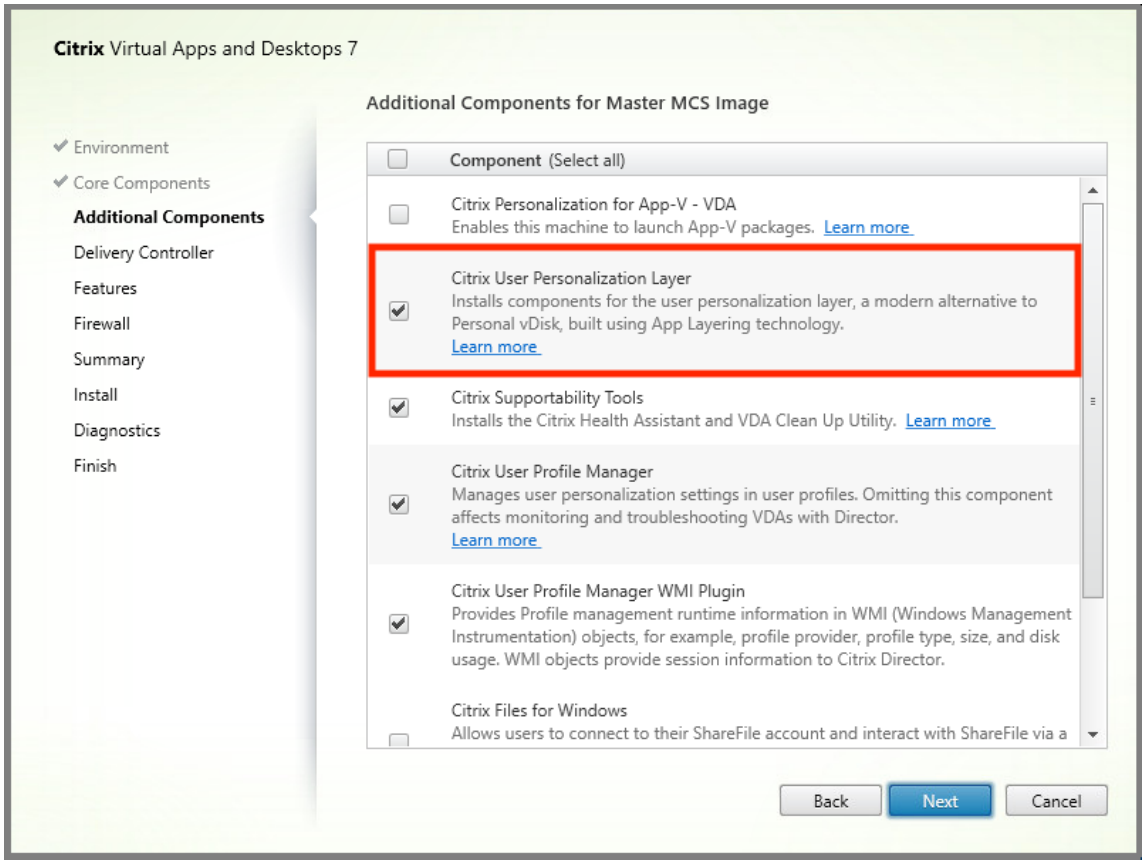
 




a) **Kernkomponenten:** Klicken Sie auf **Weiter**.

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.

4. 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 Web Studio hochgeladen werden.

> **Hinweis:**
>
> Wenn Sie lediglich den Benutzerpersonalisierungslayer (UPL) aktualisieren möchten, können Sie dies mit einer neueren Version des Benutzerpersonalisierungslayers und dem eigenständigen Installationspaket tun. Sie müssen den VDA nicht aktualisieren.

#### Schritt 3: Erstellen eines Maschinenkatalogs

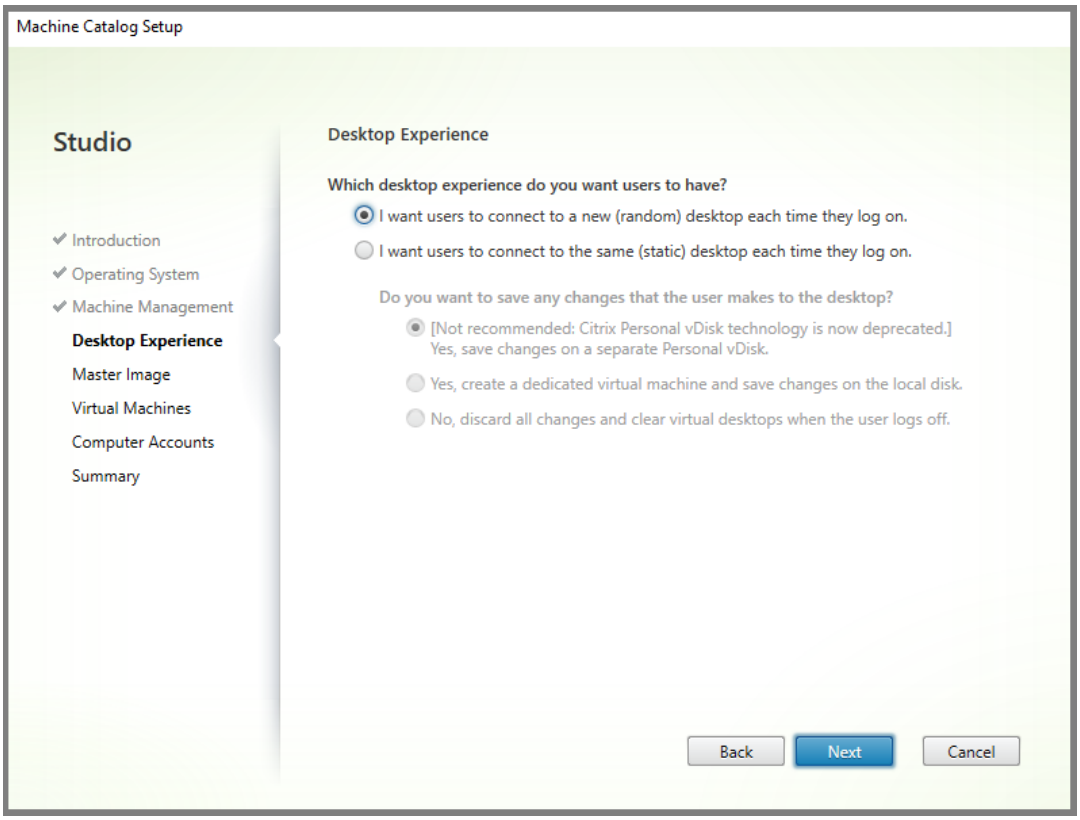
Führen Sie in Web Studio folgende Schritte aus, um einen Maschinenkatalog zu erstellen. Verwenden Sie die folgenden Optionen während der Katalogerstellung:

1. Wählen Sie unter **Betriebssystem** die Einstellung **Betriebssystem für Einzelsitzungen**.

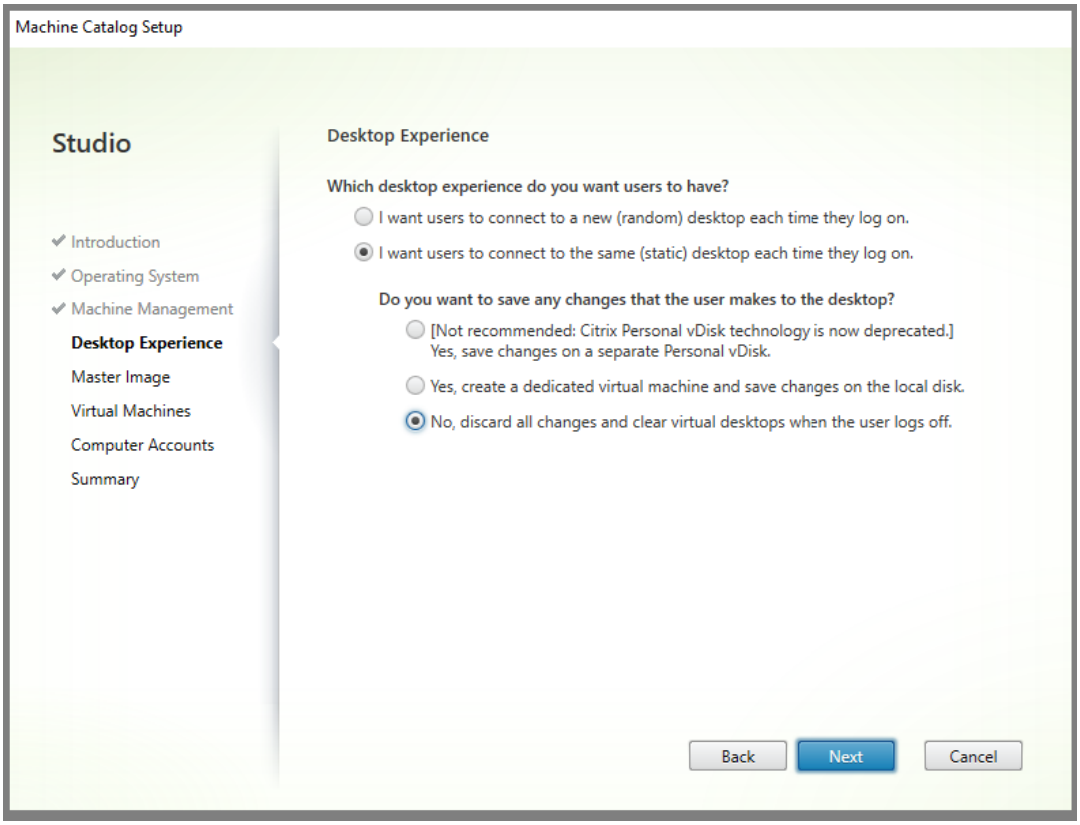
2. Wählen Sie unter **Maschinenverwaltung** die Einstellung **Maschinen mit Energieverwaltung**. Zum Beispiel virtuelle Maschinen oder Blade-PCs.
3. Wählen Sie unter **Desktoperfahrung** den Katalogtyp **Gepoolt-zufällig** oder **Gepoolt-statisch**, wie in den folgenden Beispielen angegeben:

   - **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 **Image** 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

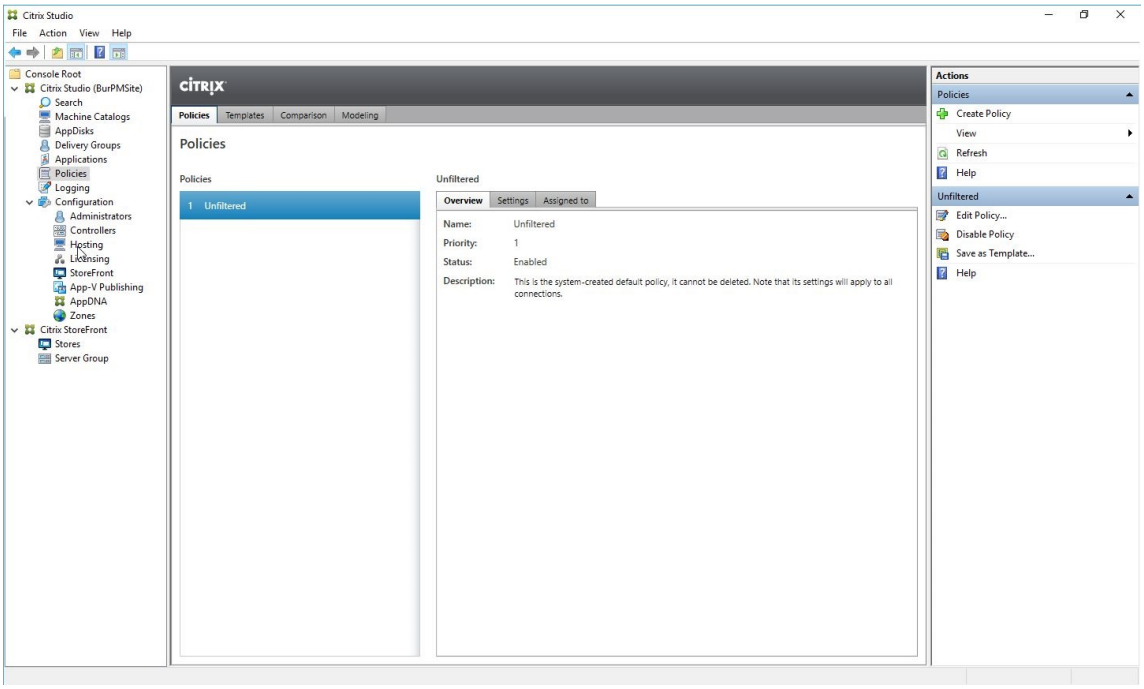
Um die Bereitstellung von Benutzerlayern in Virtual Delivery Agents zu aktivieren, definieren Sie mit den Konfigurationsparametern Folgendes:

- Wo im Netzwerk auf die Benutzerlayer zugegriffen werden soll.
- Die maximale Größe der Datenträger für die Benutzerlayer.

Die Parameter als benutzerdefinierte Citrix Richtlinien in Web Studio und die Zuweisung zu Ihrer Bereitstellungsgruppe.

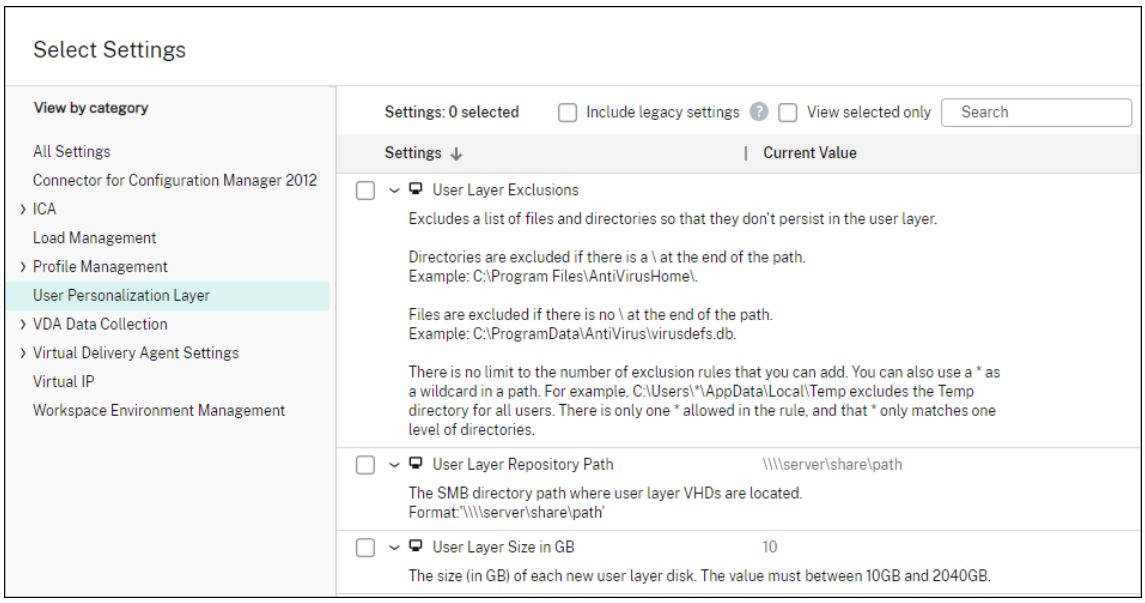
1. Melden Sie sich bei Web Studio an und wählen Sie im linken Bereich **Richtlinien**.




2. Wählen Sie in der Aktionsleiste **Richtlinie erstellen**. Das Fenster Richtlinie erstellen wird angezeigt.
3. Geben Sie “`user layer`”in das Suchfeld ein. Drei Richtlinien werden in der Liste der verfügbaren Richtlinien angezeigt:
    - Benutzerlayerausschlüsse
    - Repositorypfad für Benutzerlayer
    - Größe von Benutzerlayer in GB

    > **Hinweis:**
    >
    > Das Erhöhen der Größe wirkt sich auf neue Benutzerlayer aus und erweitert vorhandene Benutzerlayer. Das Verringern der Größe wirkt sich nur auf neue Benutzerlayer aus. Vorhandene Benutzerlayer werden nie verkleinert.

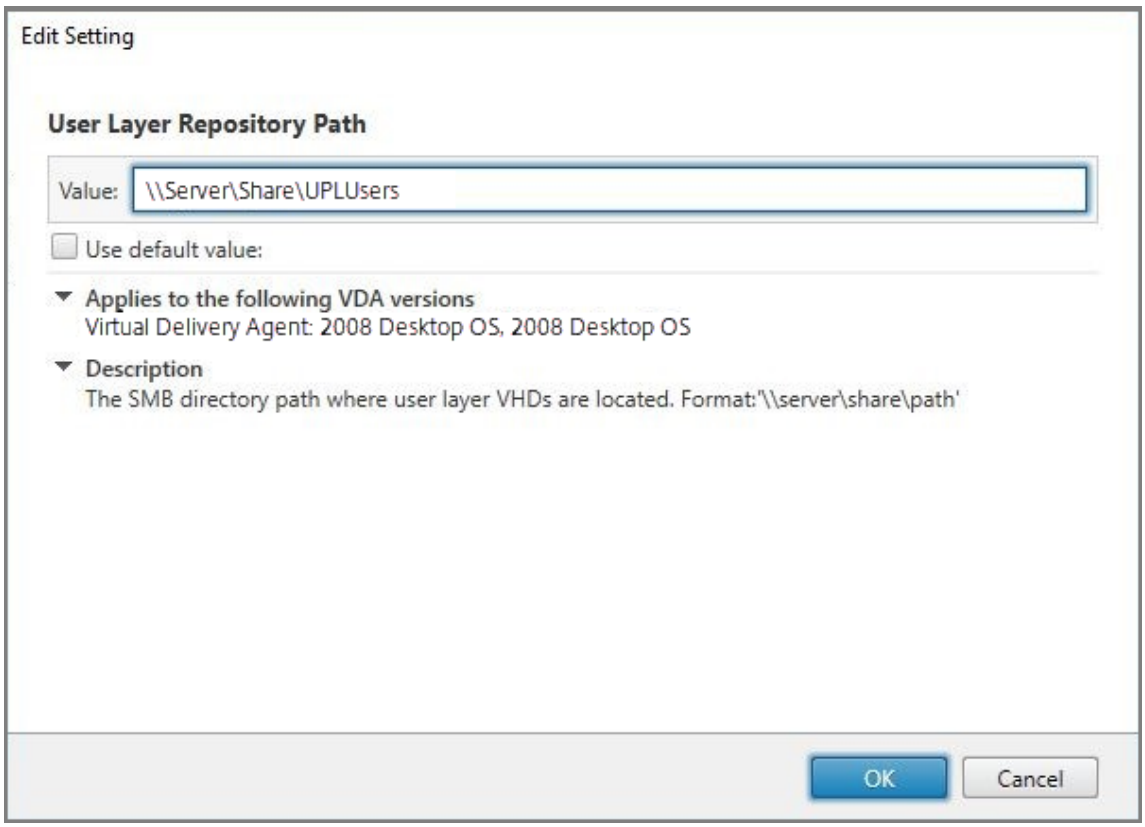
 




4. Markieren Sie das Kontrollkästchen neben **Repositorypfad für Benutzerlayer** und klicken Sie auf **Bearbeiten**. Das Fenster **Einstellung bearbeiten** wird angezeigt.
5. Geben Sie einen Pfad im Feld **Wert** ein und klicken Sie auf **Speichern**:

   - **Pfadformat:** `\\server-name-or-address\share-name\folder`
   - **Pfadbeispiel:** `\\Server\Share\UPLUsers`
   - **Beispiel für resultierende Pfade:** Für den Benutzer **Alex** in **CoolCompanyDomain** würde der Pfad lauten: `\\Server\Share\UPLUsers\Users\CoolCompanyDomain_Alex\A_OK`

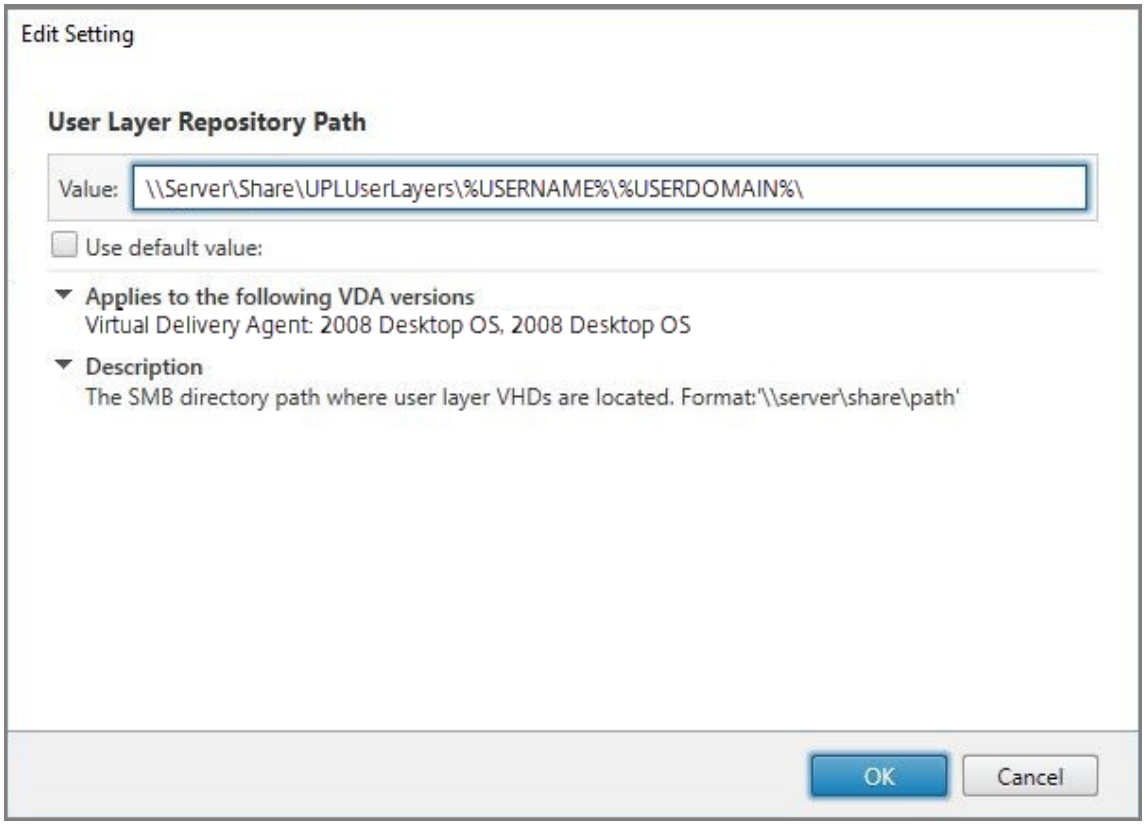



Sie können den Pfad mithilfe der Variablen %USERNAME% und %USERDOMAIN%, der Maschinenumgebungsvariablen und von Active Directory-Attributen anpassen. Wenn diese Variablen erweitert werden, führen sie zu expliziten Pfaden.

Beispiel für Umgebungsvariablen:

- **Pfadformat:** \\Server-name-or-address\share-name\folder-with-environment-variables
- **Pfadbeispiel:** \\Server\Share\UPLUserLayers\\%USERNAME%\\%USERDOMAIN%
- **Beispiel für resultierende Pfade:** Für den Benutzer **Alex** in **CoolCompanyDomain** würde der Pfad \\Server\Share\UPLUserLayers\Alex\CoolCompanyDomain\A_OK lauten.

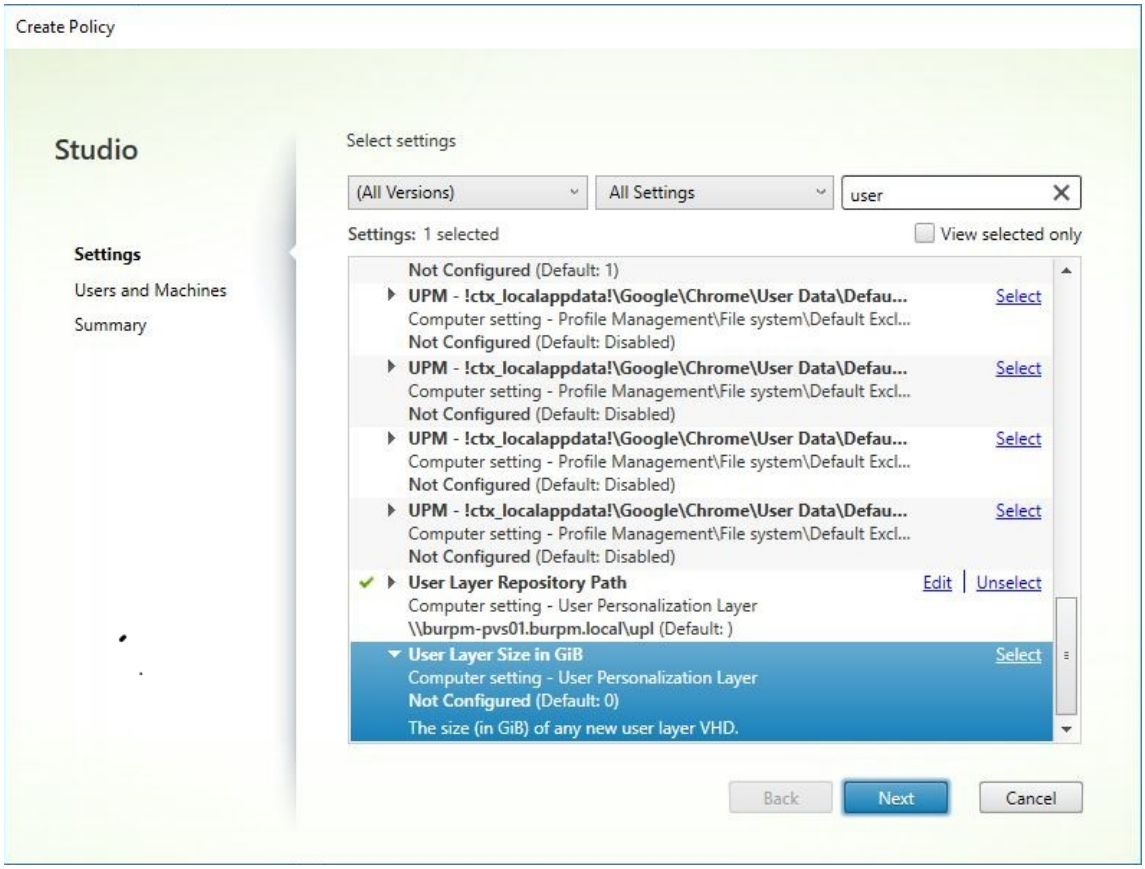



Beispiel für benutzerdefinierte AD-Attribute:

- Pfadformat: `\\Server-name-or-address\share-name\AD-attribute`
- Pfadbeispiel: `\\Server\share\\#sAMAccountName#`
- Beispiel für resultierende Pfade: `\\Server\share\JohnSmith` (wenn #sAMAccount-Name# für den aktuellen Benutzer in JohnSmith aufgelöst wird)

6. Optional: Markieren Sie das Kontrollkästchen neben **Größe von Benutzerlayer in GB** und klicken Sie auf **Bearbeiten**:

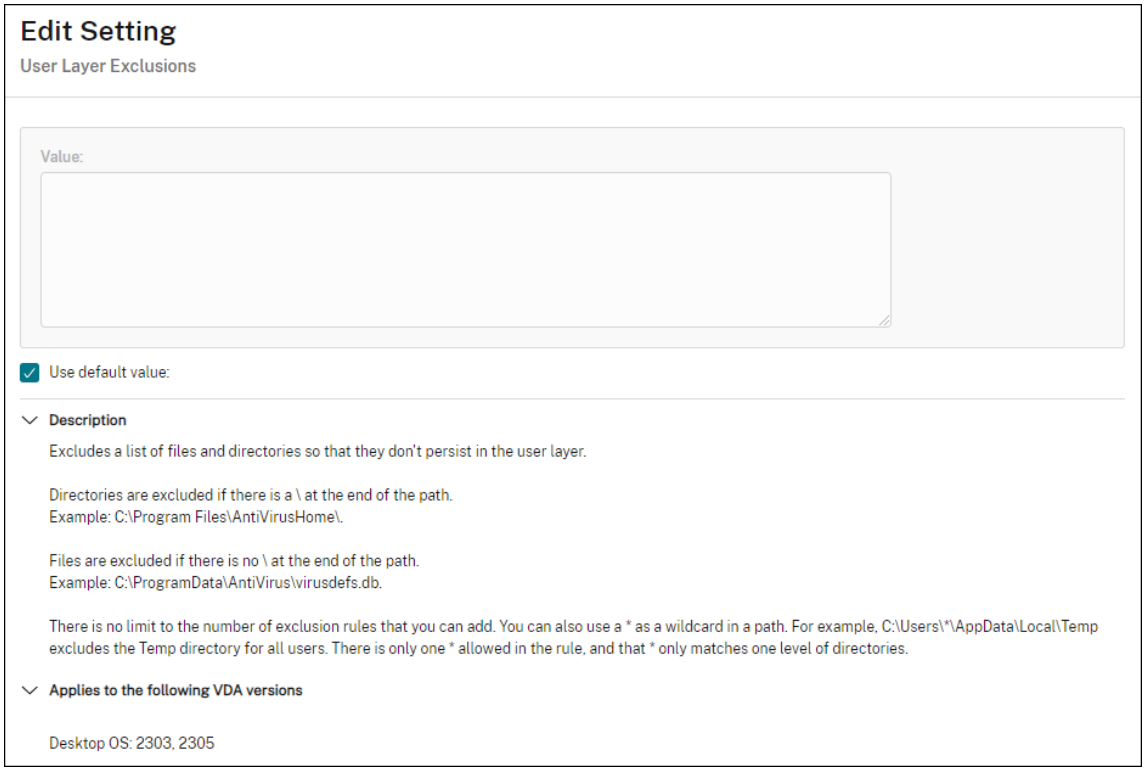
 




Das Fenster “Einstellungen bearbeiten”wird angezeigt.

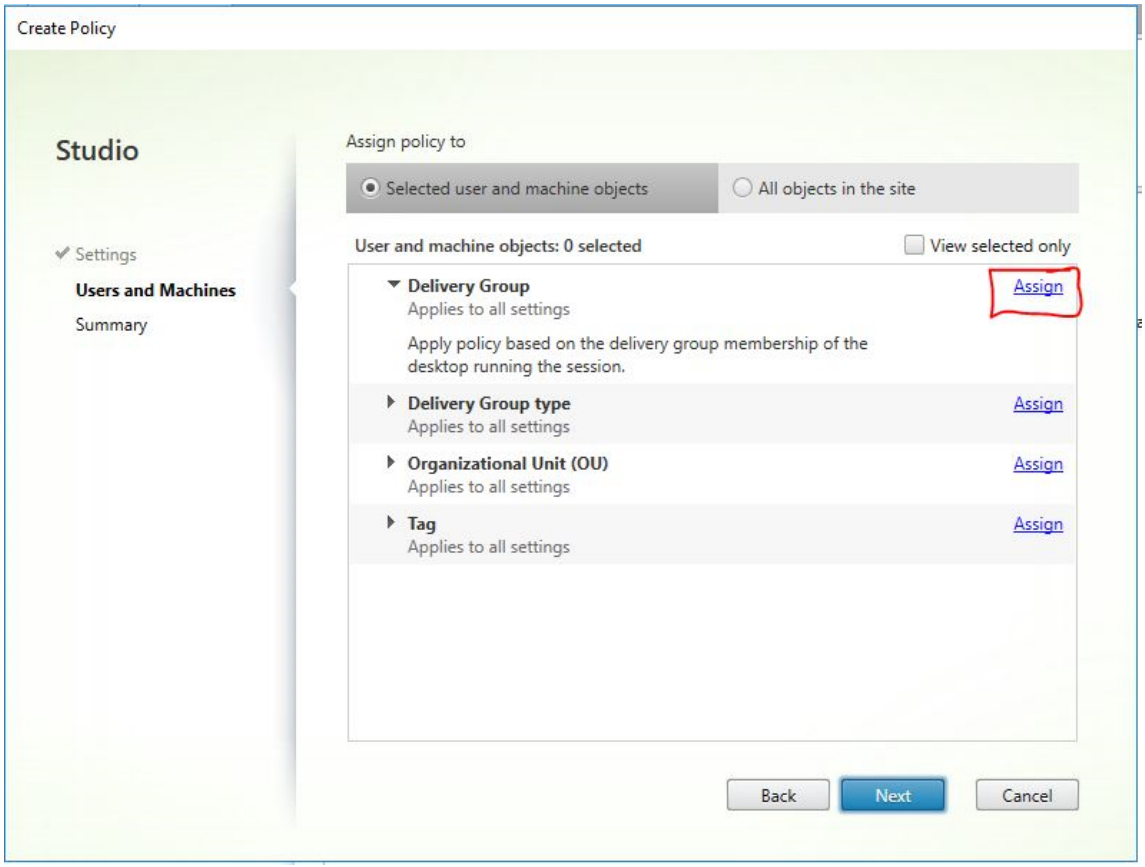
7. Optional: Ändern Sie den Standardwert von **10 GB** auf die maximale Größe, die jeder Benutzerlayer wachsen kann. Klicken Sie auf **Speichern**.
8. Optional: Markieren Sie das Kontrollkästchen neben **Benutzerlayerausschlüsse** und klicken Sie auf **Bearbeiten**.



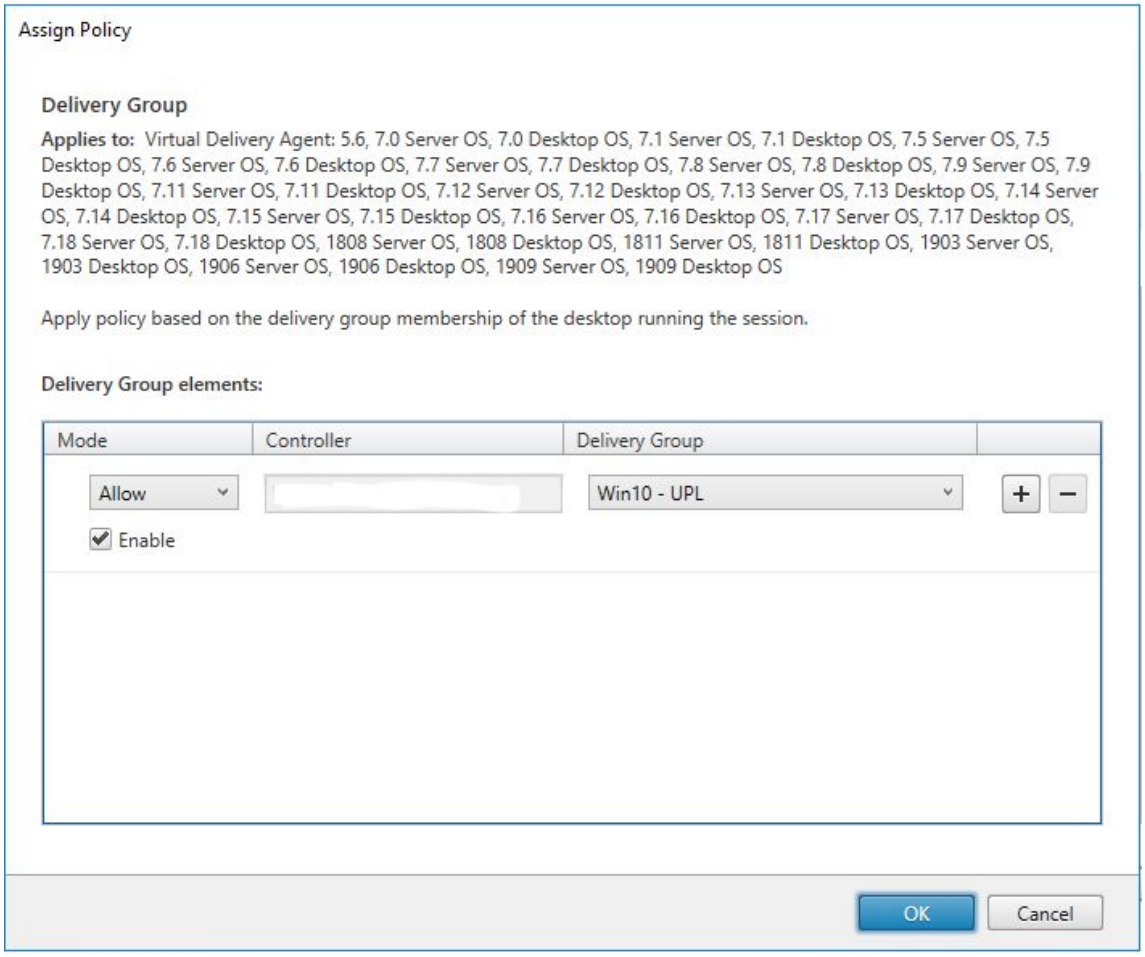

9. Optional: Geben Sie die auszuschließenden Dateien und Ordner an und klicken Sie dann auf **Speichern**. Weitere Informationen finden Sie in der Dokumentation zu Citrix App Layering.
10. Klicken Sie auf **Weiter**, um Benutzer und Maschinen zu konfigurieren, die Sie zuweisen möchten. Klicken Sie neben **Bereitstellungsgruppe** auf den Link “Zuweisen”(im Bild markiert):



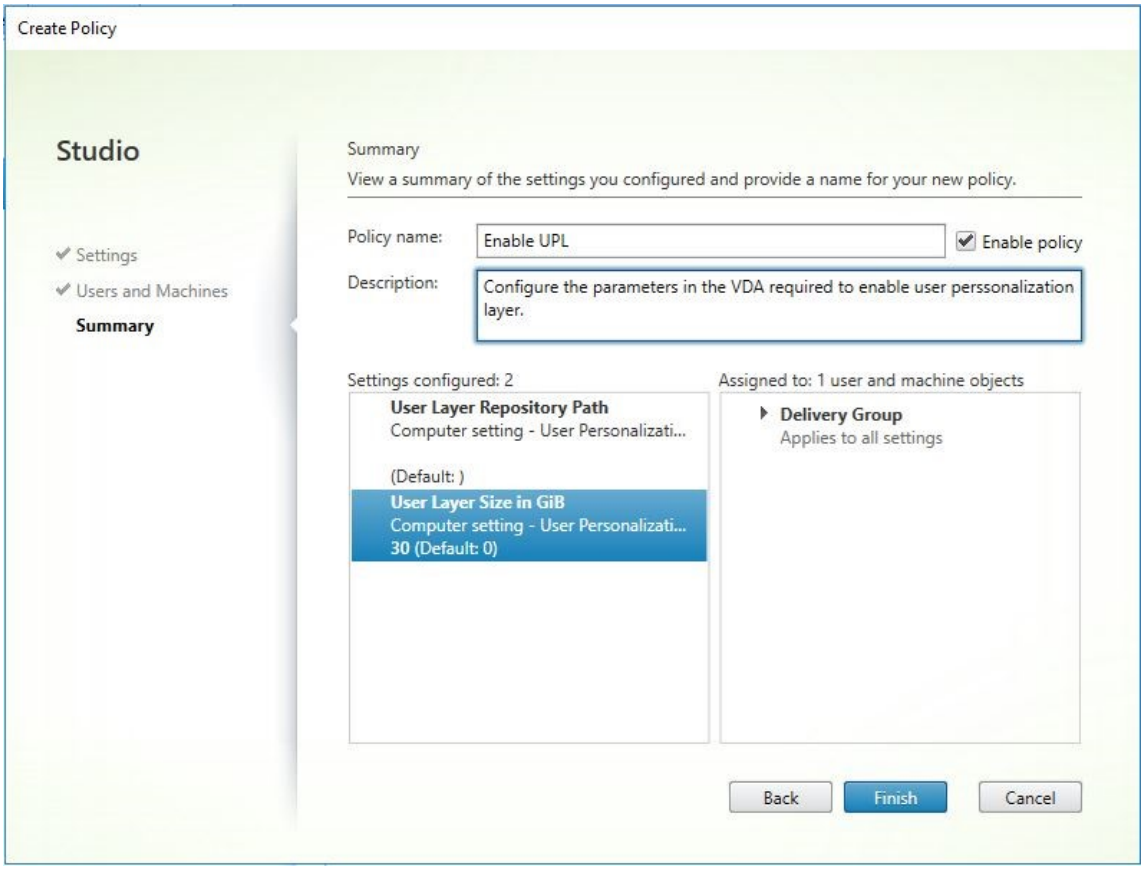

11. Wählen Sie im **Bereitstellungsgruppenmenü** die im vorherigen Abschnitt erstellte Bereitstellungsgruppe aus. Klicken Sie auf **OK**.




12. Geben Sie einen Namen für die Richtlinie ein. Klicken Sie auf das Kontrollkästchen, um die Richtlinie zu aktivieren, und klicken Sie auf **Fertigstellen**.




### Konfigurieren von Sicherheitseinstellungen im Benutzerlayerordner

Als Domänenadministrator können Sie mehrere Speicherorte für Ihre Benutzerlayer angeben. Erstellen Sie einen Unterordner `\Users` für jeden Speicherort (einschließlich des Standardspeicherorts). Schützen Sie jeden Speicherort über die 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**

  ```
  We were unable to attach your user layer because it is in use. Any changes you make to application settings or data will not be saved. Be sure to save any work to a shared network location.<!--NeedCopy-->
  ```

- **Benutzerlayer nicht verfügbar**

  ```
  We were unable to attach your user layer. Any changes you make to application settings or data will not be saved. Be sure to save any work to a shared network location.<!--NeedCopy-->
  ```

- **System wird nach der Benutzerabmeldung nicht zurückgesetzt**

  ```
  This system was not shut down properly. Please log off immediately and contact your system administrator.<!--NeedCopy-->
  ```

### Protokolldateien für die Fehlerbehebung

Die Protokolldatei ulayersvc.log enthält die Ausgabe der Benutzerpersonalisierungslayer-Software, in der Änderungen erfasst werden.

```
1 C:\ProgramData\Unidesk\Logs\ulayersvc.log
2 <!--NeedCopy-->
```

### Rückgewinnung von Benutzerlayer/UPL-Speicherplatz

Sie können die **Rückgewinnung von Benutzerlayer-/UPL-Speicherplatz** verwenden, um die VHDX-Dateien bei jeder Benutzerabmeldung automatisch zu komprimieren.
Weitere Informationen finden Sie unter Rückgewinnung von Benutzerlayer/UPL-Speicherplatz

### Einschränkungen

Berücksichtigen Sie folgende Einschränkungen bei der Installation und Verwendung des Benutzerpersonalisierung Features.

- Versuchen Sie *nicht*, die Benutzerpersonalisierungslayer-Software auf einem Layer innerhalb des App Layering bereitzustellen. Stellen Sie Benutzerpersonalisierungslayer in Citrix Virtual Apps and Desktops bereit, oder aktivieren Sie Benutzerlayer in einer App Layering-Imagevorlage (nicht beides). Jeder Prozess erzeugt die Benutzerlayer, die Sie benötigen.
- 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). Die beste Lösung ist, 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.
- Wenn sich ein Benutzer von einer Sitzung ab- und wieder anmeldet, wird die neue Sitzung auf einer anderen Maschine im Pool ausgeführt. In VDI-Umgebungen listet Microsoft Software Center eine Anwendung als **Installiert** auf der ersten Maschine auf, auf der zweiten wird sie jedoch als **Nicht verfügbar** angezeigt.

  Weisen Sie den Benutzer an, zur Ermittlung des tatsächlichen Anwendungsstatus die Anwendung im Software Center auszuwählen und auf **Installieren** zu klicken. SCCM aktualisiert dann den Status dann mit dem tatsächlichen Wert.
- Gelegentlich wird das Softwarecenter auf einem VDA mit aktiviertem Benutzerpersonalisierungslayer unmittelbar nach dem Start beendet. Um dieses Problem zu vermeiden, beachten 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.

- In Gruppenrichtlinien (Computereinstellungen) setzen Benutzerlayereinstellungen die Einstellungen für das Masterimage außer Kraft. Daher sind die Änderungen, die Sie unter "Computereinstellungen"mit einem Gruppenrichtlinienobjekt vornehmen, 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.

- Der letzte Benutzer, der sich bei einem Masterimage angemeldet hat, darf kein Domänenbenutzerkonto verwendet haben. Andernfalls treten auf den auf Basis dieses Images bereitgestellten Maschinen Probleme auf.
- Benutzerdefinierte Zertifikate bleiben nicht erhalten, wenn UPL in einer reinen Azure AD-Umgebung aktiviert ist. Ursache ist zugrunde liegendes Problem in Windows, das unter Azure ausgeführt wird. Wenn Microsoft dieses Problem in einer zukünftigen Verbesserung behebt, werden wir diesen Artikel aktualisieren.

## Komponenten entfernen

June 27, 2024

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 Apps and 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 im Verzeichnis `\x64\XenDesktop Setup` 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 Web Studio entfernt:

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /remove /components
webstudio
```

### Entfernen von VDAs über die Befehlszeile

Führen Sie im Verzeichnis `\x64\XenDesktop Setup` den Befehl `XenDesktopVdaSetup.exe` aus.

- Zum Entfernen einer oder mehrerer Komponenten verwenden Sie die Optionen `/remove` und `/components`. Mit `/remove /components vda,plugin` werden beispielsweise der VDA und die Citrix Workspace-App entfernt.
- Die Option `/removeall` entfernt nur den VDA. Die Citrix Workspace-App wird nicht entfernt.

Informationen zu Befehl und Parametern finden Sie unter Installieren über die Befehlszeile.

Nach dem Entfernen wird die Maschine in der Standardeinstellung automatisch neu gestartet.

Informationen zum Entfernen von VDAs mit einem Skript in Active Directory finden Sie unter Installieren oder Entfernen von VDAs mit Skripts.

## Upgrade und Migration

June 27, 2024

### Einführung

Bei Upgrades wird eine Bereitstellung auf Citrix Virtual Apps and Desktops 7 **Aktuelles Release (CR)** 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.

#### Upgradeübersicht

1. Lesen Sie den Artikel Upgrade einer Bereitstellung, bevor Sie mit dem Upgrade beginnen. Dies ist die Hauptinformationsquelle zum Vorbereiten und Ausführen von Upgrades.
2. Vergewissern Sie sich, dass Ihre aktuellen Customer Success Services-Daten gültig und nicht abgelaufen sind. Weitere Informationen finden Sie unter Verlängerungslizenzen für Customer Success Services.
3. Führen Sie die angegebene Vorbereitung aus.
4. Führen Sie Installationsprogramme aus, um Kernkomponenten zu aktualisieren.

5. Upgrade der Systemdatenbanken und der Site
6. Aktualisieren Sie VDAs auf Images (oder direkt auf Maschinen).
7. Führen Sie das Upgrade anderer Komponenten aus.

Alle Vorbereitungs- und Upgradeschritte werden unter Upgrade einer Bereitstellung erläutert.

### Mögliche Versionen für ein Upgrade

Sie können von folgender Software ein Upgrade auf Citrix Virtual Apps and Desktops 2402 LTSR durchführen:

- Virtual Apps and Desktops 2203 LTSR mit oder ohne CUs, bis einschließlich CU4
- Virtual Apps and Desktops 1912 LTSR mit oder ohne CUs, bis einschließlich CU8
- Derzeit unterstützte CR-Versionen von Citrix Virtual Apps and Desktops

Sie finden auch im [Citrix Upgrade Guide](/en-us/upgrade.html) eine Liste der Versionen von Citrix Virtual Apps and Desktops (sowie XenApp und XenDesktop) von denen ein Upgrade möglich ist.

> Hinweis:
>
> - Bevor der Upgrade-Vorgang gestartet wird, empfiehlt Citrix Kunden, das Upgrade in einer kontrollierten Umgebung zu testen und sicherzustellen, dass es ihren spezifischen Anforderungen entspricht. Darüber hinaus empfehlen wir, alle relevanten Produktdokumentationen, einschließlich der Liste der veralteten Versionen und bekannter Probleme, zu überprüfen, um einen reibungslosen Übergang zu gewährleisten. Dieser Ansatz trägt dazu bei, potenzielle Störungen der Produktionssysteme zu minimieren, und verbessert das allgemeine Upgrade-Erlebnis.
> - Citrix Virtual Apps and Desktops 1912 LTSR wird bald das Ende der Lebensdauer erreichen. Weitere Informationen zu unterstützten Versionen finden Sie in der Produktmatrix.

### 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?**

  Eine Abbildung und eine Beschreibung der empfohlenen Upgradereihenfolge 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](/en-us/upgrade).

- **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](https://www.citrix.com/support/product-lifecycle/milestones/citrix-virtual-apps-and-desktops.html).

- **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.

For details, see [Servicing Options]( https://www.citrix.com/support/citrix-customer-success-services/citrix-virtual-apps-and-desktops-servicing-options.html).

- **Muss ich meine Lizenzen aktualisieren?**

  Vergewissern Sie sich, 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 beachten Sie den Vorbereitungshinweise.

- **Welche Betriebssysteme werden unterstützt?**

  Der Artikel Systemanforderungen für die Version, auf die Sie aktualisieren, enthält die unterstützten Betriebssysteme.

  Wenn Ihre derzeitige Bereitstellung nicht mehr unterstützte Betriebssysteme umfasst, lesen Sie die Informationen unter Ältere Betriebssysteme.

- **Welche Versionen von VMware vSphere (vCenter + ESXi) werden unterstützt?**

  CTX131239 enthält eine Liste der unterstützten Hosts und Versionen sowie Links zu bekannten Problemen.

- **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 für Windows

## Weitere Informationen

[Long Term Service Release (LTSR)](https://www.citrix.com/support/citrix-customer-success-services/citrix-virtual-apps-and-desktops-servicing-options.html)

**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 2203 LTSR zum Beispiel, verwenden Sie den Link auf der Seite **Neue Features** für das neueste CU. Jede CU-Seite enthält Informationen zur unterstützten Version, Anweisungen und einen Link zum CU-Downloadpaket.

### Migrieren

#### Migrieren in die Cloud

Sie können die automatische Konfiguration verwenden, um eine lokale Citrix Virtual Apps and Desktops-Bereitstellung in die Cloud zu migrieren. Weitere Informationen finden Sie unter Migrieren in die Cloud.

#### Legacymigration

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.

Es gibt keine unterstützten Tools oder Skripts zum Migrieren von XenApp und XenDesktop-Versionen oder zum Migrieren älterer Citrix Virtual Apps and Desktops-Versionen. *Upgrades* werden für die im Citrix Upgrade Guide <!–aufgeführten Versionen von Citrix Virtual Apps and Desktops unterstützt und <!–> in dieser Produktdokumentation beschrieben.

Informationen zu früheren XenApp 6.x-Migrationsinhalten siehe unten. Weder die Skripts noch die Artikel werden unterstützt oder gepflegt.

- Open-Source-Migrationsskripts für XenApp 6.x sind auf https://github.com/citrix/xa65migrationtool verfügbar. Citrix unterstützt und pflegt diese Migrationsskripts nicht.
- Änderungen in 7.x
- Upgrade eines XenApp 6.5-Workers auf einen neuen VDA
- Migrieren von XenApp 6.x

## Upgrade einer Bereitstellung

June 27, 2024

## 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.

Stellen Sie vor dem Upgrade auf einen Citrix Virtual Apps and Desktops-Release sicher, dass Ihr aktuelles Customer Success Services-Abonnement noch nicht abgelaufen ist. Weitere Informationen finden Sie unter Verlängerungslizenzen für Customer Success Services.

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.

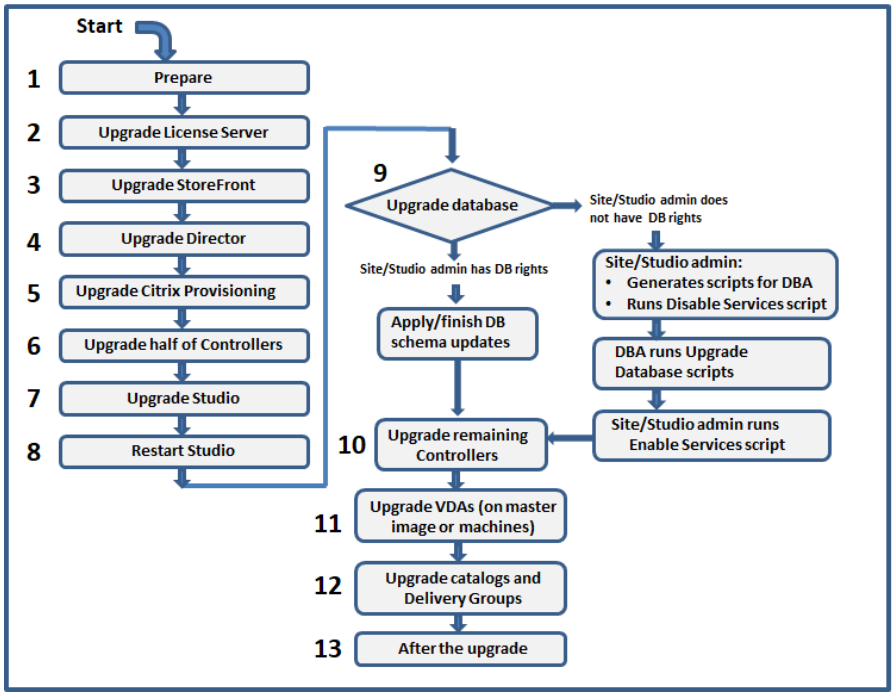
Sie können Upgrades aller Komponenten durchführen, die mit dem Komplettinstallationsprogramm (und den dedizierten VDA-Installationspaketen) installiert werden können, sofern eine neuere Version verfügbar ist. Informationen zu anderen Komponenten, die nicht mit dem Komplettinstallationsprogramm installiert 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.).

## Hybrid Rights-Lizenzen

Hybrid Rights-Lizenzen sind befristete Abonnementlizenzen, die zusätzlich zum Cloudabonnement bereitgestellt werden, wenn ein Kunde von einer unbefristeten Lizenz auf ein Cloudabonnement umsteigt. Sie können auch ein Hybrid Rights-Add-On für Ihr DaaS-Abonnement erwerben.

Wenn Sie eine Hybrid Rights-Lizenz mit einem SaaS-Attribute haben, haben Sie nach einem Upgrade auf Citrix Virtual Apps and Desktops LTSR 2203 und höher Zugriff auf Funktionen, die nicht mit Citrix Virtual Apps and Desktops LTSR 1912 verfügbar sind. Zu diesen Funktionen gehören das Provisioning und Hosting von Workloads in öffentlichen Clouds, wie Microsoft Azure, AWS EC2 und Google Cloud. Aktualisieren Sie den Lizenzserver vor dem Bereitstellen der neuen Lizenzdatei auf die aktuelle Version.

Wenn Sie Zugriff auf eine Hybrid Rights-Lizenz ohne SaaS-Attribut haben, führen Sie folgende Schritte aus, um Zugriff auf die neue Hybrid Rights-Lizenz mit SaaS-Attribut zu erhalten:

> **Hinweis:**
>
> - Sie erhalten eine E-Mail mit einem neuen Lizenzcode. Weitere Informationen finden Sie unter Mit Lizenzzugangscode.
> - Ihre vorhandenen Lizenzen sind annulliert. Annullierte Lizenzen müssen vom Lizenzserver gelöscht und dann neu installiert werden. Weitere Informationen finden Sie unter Löschen von Lizenzdateien.

1. Rufen Sie unter citrix.com das Portal zur Lizenzverwaltung auf und laden Sie die neue Hybrid Rights-Lizenzdatei mit aktivierten Cloudprovisioningrechten (SaaS-Attribut) herunter. Weitere Informationen finden Sie unter Lizenzen herunterladen. Die folgende Abbildung zeigt die Hybrid Rights-Lizenzdatei mit SaaS-Attribut im Increments-Abschnitt.


2. Installieren Sie die Hybrid Rights-Lizenzdatei auf dem Lizenzserver. Weitere Informationen finden Sie unter Lizenzen installieren.
3. Wenn sich Lizenzedition oder -modell ändern, müssen Sie zunächst mit dem Broker-Befehl die Edition und das Modell festlegen und dann das direkte Upgrade starten. Weitere Informationen zu Broker-Befehlen finden Sie im Abschnitt Broker PowerShell SDK.

Weitere Informationen zur Unterstützung öffentlicher Clouds in Citrix Virtual Apps and Desktops (aktuelles Release und Long Term Service Release) finden Sie unter CTX270373.

## 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:

- Persönliche vDisks, AppDisks und nicht unterstützte Hosts entfernen
- VDAs mit PvD- oder AppDisk-Komponenten
- 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 Web 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.

> **Hinweis:**
>
> Nach dem Upgrade von Web Studio werden die Versionsinformationen möglicherweise nicht sofort aktualisiert. Möglicherweise werden Sie aufgefordert, Web Studio zu aktualisieren, obwohl es bereits auf dem neuesten Stand ist. Um das Problem zu beheben, öffnen Sie im Web Studio-Server Internetinformationsdienste (IIS)-Manager, gehen Sie zu "Startseite > Websites > Standardwebsite"und wählen Sie unter "Website verwalten"die Option **Neu starten** aus.

#### Schritt 8: Studio neu starten

Starten Sie Web 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 Upgrade 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**.

> **Hinweis:**
>
> Um **Upgrade der übrigen Delivery Controller durchführen** verfügbar zu machen, erstellen Sie mindestens einen Maschinenkatalog und eine Bereitstellungsgruppe für die Site.

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.

### 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 Update für Ihre Bereitstellung durchführen, können Datenbankschemas aktualisiert werden. In der folgenden Tabelle sind die Datenbankschemas aufgeführt, die aktualisiert werden:

| From/To | 1912 CU1 | 1912 CU2 | 1912 CU3 | 1912 CU4 | 1912 CU5 | 2203 RTM | 2203 CU1 | 2203 CU2 | 2203 CU3 |
|---|---|---|---|---|---|---|---|---|---|
| 7.15 RTM/CU | Site; Monitor; config | Site; Monitor; config | Site; Monitor; config | Site; Monitor; config | Site; Monitor; config | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging |
| 1912 RTM | Config | Site; Config | Site; Config | Site; Monitor; config | Site; Monitor; config | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging |
| 1912 CU1 | | Site | Site; Config | Site; Monitor; config | Site; Monitor; config | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging |
| 1912 CU2 | | | Site; Config | Site; Monitor; config | Site; Monitor; config | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging |
| 1912 CU3 | | | | Site; Monitor; config | Site; Monitor; config | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging |
| 1912 CU4 | | | | | Site; Config | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging |
| 1912 CU5 | | | | | | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging |
| 1912 CU6 | | | | | | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging |
| 1912 CU7 | | | | | | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging |
| 2203 RTM | | | | | | | Config | Config | Config |
| 2203 CU1 | | | | | | | | Config | Config |
| 2203 CU2 | | | | | | | | | 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 2203 oder höher

Wurde die PvD-Komponente (persönliche vDisk) jemals auf einem VDA installiert, kann dieser nicht auf Version 2203 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 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 (2203 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.
2. Installieren Sie den neuen VDA.

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

> **Hinweis:**
>
> *Kann ich Personal vDisk mit Windows 7-Desktops in XenApp und XenDesktop 7.15 LTSR verwenden?*
>
> Citrix hat Personal vDisk (PvD) von XenApp und XenDesktop 7.6 LTSR ausgeschlossen. Dies wurde im Januar 2016 angekündigt. Darüber hinaus hat Citrix angekündigt, dass die PvD-Technologie ausläuft und empfiehlt, dass Kunden künftig Citrix App Layering verwenden. Citrix App Layering (Version 4.4 und höher) ist eine kompatible Komponente von XenApp und XenDesktop 7.15 LTSR. Um Kunden mit vorhandenen PvD-Bereitstellungen unter Windows 7 jedoch bei der Migration auf die Citrix App Layering-Technologie zu unterstützen, hat Citrix beschlossen, bis zum 14. Januar 2020 eine zeitlich begrenzte Unterstützung für PvD-Bereitstellungen für Windows 7-Desktops über XenApp und XenDesktop 7.15 LTSR Cumulative Updates (CUs) bereitzustellen. Die PvD-Komponente wird aus den LTSR-CUs entfernt und nach dem 14. Januar 2020 nicht mehr unterstützt. Darüber hinaus sind die LTSR-Sites nicht mehr konform, wenn PvD für Windows 7 über

> den 14. Januar 2020 hinaus verwendet wird. PvD für Windows 10 ist weiterhin von 7.15 LTSR ausgeschlossen. Daher sollten Kunden es nicht mit 7.15 LTSR-Sites verwenden.

### Persönliche vDisks, AppDisks und nicht unterstützte Hosts entfernen

Die folgenden Technologien und Hosttypen werden in Bereitstellungen mit dem aktuellen Release von Citrix Virtual Apps and Desktops 7 nicht unterstützt:

- **Persönliche vDisks (PvD)** zum Speichern von Daten neben Benutzer-VMs in Katalogen. Der Benutzerpersonalisierungslayer steuert jetzt die Benutzerpersistenz.
- **AppDisks** zum Verwalten von Anwendungen, die in Bereitstellungsgruppen verwendet werden.
- **Hosttypen:** Azure Classic, CloudPlatform (das ursprüngliche Citrix Produkt).
  - Informationen zu Hosttypen, die in dieser Version unterstützt werden, finden Sie unter Systemvoraussetzungen.
  - Weitere Informationen zu Möglichkeiten der Weiterverwendung von ARM und AWS finden Sie unter CTX270373.

Wenn Ihre aktuelle Bereitstellung persönliche vDisks oder AppDisks verwendet oder Verbindungen zu nicht unterstützten Hosttypen enthält (zum Beispiel Microsoft Azure Classic), können Sie erst dann ein Upgrade auf Version 2006 (oder höhere unterstützte Versionen) durchführen, wenn Sie die Elemente, die diese Technologien verwenden, entfernt haben. Wenn Ihre aktuelle Bereitstellung Verbindungen mit Hosts öffentlicher Clouds (z. B. AWS) enthält, müssen Sie vor dem Upgrade sicherstellen, dass Sie über eine Hybrid Rights-Lizenz verfügen. Wenn das Installationsprogramm eine nicht unterstützte Technologie oder Hostverbindung ohne Hybrid Rights-Lizenz erkennt, wird das Upgrade angehalten oder beendet und eine Meldung mit einer Erläuterung angezeigt. Die Installationsprotokolle enthalten die Details.

Zur Gewährleistung eines erfolgreichen Upgrades lesen Sie die Informationen zum Entfernen nicht unterstützter Elemente und folgen Sie den Anweisungen.

- PvDs entfernen
- AppDisks entfernen
- Nicht unterstützte Hostelemente entfernen

Selbst wenn Sie keine PvD oder AppDisks in Ihrer Bereitstellung verwenden, waren entsprechende MSI evtl. in früheren VDA-Installationen oder Upgrades enthalten. Vor einem Upgrade der VDAs auf Version 2006 (oder eine höhere unterstützte Version) müssen Sie diese Software entfernen, selbst wenn Sie sie nie verwendet haben. Wenn Sie die grafische Benutzeroberfläche verwenden, kann die Entfernung für Sie durchgeführt werden. Bei Verwendung der CLI können Sie Entfernungsoptionen hinzufügen. Weitere Informationen finden Sie unter Upgrade von VDAs mit PvD- oder AppDisk-Komponenten.

### PvDs entfernen

Ein Bereitstellungsupgrade ist erst möglich, wenn Sie alle Maschinen entfernen, die für die Verwendung von PvDs konfiguriert sind. Dies gilt für Kataloge und Bereitstellungsgruppen.

Zum Entfernen von PvDs aus Gruppen und Katalogen gehen Sie wie folgt vor:

1. Wenn eine Bereitstellungsgruppe Maschinen aus einem Katalog enthält, der PvDs verwendet, entfernen Sie diese über Studio aus der Gruppe.
2. Löschen Sie über Studio alle Kataloge mit Maschinen, die PvD verwenden.

**VDA-Upgrades:** Beim Bereitstellungsupgrade wird nicht erkannt, ob die AppDisk- oder PvD-Komponenten auf VDAs installiert sind. Die VDA-Installationsprogramme erkennen dies. Weitere Informationen finden Sie unter VDAs mit PvD- oder AppDisk-Komponenten.

Wenn Sie App Layering anstelle von PvDs verwenden möchten, lesen Sie die Informationen zum Verschieben von Daten unter Migrieren von PvD zu App Layering.

### AppDisks entfernen

Ein Bereitstellungsupgrade kann erst fortgesetzt werden, wenn Sie AppDisks aus allen Bereitstellungsgruppen entfernen, die diese verwenden, und dann die AppDisks selbst entfernen.

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Gruppe aus und klicken Sie im Aktionsbereich auf **AppDisks verwalten**.
3. Klicken Sie auf die Aktion, mit der die AppDisk aus der Gruppe entfernt wird.
4. Wiederholen Sie die Schritte 2 und 3 für jede Bereitstellungsgruppe, die AppDisks verwendet.
5. Wählen Sie im Studio-Navigationsbereich **AppDisks**.
6. Wählen Sie eine AppDisk aus und klicken Sie auf die Aktion, mit der die AppDisk gelöscht wird.
7. Wiederholen Sie die Schritte 5 und 6 für jede AppDisk.

**VDA-Upgrades:** Beim Bereitstellungsupgrade wird nicht erkannt, ob die AppDisk- oder PvD-Komponenten auf VDAs installiert sind. Die VDA-Installationsprogramme erkennen dies. Weitere Informationen finden Sie unter VDAs mit PvD- oder AppDisk-Komponenten.

### Nicht unterstützte Hostelemente entfernen

Ein Bereitstellungsupgrade auf Version 2006 (oder eine höhere unterstützte Version) ist nicht möglich, wenn die Site Verbindungen zu nicht unterstützten Hosttypen wie Citrix CloudPlatform oder Microsoft Azure Classic aufweist. Führen Sie vor einem Upgrade die folgenden Schritte aus.

In Studio:

- Löschen Sie alle Verbindungen zu nicht unterstützten Hosts.

- Enthält eine Bereitstellungsgruppe Maschinen aus einem Katalog, der mit einem Masterimage eines nicht unterstützten Hosts erstellt wurde, entfernen Sie die Maschinen aus der Gruppe.
- Löschen Sie alle Kataloge, die mit einem Masterimage eines nicht unterstützten Hosts erstellt wurden.

#### VDAs mit PvD- oder AppDisk-Komponenten

Wenn Komponenten, die PvD- und AppDisk-Technologien ermöglichen, auf einem VDA installiert sind, kann dieser erst aktualisiert werden, wenn die Komponenten entfernt wurden.

> **Hinweis:**
>
> Beim Upgrade auf Version 1912 mussten Sie den VDA deinstallieren und dann den neuen VDA installieren. In dieser Version werden Sie gefragt, ob Citrix die Komponente entfernen und das Upgrade dann fortsetzen soll.

AppDisk- und PvD-Komponenten wurden möglicherweise in früheren VDA-Versionen installiert, selbst wenn Sie sie nie verwendet haben:

- Grafische Benutzeroberfläche: In den VDA-Installationsprogrammen enthielt die Seite **Zusätzliche Komponenten** die Option **Citrix AppDisk/Persönliche vDisk**. 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 die Komponente installiert.
- CLI: Mit der Option `/baseimage` wurde die Komponente installiert.

**Aktion** Erkennt das VDA-Installationsprogramm keine AppDisk- oder PvD-Komponenten im aktuell installierten VDA, wird das Upgrade fortgesetzt.

Erkennt das Installationsprogramm AppDisk- oder PvD-Komponenten im aktuell installierten VDA:

- Grafische Benutzeroberfläche: Das Upgrade wird angehalten. In einer Meldung werden Sie gefragt, ob die nicht unterstützten Komponenten automatisch entfernt werden sollen. Wenn Sie auf **OK** klicken, werden die Komponenten automatisch entfernt und das Upgrade fortgesetzt.
- CLI: Um ein Fehlschlagen des Befehls zu vermeiden, schließen Sie die folgenden Optionen ein:
  - `/remove_appdisk_ack`
  - `/remove_pvd_ack`

### 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.

- Citrix Virtual Apps and Desktops (aktuelles Release):
  - 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.

- Informationen zu LTSRs finden Sie in den Komponentenlisten Ihrer LTSR- plus CU-Version. (Wählen Sie Ihre LTSR-Version auf der Hauptseite der Citrix Virtual Apps and Desktops-Produktdokumentation.)

### 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 V |
|---|---|---|---|
| Windows 7 und Windows 8 | VDA | 7.15 LTSR | 7.16 |
| Windows 7 und Windows 8 | Andere Installer-Komponenten | 7.17 | 7.18 |
| Windows 10-Versionen vor 1607 | VDA | 7.15 LTSR | 7.16 |
| Windows 10 x86 version | VDA | 1906.2.0 | 1909 |
| Windows Server 2008 R2 | VDA | 7.15 LTSR | 7.16 |
| Windows Server 2008 R2 | Andere Installer-Komponenten | 7.17 | 7.18 |
| Windows Server 2012 | VDA | 7.15 LTSR | 7.16 |
| Windows Server 2012 | Andere Installer-Komponenten | 7.17 | 7.18 |
| Windows Server 2012 R2 | Andere Installer-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 (Einschließlich interne Upgrades für Ihr Betriebssystem. Zum Beispiel Windows 10 Version 1903 auf Windows 10 Version 1909). Andernfalls wird die Citrix-Software nicht unterstützt. Installieren Sie dann die neue Komponente.
- Um das Betriebssystem auf einer VDA-Maschine ohne Reimaging zu aktualisieren, müssen Sie zunächst eine VDA-Version installieren, die von dem aktualisierten Betriebssystem unterstützt wird, oder nach dem Upgrade des Betriebssystems den VDA aktualisieren. Andernfalls wird die Citrix-Software nicht unterstützt. Sie können ein Upgrade auf die folgenden Mindestbetriebssystemversionen durchführen, wenn Sie ein direktes Upgrade durchführen, ohne den VDA zu deinstallieren:
  - Windows 11 mit installiertem kumulativen Update 2023-07 für Windows 11 (KB5028185) oder höher (Build 22621.1992 oder höher) .
  - Windows 10 mit installiertem dynamischem Update 2023-07 für Windows 10 (KB5028311).
- Wenn die Windows-Version, auf die Sie ein Upgrade durchführen möchten, nicht der oben genannten Richtlinie entspricht, müssen Sie den VDA vor dem Upgrade des Betriebssystems

deinstallieren und nach Abschluss des Betriebssystem-Upgrades eine unterstützte VDA-Version installieren.

**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.

> **Hinweis:**
>
> VDAs werden zwar später in der Aktualisierungsreihenfolge aktualisiert, doch ist es ratsam, vor einem Upgrade ein Installationsprogramm auszuwählen und das Verfahren zu überprüfen, damit Sie wissen, was Sie zu erwarten haben.

### Installationsprogramm und Schnittstelle auswählen

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).

- Kernkomponenten über die grafische Oberfläche installieren/aktualisieren
- Kernkomponenten über die Befehlszeile installieren/aktualisieren
- VDAs über die grafische Oberfläche installieren/aktualisieren
- VDAs über die Befehlszeile installieren/aktualisieren

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 das aktuelle 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 SQL Server Express LocalDB 2019 sein. Weitere Informationen zum Ersetzen von SQL Server Express LocalDB durch die 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. Das Datum muss mindestens 2021.11.15 sein.

#### Vergewissern Sie sich, dass Ihr Citrix Lizenzserver kompatibel ist

Vergewissern Sie sich, 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 auf dem Installationsmedium im Verzeichnis `XenDesktop Setup` folgenden Befehl aus: `.\LicServVerify.exe -h <license-server-fqdn> -p 27000 -v`. Der Bildschirm zeigt, 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.

#### Anwendungen und Konsolen schließen

Bevor Sie ein Upgrade durchführen, schließen Sie alle Programme, die Dateisperren verursachen können, einschließlich Verwaltungskonsolen und PowerShell-Sitzungen.

Das Neustarten der Maschine stellt sicher, dass alle Dateisperren aufgehoben werden und keine Windows-Updates ausstehen.

Vor Durchführung eines Upgrades beenden Sie Überwachungsdienste von Drittanbietern und deaktivieren Sie sie.

#### Sicherstellen, dass die erforderlichen Berechtigungen vorliegen

Auf den Maschinen, auf denen Sie die Produktkomponenten aktualisieren, müssen Sie sowohl Domänenbenutzer als auch lokaler Administrator sein.

Sitedatenbank und Site können automatisch oder manuell aktualisiert werden. Für ein automatisches Datenbankupgrade müssen die Berechtigungen des Studio-Benutzers die Berechtigung zum Aktualisieren des SQL Server-Datenbankschemas umfassen (z. B. Datenbankrolle `db_securityadmin` oder `db_owner`). Weitere Informationen finden Sie unter Datenbanken.

Hat der Studio-Benutzer diese Berechtigungen nicht, werden bei einem manuellen Datenbankupgrade Skripts generiert. Der Studio-Benutzer führt einige 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.
- Vergewissern Sie sich, dass Sie über eine Hybrid Rights-Lizenz verfügen, wenn Sie Verbindungen mit Hosts öffentlicher Clouds (z. B. AWS) hinzufügen möchten. Andernfalls wird der Vorabtest für die Site angehalten oder beendet, und es wird eine Meldung mit einer Erläuterung angezeigt.

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.

#### Tests ausführen

- 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. Das 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 das jeweilige 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 für die Sitedatenbank (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.

### SQL Server Express LocalDB ersetzen

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, vergewissern Sie sich, 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 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 Version SQL Server Express LocalDB 2019. Wenn Sie ursprünglich einen Delivery Controller einer Version vor 1912 installiert hatten und SQL Server Express LocalDB seitdem nicht durch die 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 2019.
- 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\NETWORKSERVICE"cmd
   ```

   Optional können Sie mit `whoami` überprüfen, ob die Eingabeaufforderung unter dem Netzwerkdienstkonto ausgeführt wird.

   ```
   whoami
   ```

   ```
   nt authority\networkservice
   ```

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`.

```
HADatabaseName.*
HADatabaseName_log.*
HAImportDatabaseName.*
HAImportDatabaseName_log.*
<!--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 2019. 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\150\Tools\Binn`.)
10. Starten Sie den Citrix Dienst für hohe Verfügbarkeit.
11. Vergewissern Sie sich, 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.

## Backup oder Migrieren der Konfiguration

June 27, 2024

Mit diesem Feature können Sie ein Backup Ihrer DaaS-Konfigurationen erstellen. Backups erleichtern die Migration der Konfigurationen von einer Cloudsite zu einer anderen. Sie ermöglichen auch die sofortige Wiederherstellung einer Site in Notfällen.
Sie können Backups auf folgende Weisen erstellen:

1. Backup + Wiederherstellen
   a) Integriert in WebStudio.
2. Automatisiertes Konfigurationstool (ACT)

a) PowerShell-basiertes Tool. Installieren Sie das Tool, um es zu verwenden.

Die Backups können verwendet werden für:

1. Wiederherstellung
2. Migration

Citrix empfiehlt die folgenden Tools für die beschriebenen Szenarien.

### Backup

| Umgebung | Anwendungsfall | Empfohlenes Tool | Besondere Erwägungen | Link |
|---|---|---|---|---|
| DaaS | On-Demand- und geplante Backups | Backup + Wiederherstellen | Citrix behält das Backup und der Benutzer kann es bei Bedarf herunterladen | Backup und Wiederherstellen in Studio |
| On-Premises | On-Demand-Backups | ACT | Der Benutzer behält das Backup | Backup und Wiederherstellung mit dem automatisierten Konfigurationstool |

### Migration

| Umgebung | Anwendungsfall | Empfohlenes Tool | Besondere Erwägungen | Link |
|---|---|---|---|---|
| On-Premises zur Cloud | On-Premises-Site zu DaaS migrieren | ACT | | On-premises zu Cloud migrieren |
| | Mehrere On-Premises-Sites zu einer DaaS-Site migrieren | ACT | Sites zusammenführen | Mehrere On-Premises-Sites in eine Cloudsite zusammenführen |

| Umgebung | Anwendungsfall | Empfohlenes Tool | Besondere Erwägungen | Link |
|---|---|---|---|---|
| On-Premises zu On-Premises | On-Premises-Site zu einer anderen On-Premise-Site migrieren | ACT | | POC Guide: Automated Configuration Tool – Migration von On-Premises- zu On-Premises-Site |
| | Mehrere On-Premises-Sites auf eine andere On-Premises-Site migrieren | ACT | Sites zusammenführen | POC Guide: Automated Configuration Tool – Migration von On-Premises- zu On-Premises-Site<br>Mehrere On-Premises-Sites in eine Cloudsite zusammenführen |
| Cloud zu Cloud | Eine DaaS-Site zu einer anderen DaaS-Site migrieren | ACT | | Von Cloud zu Cloud migrieren |
| Mehrere DaaS-Sites zu einer DaaS-Site konsolidieren | ACT | Sites zusammenführen | | Von Cloud zu Cloud migrieren<br>Mehrere On-Premises-Sites zu einer einzigen Cloudsite migrieren |

## Sicherheit

June 27, 2024

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 Multifaktorauthentifizierung für Windows oder eine bestimmte Anwendung. Mit der Multifaktorauthentifizierung 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/.

## FIDO2- und WebAuthn-Authentifizierung

June 27, 2024

### Lokale Autorisierung und virtuelle Authentifizierung mit FIDO2 und WebAuthn

Auf Geräten mit TPM 2.0 und Windows Hello können Benutzer sich in ihrer virtuellen Sitzung bei Anwendungen, die FIDO2 oder WebAuthn verwenden, mit FIDO2-Sicherheitsschlüsseln und integrierter Biometrie authentifizieren.

Weitere Informationen zu FIDO2 finden Sie unter FIDO2: WebAuthn & CTAP.

Weitere Informationen zur Verwendung dieses Features finden Sie unter FIDO2-Umleitung.

> **HINWEIS**
>
> Das Feature unterstützt allerdings nicht die Anmeldung bei virtuellen Sitzungen mit WebAuthn oder FIDO2. Es ermöglicht lediglich die Verwendung dieser Authentifizierungsmethoden für Anwendungen innerhalb einer virtuellen Sitzung.
>
> Dieses Feature wird nicht in Double-Hop-Szenarios unterstützt.

### Unterstützungsmatrix

| Betriebssystem des Sitzungshosts | Authentifizierung bei Webanwendungen | UWP-Anwendungsauthentifizierung |
|---|---|---|
| Windows Server 2016 | Über USB-Umleitung unterstützt | Nicht unterstützt |
| Windows Server 2019 | Unterstützt | Nicht unterstützt |
| Windows Server 2022 | Unterstützt | Unterstützt |
| Windows 10 | Unterstützt | Unterstützt |
| Windows 11 | Unterstützt | Unterstützt |

Weitere Informationen finden Sie in den folgenden Anforderungen.

## Authentifizierung bei Webanwendungen

### Anforderungen

Im Folgenden werden die Voraussetzungen für die Verwendung der FIDO2- und der WebAuthn-Authentifizierung bei Webanwendungen aufgeführt:

#### Citrix Steuerungsebene

- Citrix Virtual Apps and Desktops 2009 oder höher

#### Sitzungshost

- Betriebssystem
  - Windows 10 1809 oder höher
  - Windows Server 2019 oder später
- VDA
  - Windows: Version 2009 oder später

#### Clientgerät

- Betriebssystem
  - Windows 10 1809 oder höher
  - Linux: Siehe Systemanforderungen der Workspace-App für Linux.
- Workspace-App

  - Windows: Version 2009.1 oder später
  - Linux: 2303 oder später

#### Anforderungen an den Webbrowser

- Nur 64-Bit-Browser

#### Unterstützte Authentifizierungsmethoden

- FIDO2-Sicherheitsschlüssel
- Windows Hello
  - TPM 2.0
  - Integrierte Biometrie
    - Gesichtserkennung
    - Fingerabdruckscanner
  - WebAuthn

### UWP-Anwendungsauthentifizierung

Mit der Veröffentlichung von Citrix Virtual Apps and Desktops 2112 unterstützt Citrix die WebAuthn- und FIDO2-Authentifizierung bei UWP-Anwendungen.

Anwendungen wie Microsoft Teams, Microsoft Outlook für Office 365 und OneDrive verwenden eine UWP-Anwendung zur Authentifizierung als Link zu Azure Active Directory. Citrix unterstützt jetzt FIDO2 zur Authentifizierung dieser Anwendungen.

#### Anforderungen

Im Folgenden werden die Voraussetzungen für die Verwendung der FIDO2- und der WebAuthn-Authentifizierung bei UWP-Anwendungen aufgeführt:

#### Citrix Steuerungsebene

- Citrix Virtual Apps and Desktops 2112 oder später

#### Sitzungshost

- Betriebssystem
  - Windows 10 1809 oder höher

  - Windows Server 2022 oder später
- VDA
  - Windows: Version 2112 oder höher

**Clientgerät**

- Betriebssystem
  - Windows 10 1809 oder höher
  - Linux: Siehe Systemanforderungen der Workspace-App für Linux.
- Workspace-App
  - Windows: Version 2009.1 oder später
  - Linux: 2303 oder später

**Unterstützte Authentifizierungsmethoden**

- FIDO2-Sicherheitsschlüssel
- Windows Hello
  - TPM 2.0
  - Integrierte Biometrie
    - Gesichtserkennung
    - Fingerabdruckscanner
  - WebAuthn

> **Hinweis:**
>
> In Szenarien, in denen die FIDO2-Umleitung nicht verfügbar ist, weil die Funktion von Client, VDA oder Betriebssystem nicht unterstützt wird, können USB-basierte FIDO2-Schlüssel mithilfe der USB-Umleitung umgeleitet werden.
> In Szenarien mit verfügbarer FIDO2-Umleitung kann auch eine USB-Umleitung zur Umleitung von USB-basierten FIDO2-Schlüsseln verwendet werden. In diesem Fall müssen Sie die FIDO2-Umleitung deaktivieren und die entsprechenden USB-Umleitungsregeln konfigurieren.
> Einzelheiten zur Konfiguration der USB-Umleitungsregeln finden Sie in der Dokumentation zur Konfiguration von USB-Umleitungsgeräten.

## Citrix Virtual Apps and Desktops und Citrix Gateway integrieren

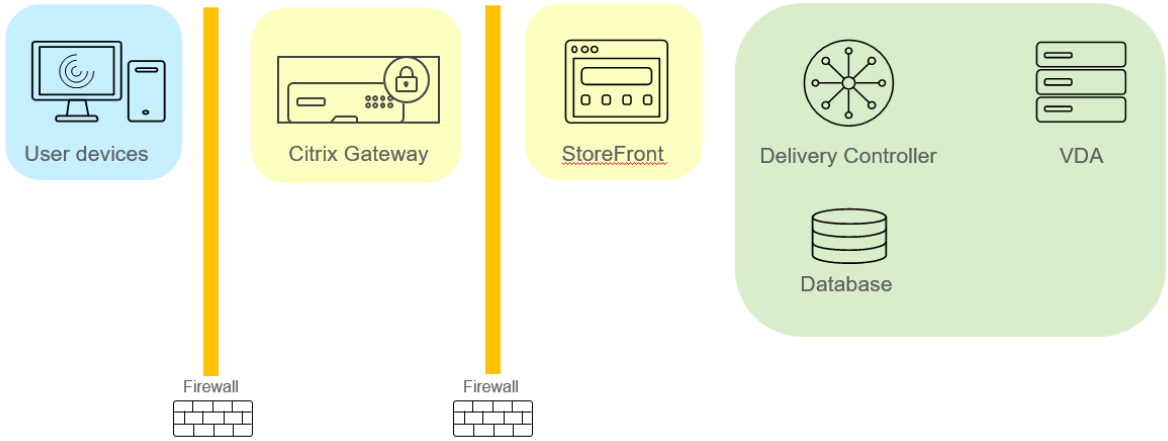
June 27, 2024

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.

## Bewährte Methoden und Überlegungen zur Sicherheit

June 27, 2024

> **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, wie 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 Konfigurieren von TLS finden Sie unter Transport Layer Security (TLS).

Übernehmen Sie die für Windows empfohlenen bewährten Methoden bei der Benutzerkontenverwaltung. Erstellen Sie kein Konto auf einer Vorlage oder einem Image, bevor dieses durch Maschinenerstellungsdienste (MCS) oder Provisioning Services dupliziert wurde. Planen Sie keine Aufgaben mit gespeicherten privilegierten Domänenkonten. Erstellen manuell Sie keine freigegebenen Active Directory-Computerkonten. Durch diese Vorgehensweise wird verhindert, dass ein lokales permanentes Kontokennwort für einen Angriff unter Anmeldung bei mit MCS bzw. PVS freigegebenen Images Anderer verwendet wird.

#### 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 Config Synchronizer-Dienst erfordert, dass das NETWORK SERVICE-Konto zur Gruppe der lokalen Administratoren auf dem Delivery Controller gehört. Dies gestattet dem lokalen Hostcache den einwandfreien Betrieb.

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. Erstellen 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.

## Smartcards

June 27, 2024

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 müssen. 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 das Schnelle-Smartcard-Feature 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 smartcardäquivalenter 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 möglicherweise 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. Das Smartcard-Middlewarepaket bietet erweiterte Features. 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-Feature

Das Schnelle-Smartcard-Feature ist eine Verbesserung gegenüber der alten HDX PC/SC-basierten Smartcardumleitung. Das Feature verbessert die Leistung, wenn Smartcards in WANs mit hoher Latenz verwendet werden. Wenn die Latenz hoch ist, kann die Leistungsverbesserung erheblich sein (z. B. 15 Sekunden für eine Schnelle-Smartcard-Anmeldung unter Windows im Vergleich zu mehr als 1 Minute bei der PC/SC-basierten Smartcardumleitung).

Das Schnelle-Smartcard-Feature sind standardmäßig auf Hostmaschinen mit derzeit unterstützten Windows-VDAs aktiviert. Um das Schnelle-Smartcard-Feature 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 das Schnelle-Smartcard-Feature auf dem Client zu aktivieren, fügen Sie den ICA-Parameter "SmartCardCryptographicRedirection"in die Datei *default.ica* der zugehörigen StoreFront-Site ein:

```
[WFClient]
SmartCardCryptographicRedirection=On
```

Darüber hinaus kann das Schnelle-Smartcard-Feature auf der Clientseite mit den folgenden Registrierungseinstellungen zwangsweise aktiviert oder deaktiviert werden (z. B. zu Diagnosezwecken):

- HKLM\SOFTWARE[\WOW6432Node]\Citrix\ICA Client\SmartCard\ForceEnableCryptographicRedirection (als ein DWORD-Wert, der nicht Null ist)

Oder

- HKLM\SOFTWARE[\WOW6432Node]\Citrix\ICA Client\SmartCard\ForceDisableCryptographicRedirection (als ein DWORD-Wert, der nicht Null ist)

Die 32-Bit-Registrierungsstruktur muss angegeben werden (mit `WOW6432Node`), wenn der Clientcomputer 64-Bit ist.

Einschränkungen:

- Nur die Citrix Workspace-App für Windows unterstützt das Schnelle-Smartcard-Feature Wenn Sie das Schnelle-Smartcard-Feature in der Datei default.ica konfigurieren, verwenden Citrix Workspace-Apps für andere Betriebssysteme als Windows weiterhin die alte PC/SC-Umleitung.
- Das Schnelle-Smartcard-Feature unterstützt nur das Double-Hop-Szenario ICA > ICA, mit aktivierter Smartcard auf beiden Hops. Da das Schnelle-Smartcard-Feature keine ICA > RDP-Double-Hops unterstützt, funktioniert ein solches Szenario nicht.
- Das Schnelle-Smartcard-Feature unterstützt Cryptography Next Generation nicht. Daher unterstützt das Schnelle-Smartcard-Feature keine Smartcards mit Elliptic Curve Cryptography (ECC).
- Das Schnelle-Smartcard-Feature unterstützt nur Schlüsselcontaineroperationen mit Schreibschutz.
- Das Schnelle-Smartcard-Feature unterstützt das Ändern der Smartcard-PIN nicht.

Ab VDA-Version 2203 und Citrix Workspace-App-Version 2202 für Windows (oder höher) ist das Schnelle-Smartcard-Feature mit Cryptography Next Generation (CNG) kompatibel. Darüber hinaus werden Elliptic Curve Cryptography (ECC)-Smartcards mit den folgenden Kurven unterstützt: P-256, P-384, P-521 Bit, sowohl für ECDSA als auch für ECDH.

Ab VDA-Version 2203 bietet das Schnelle-Smartcard-Feature die Möglichkeit, die Smartcard-PIN zwischen den Anwendungen aus der Anmeldesitzung desselben Benutzers zwischenzuspeichern. Wenn beispielsweise **Sitzungs-PIN-Caching** aktiviert ist und der Endbenutzer seine Smartcard-PIN bereit in Outlook angegeben hat und Word dann zum Signieren eines Dokuments verwendet wird, verwendet Word die bereits zwischengespeicherte Smartcard-PIN (an Outlook gesendet). Das **Sitzungs-PIN-Caching** unterstützt die Benutzererfahrung, da die Smartcard-PIN weniger oft eingegeben werden muss. Wenn die Smartcard für die Anmeldung am VDA verwendet wird, kann die Windows-Smartcard-Anmelde-PIN optional im **Sitzungs-PIN-Cache**gespeichert werden. Dies kann die Benutzererfahrung noch weiter verbessern.

Das **Zwischenspeichern der Sitzungs-PIN** ist standardmäßig deaktiviert. Es kann mit den folgenden Registrierungseinstellungen auf dem VDA aktiviert und gesteuert werden:

In HKLM\SOFTWARE\Citrix\SmartCard:

- `EnablePinSessionCache` als DWORD (ungleich Null zum Aktivieren)
- `EnableLogonPinSessionCache` als DWORD (ungleich Null zum Aktivieren)
- `PinSessionCacheEntryStaleTimeout` als DWORD (Anzahl der Sekunden, bis ein Eintrag veraltet ist, der Standardwert ist 1 Stunde)

### 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 Smart-

card eingeführt wird. In der DK-Norm (Deutsche Kreditwirtschaft) sind vier Kontaktkartenleserklassen festgelegt.

- Smartcardleser der Klasse 1 sind die häufigsten Geräte und haben normalerweise 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 eingebauter sicherer Zehnertastatur 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 Zehnertastatur 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 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 die Smartcard bereits im Leser ist, müssen sie auf "Abbrechen"klicken.
- Wenn Benutzer aufgefordert werden, eine PIN einzugeben, müssen sie die PIN neu 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 Smartcards in Internet Explorer unter Windows 10 verwenden. 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 ihre 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).

### Zähler für Zugriff auf Smartcardleser

Mit Smartcard-Remoting können Sie verfolgen, wie oft eine Smartcard in einem Lesegerät eingesteckt oder entfernt wurde, unter Verwendung der Funktion "SCardGetStatusChange". Die Funktion aktualisiert ein Array von SCARD_READERSTATE-Datenstrukturen —je eine pro Lesegerät, das Sie überwachen. High Word (16 Bit) des dwEventState-Datenfelds für jedes SCARD_READERSTATE enthält die Anzahl der Lesegeräte. Weitere Informationen finden Sie in den Microsoft-Artikeln SCardGetStatusChangeA-Funktion und SCARD_READERSTATEA-Struktur.

Die Einstellung **Reader Insert Count Reporting** ist standardmäßig deaktiviert. Zum Aktivieren der Überwachung fügen Sie folgenden Registrierungsschlüssel hinzu:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartCard

Name: EnableReaderInsertCountReporting

Typ: DWORD

Wert: Beliebiger Wert ungleich Null

Sobald die Sitzung getrennt wird, wird der Zähler zurückgesetzt auf Null.

**Reader Insert Count Reporting** ist kompatibel mit Smartcard-Middleware von Drittanbietern.

## Smartcardbereitstellungen

June 27, 2024

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 |

| Typ | Verbindung mit StoreFront |
| --- | --- |
| 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

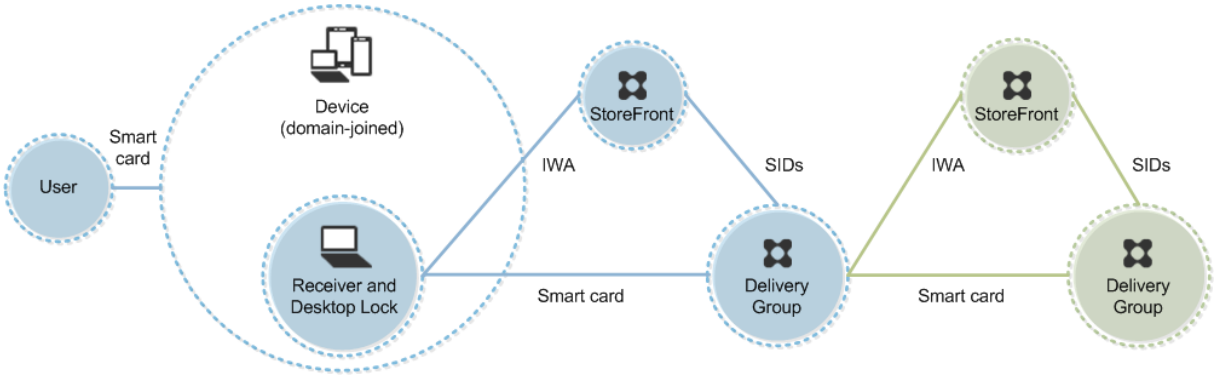
Wenn die Überprüfung von Zertifikatsperrlisten aktiviert ist und ein Benutzer führt eine Smartcard mit einem ungültigen Zertifikat in einen Smartcardleser ein, kann der Benutzer nicht authentifiziert werden oder nicht auf den mit dem Zertifikat verbundenen Desktop oder die Anwendung zugreifen. Bei

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.



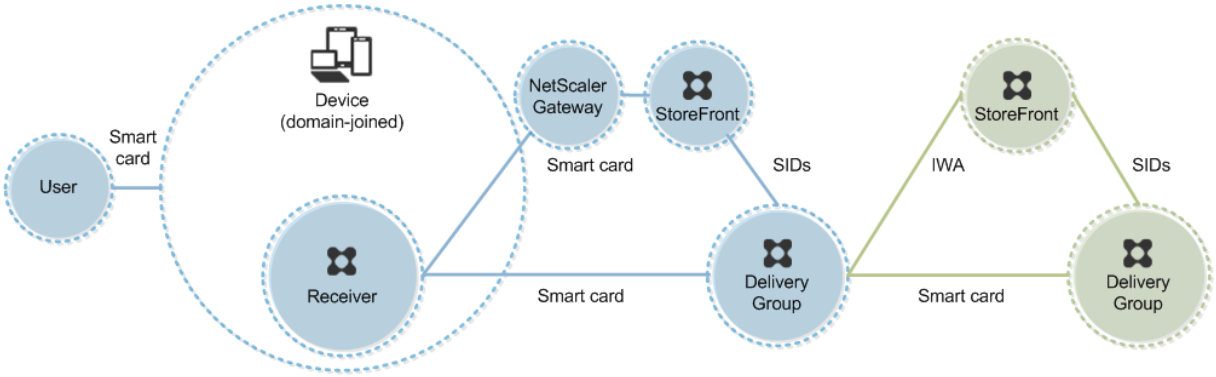

Zum Anmelden beim Gerät benötigt der Benutzer eine Smartcard und eine PIN. Der Benutzer wird dann durch Receiver beim Storefront-Server mittels integrierter Windows-Authentifizierung (IWA) authentifiziert. StoreFront übergibt die Sicherheits-IDs (SIDs) an Citrix Virtual Apps oder Citrix Virtual Desktops. 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.



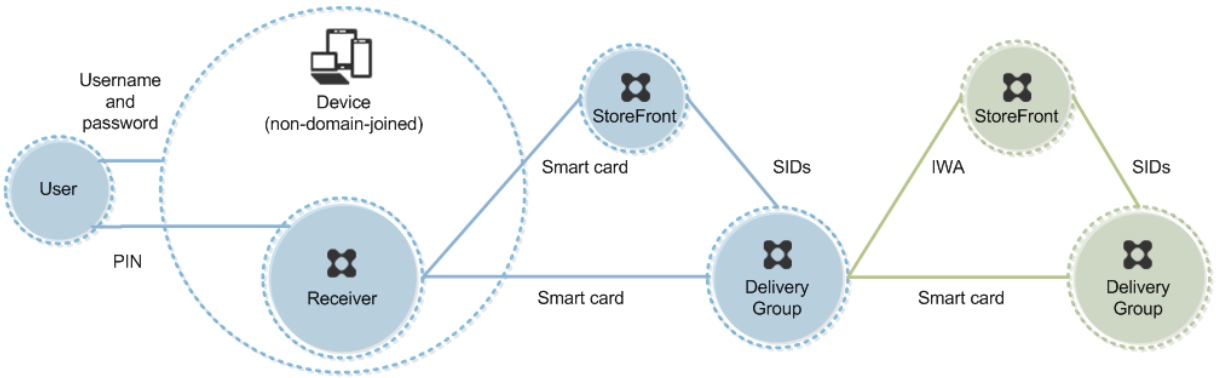

Der Benutzer meldet sich mit Smartcard und PIN beim Gerät und anschließend erneut bei Citrix Gateway oder Access Gateway an. Die zweite Anmeldung kann entweder mit Smartcard und PIN oder einem Benutzernamen und einem Kennwort erfolgen, da Receiver in dieser Bereitstellung eine bimodale Authentifizierung 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.



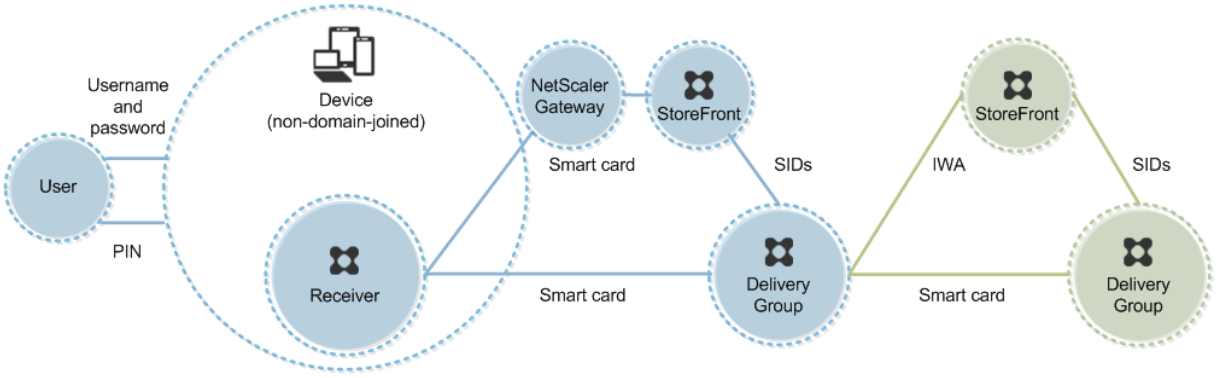
Ein Benutzer meldet sich beim Gerät an. Normalerweise muss er seinen Benutzernamen und das Kennwort eingeben, aber da das Gerät nicht Mitglied einer Domäne ist, sind die Anmeldeinformationen für diese Anmeldung optional. Da bimodale Authentifizierung in dieser Bereitstellung möglich ist, fordert Receiver 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.

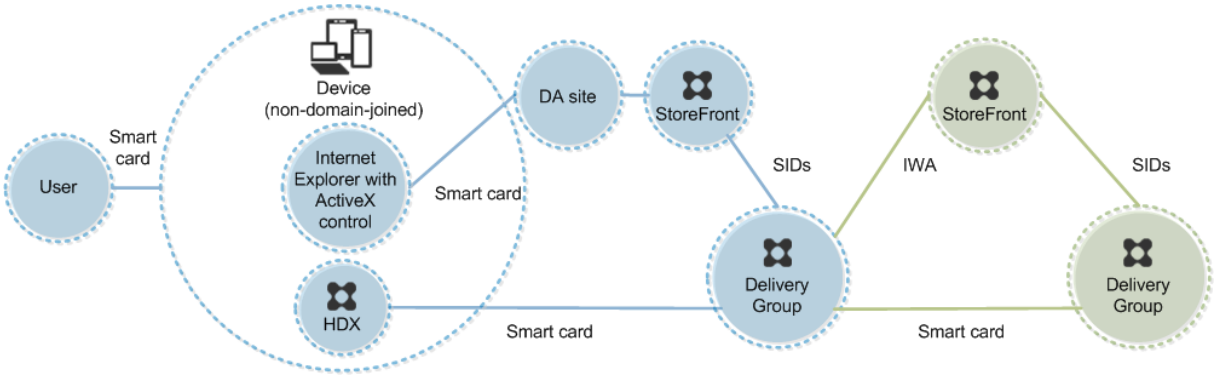
 

Diese Bereitstellung kann um einen zweiten StoreFront-Server und einen Server mit gehosteten Anwendungen auf ein Double-Hop-System erweitert werden. Ein Receiver auf dem virtuellen Desktop übernimmt die Authentifizierung beim zweiten StoreFront-Server. Für diese zweite Verbindung kann eine beliebige 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

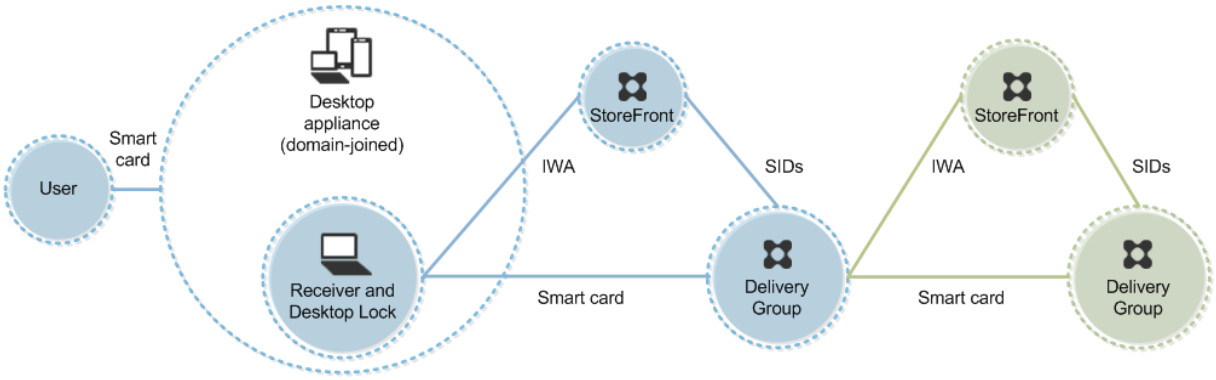
 

eine beliebige Authentifizierungsmethode verwendet werden. Die für den ersten Hop dargestellte Konfiguration kann im zweiten Hop wiederverwendet oder nur für den zweiten Hop verwendet werden.

### 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

June 27, 2024

## 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 27, 2024

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. Erstellen 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

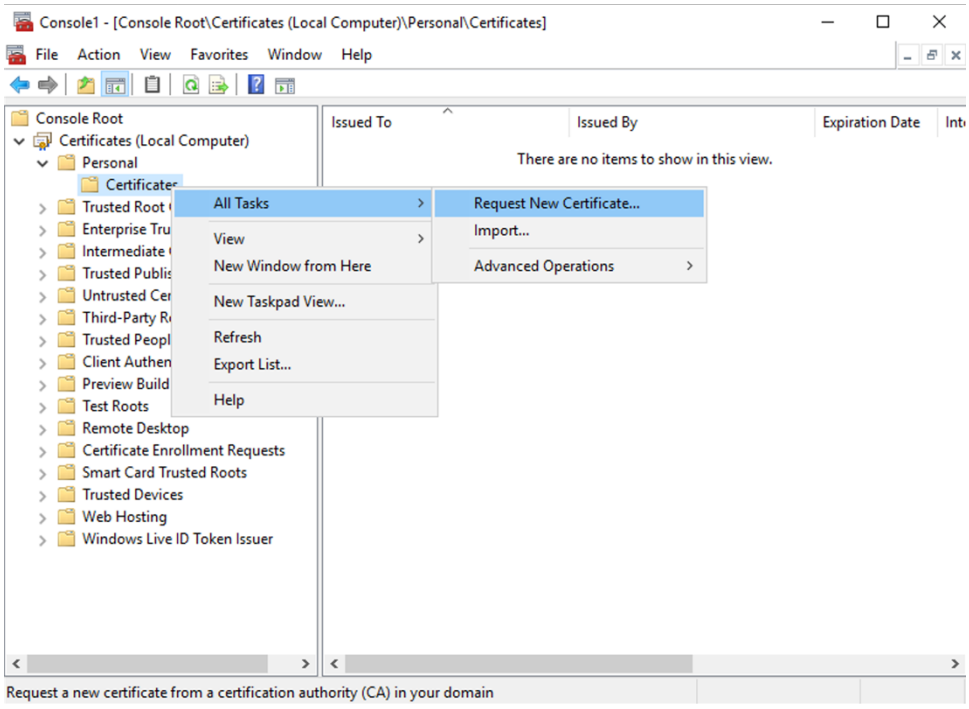
Für HTTPS wird TLS vom XML-Dienst über Serverzertifikate, nicht aber über Clientzertifikate unterstützt. In diesem Abschnitt wird das Beschaffen und Installieren von TLS-Zertifikaten für Delivery Controller beschrieben. Die gleichen Schritte können auf Cloud Connectors zum Verschlüsseln des STA- und 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

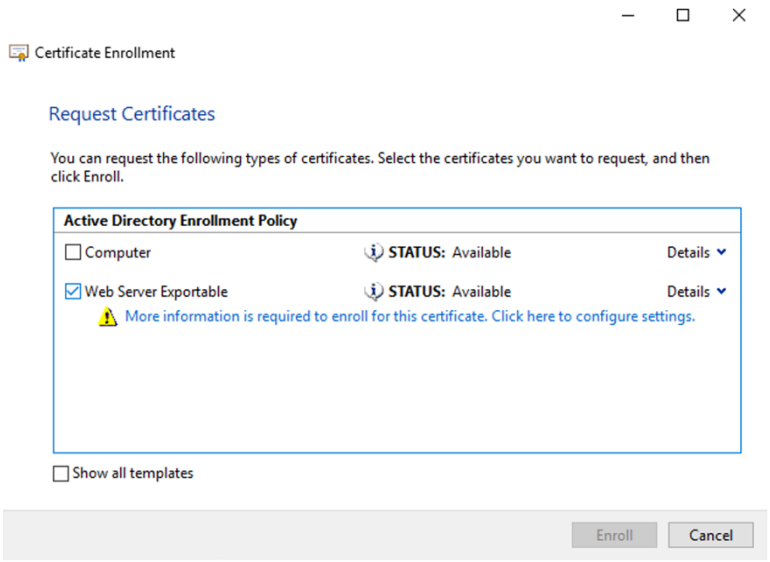
1. Öffnen Sie auf dem Delivery Controller die MMC-Konsole und fügen Sie das Zertifikat-Snap-In hinzu. Wählen Sie bei Aufforderung "Computerkonto"aus.
2. Erweitern Sie **Persönlich > Zertifikate** und verwenden Sie dann den Kontextmenübefehl **Alle Aufgaben > Neues Zertifikat anfordern**.




3. Klicken Sie auf **Weiter** und erneut auf **Weiter**, um zu bestätigen, dass Sie das Zertifikat von der Active Directory-Registrierung erwerben.

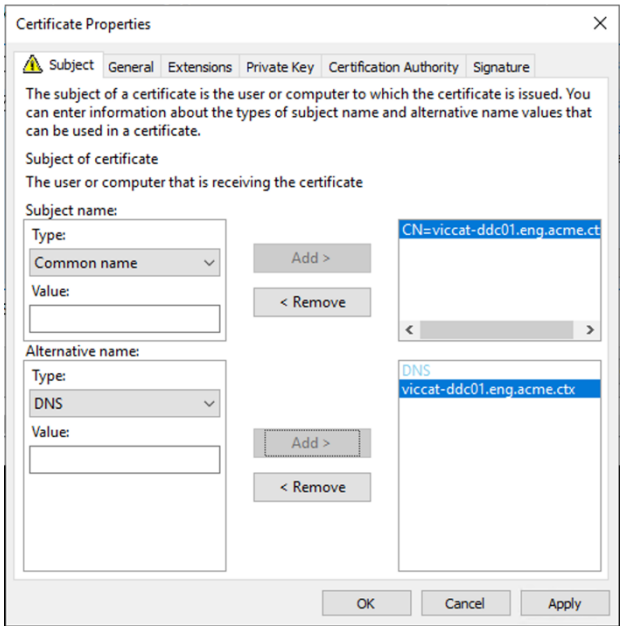
4. Wählen Sie die Vorlage für das Zertifikat “Serverauthentifizierung”aus. Wenn die Vorlage automatisch einen Antragsteller enthält, können Sie auf **Registrieren** klicken, ohne weitere Details anzugeben.




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 zu konfigurieren und das Zertifikat für die Verschlüsselung zu verwenden:

```
$IPV4_Address = Test-Connection -ComputerName $HostName -Count 1
    | Select-Object -ExpandProperty IPV4Address

$IPPort = "$($IPV4_Address):443"
```

```
4
5 $SSLxml = "http add sslcert ipport=$IPPort certhash=$Thumbprint
     appid={
6  $Formatted_Guid }
7  "
8
9 $SSLxml | netsh
10
11 . netsh http show sslcert
12 <!--NeedCopy-->
```

Bei korrekter Konfiguration zeigt die Ausgabe des letzten Befehls `.netsh http show sslcert`, dass der Listener den richtigen `IP:port` verwendet und dass `Application ID` der Anwendungs-GUID des Brokerdiensts entspricht.

Sofern die Server dem auf den Delivery Controllern installierten Zertifikat vertrauen, können Sie jetzt StoreFront-Delivery Controller und Citrix Gateway STA-Bindungen zur Verwendung von HTTPS anstelle von HTTP konfigurieren.

> **Hinweis:**
>
> Ist der Controller unter Windows Server 2016 und StoreFront unter Windows Server 2012 R2 installiert, muss die Reihenfolge der TLS-Verschlüsselungssammlungen auf dem Controller 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) enthalten. Diese 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` vor `TLS_DHE_`-Verschlüsselungssammlungen steht.

Siehe auch Prioritizing Schannel Cipher Suites auf Microsoft-MSDN.

### Ändern von HTTP- oder HTTPS-Ports

Der XML-Dienst auf dem Controller hört standardmäßig Port 80 auf HTTP-Datenverkehr und Port 443 auf HTTPS-Datenverkehr ab. Zwar können auch andere Ports verwendet werden, jedoch wird der Controller dabei nicht vertrauenswürdigen Netzwerken ausgeliefert, und es entsteht ein Sicherheitsrisiko. Das Bereitstellen eines eigenständigen StoreFront-Servers ist dem Ändern der Standardwerte vorzuziehen.

Zum Ändern der vom Controller verwendeten standardmäßigen HTTP- oder HTTPS-Ports führen Sie den folgenden Befehl in Studio aus:

```
BrokerService.exe -WIPORT \<http-port> -WISSLPORT \<https-port>
```

<http-port> ist die Portnummer für HTTP-Datenverkehr und <https-port> 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:

```
1 Get-ConfigRegisteredServiceInstance -ServiceType Broker -Binding
     XML_HTTPS |
2 Unregister-ConfigRegisteredServiceInstance
3 Get-BrokerServiceInstance | where Binding -eq "XML_HTTPS" |
4 Register-ConfigServiceInstance
5 <!--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:

- **Für TLS zu verwendendes 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 TLS-Protokollversionen unterliegen einer Hierarchie (von der niedrigsten zur höchsten Version): SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2 und TLS 1.3. 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 1.3-Protokollverbindungen zugelassen. Wenn Sie SSL 3.0 als Mindestversion angeben, sind Verbindungen für alle unterstützten Versionen zulässig. Wenn Sie TLS 1.3 als Mindestversion angeben, werden nur TLS 1.3-Verbindungen zugelassen.

  DTLS 1.0 entspricht TLS 1.1 und DTLS 1.3 entspricht TLS 1.3.
- **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 Informa-

tionen 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 | ALL | COM | GOV | ALL | COM | GOV |
|---|---|---|---|---|---|---|
| **FIPS-Modus** | Aus | Aus | Aus | Ein | Ein | Ein |
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384* | | | | X | | X |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | | | | X | | X |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA | | | | X | X | |

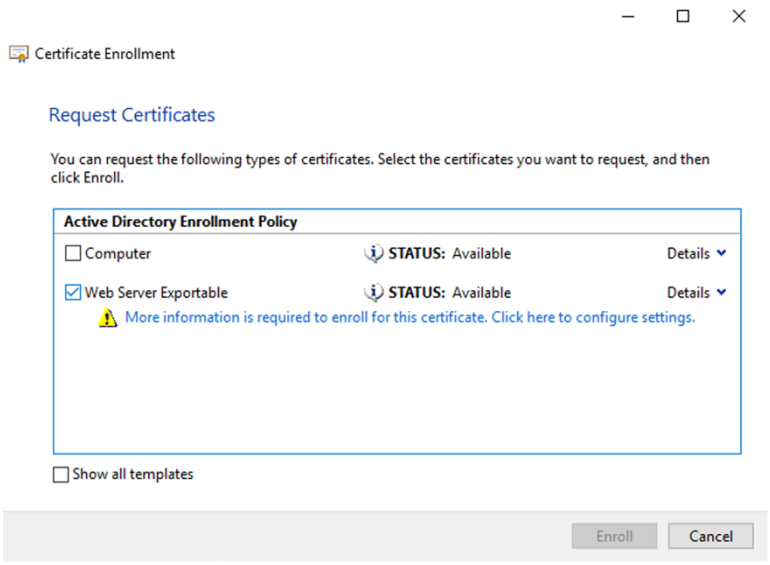
*Unter Windows Server 2012 R2 nicht unterstützt.

> **Hinweis:**
>
> Der VDA unterstützt keine DHE-Verschlüsselungssammlungen (z. B. TLS_DHE_RSA_WITH_AES_256_GCM_SHA3 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, können sie möglicherweise nicht von Receiver verwendet werden.
>
> 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.

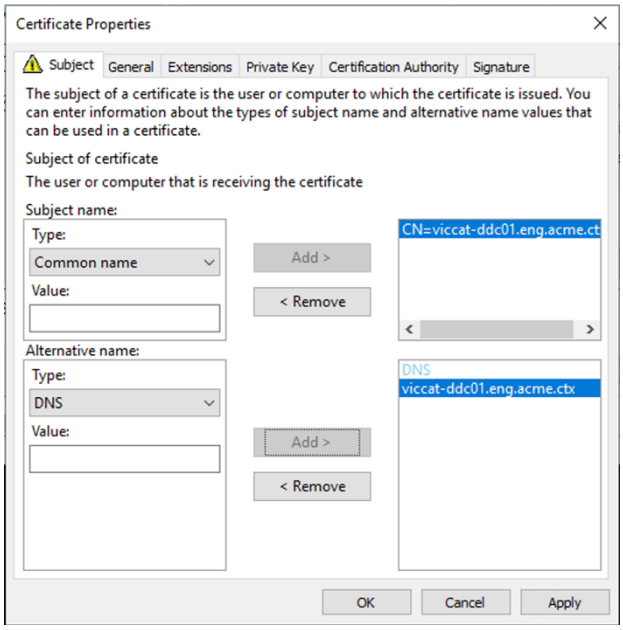
 




5. Um weitere Details für die Zertifikatvorlage anzugeben, klicken Sie auf **Details** und konfigurieren Sie Folgendes:

   **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.



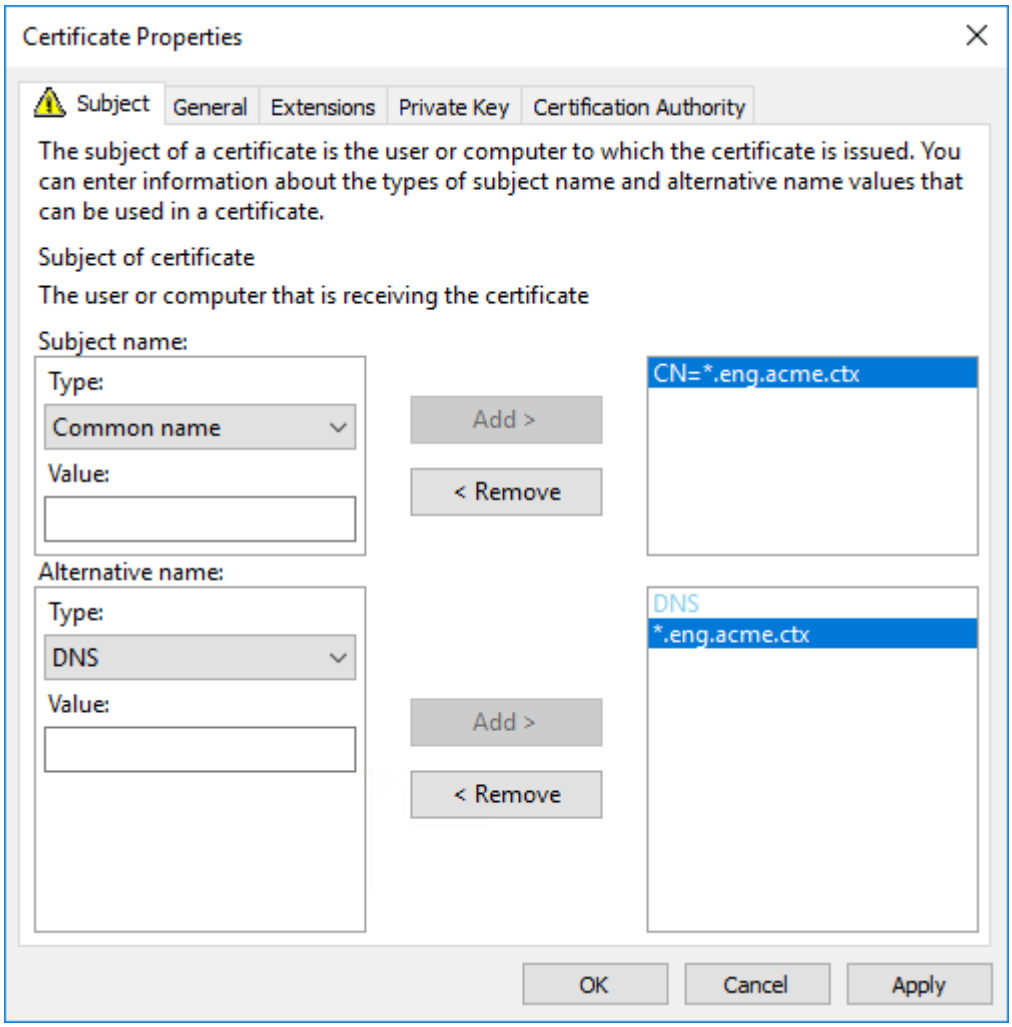

> **Hinweis:**
>
> Verwenden Sie die automatische Registrierung von Active Directory-Zertifikatdienste-Zertifikaten zur Automatisierung des Ausstellens und Bereitstellens von Zertifikaten für die VDAs. Das Verfahren wird unter https://support.citrix.com/article/CTX205473 erläutert.

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.

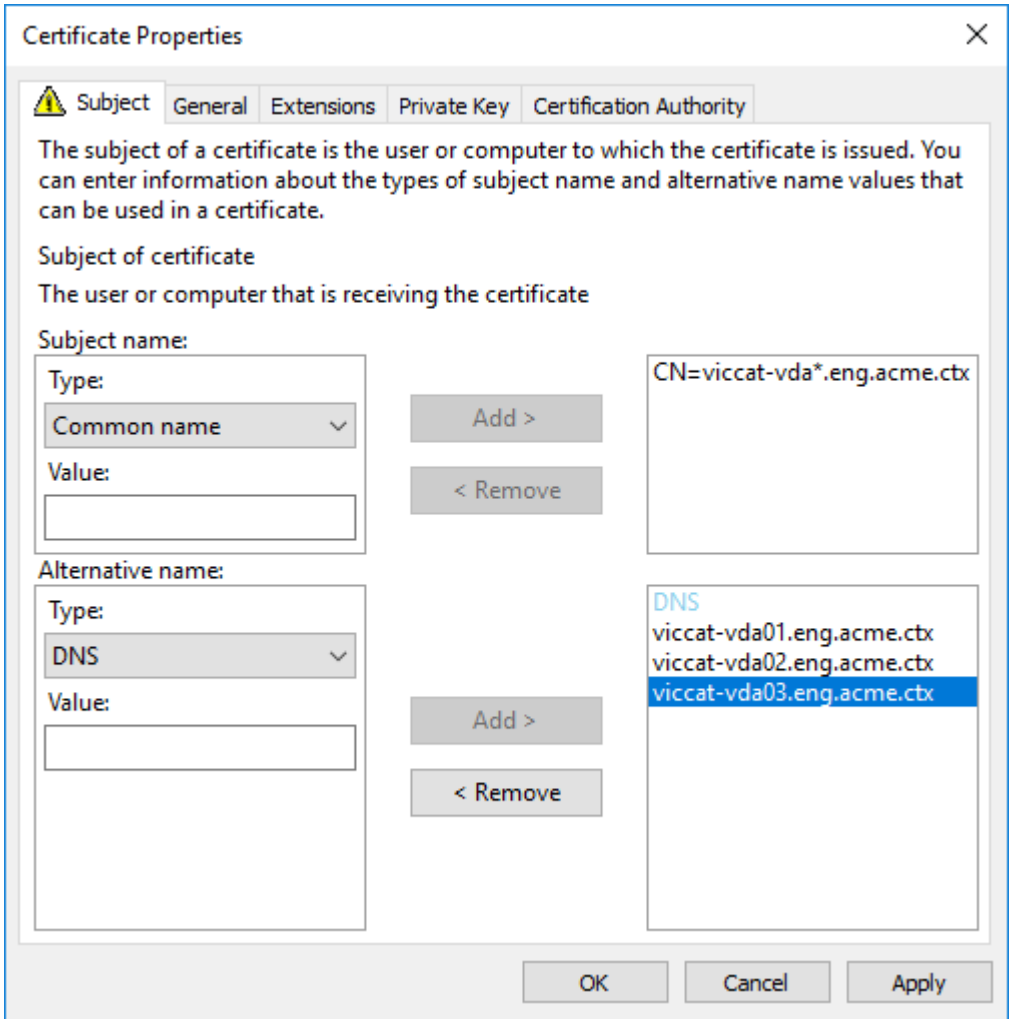



Sie können SAN-Zertifikate verwenden, um mehrere spezifische VDAs mit einem einzelnen Zertifikat zu schützen:

**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.

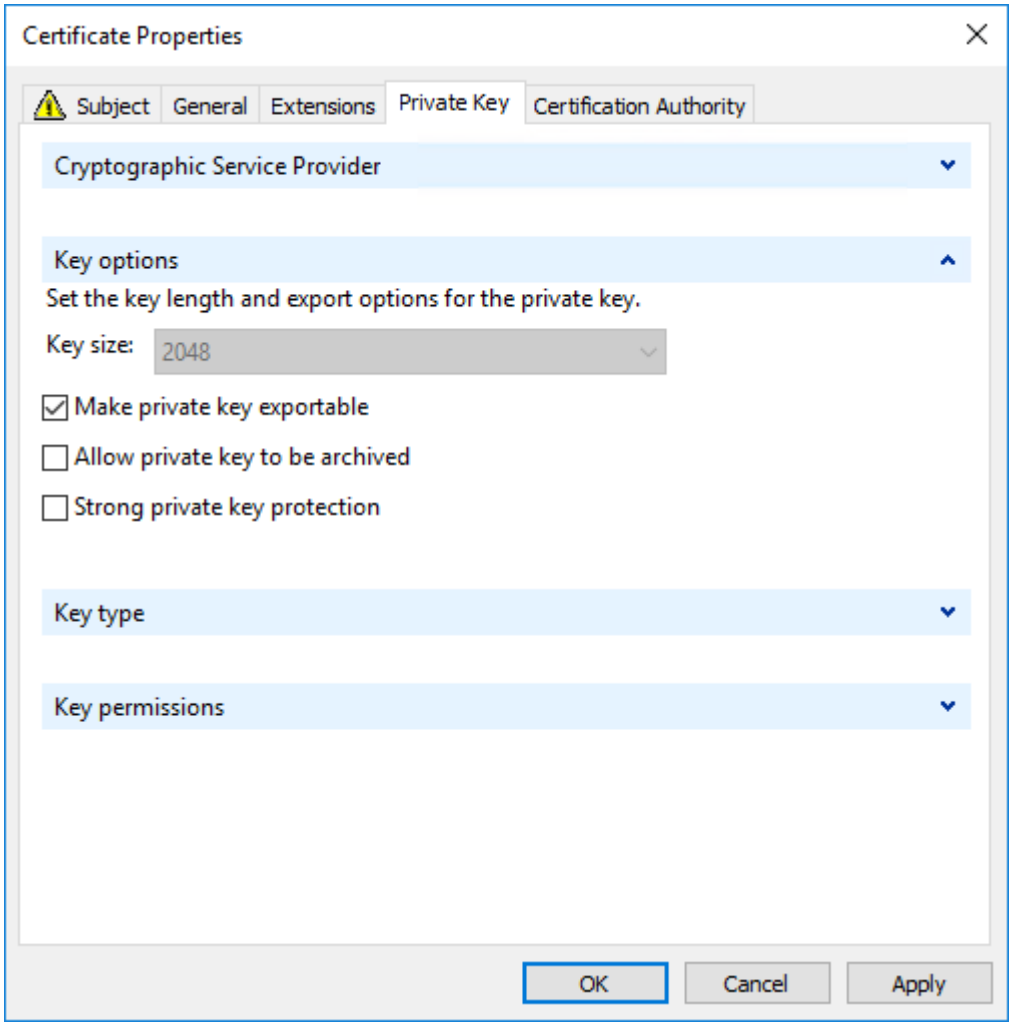
 




**Hinweis:**

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 |
|---|---|
| Aktivieren | 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_1.3”. |
| 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_1.3"
-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 1.3. 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 Receiver für Windows (Version 4.6 bis 4.9), 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. Dies betrifft alle Citrix Receiver-Versionen.

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:

- die Citrix Receiver-Version den adaptiven HDX-Transport und DTLS unterstützt (Receiver für Windows 4.7, 4.8, 4.9, Receiver für Mac 12.5, 12.6, 12.7, Receiver für iOS 7.2, 7.3.x und Receiver für Linux 13.7)

und 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 von Citrix Receiver fehlschlagen:

- Aktualisieren Sie Citrix Receiver für Windows auf Version 4.10 oder höher, Receiver für Mac auf Version 12.8 oder höher bzw. Receiver für iOS auf Version 7.5 oder höher.
- 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:**
>
> Ein geeignetes Update für Receiver für Linux ist noch nicht verfügbar. Receiver für Android (Version 3.12.3) unterstützt den adaptiven HDX-Transport und DTLS über Citrix Gateway nicht und ist daher nicht betroffen.
>
> 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. Erstellen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

### Arten von Druckverbindungen zwischen VDA und universellem Druckserver

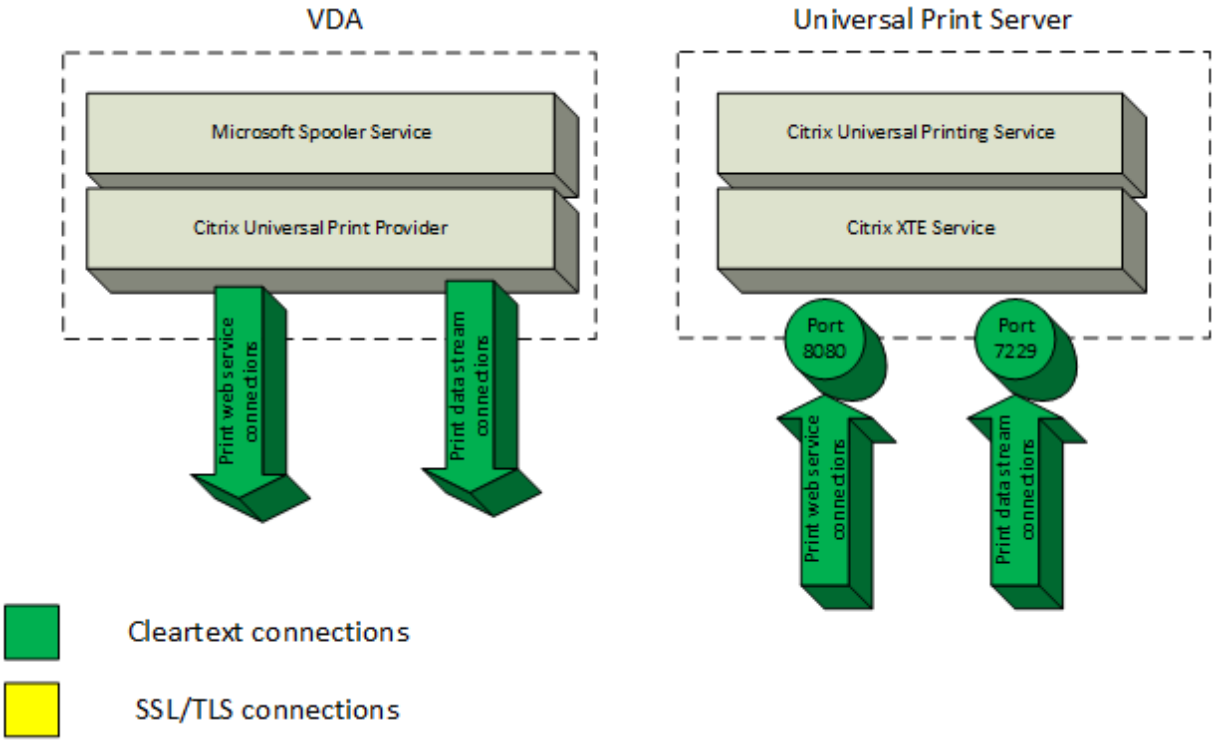
#### Klartextverbindungen

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.

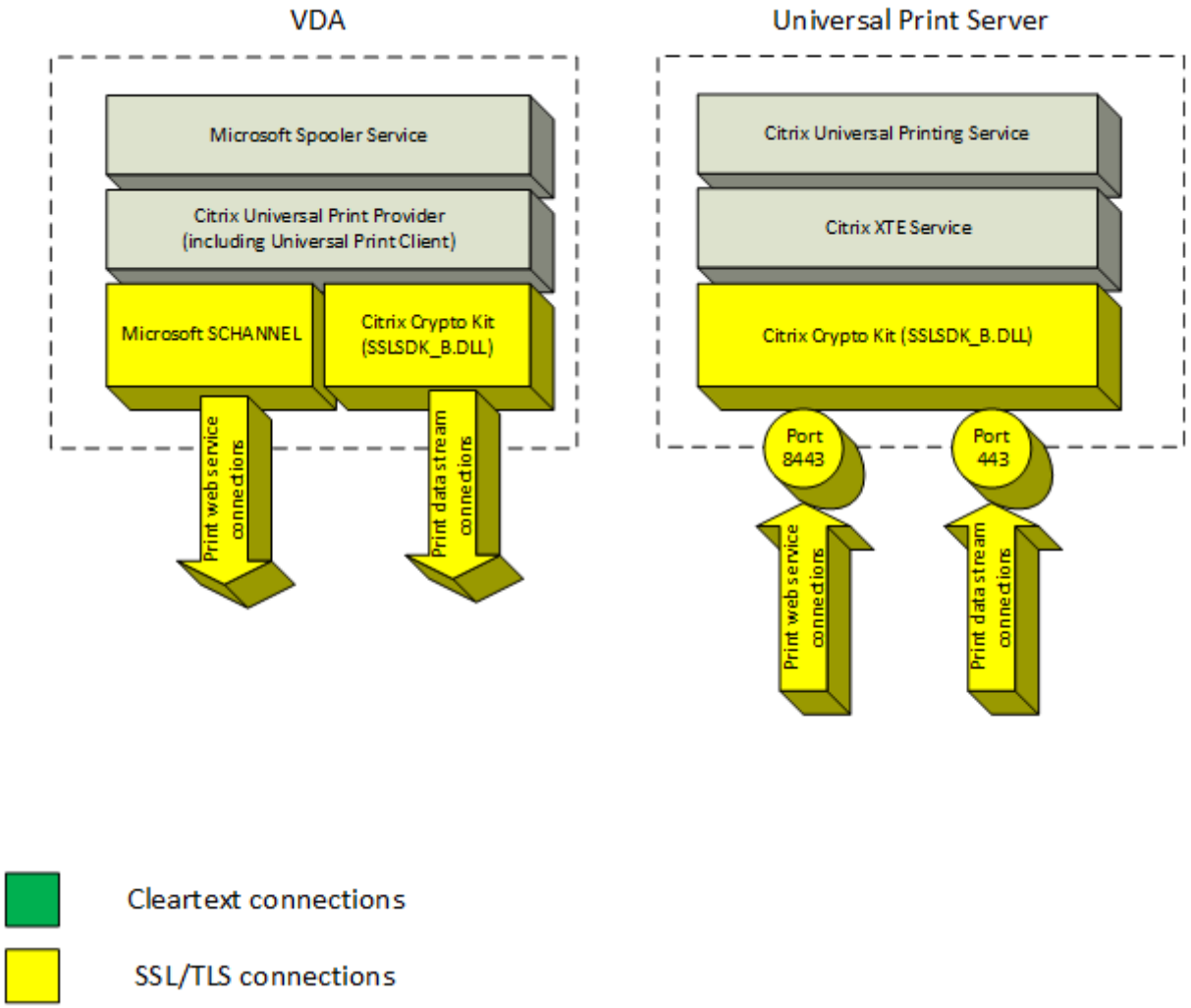



**Verschlüsselte Verbindungen**

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 im Gruppenrichtlinien-Editor **Computerkonfiguration > Administrative Vorlagen > Netzwerk > SSL-Konfigurationseinstellungen > Reihenfolge der SSL-Verschlüsselungssammlungen** auf. Wählen Sie die folgende Reihenfolge, wenn TLS 1.3 festgelegt ist:

TLS_AES_256_GCM_SHA384
TLS_AES_128_GCM_SHA256

Wählen Sie die folgende Reihenfolge, wenn TLS 1.2 festgelegt ist:

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:

- Für TLS zu verwendendes 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 1.3 und 1.2. Geben Sie die niedrigste zulässige Version an.

Die Standardversion des TLS-Protokolls ist 1.2.

> **Hinweis:**
>
> TLS 1.1 und 1.0 werden ab Citrix Virtual Apps and Desktops Version 2311 nicht mehr unterstützt.

- 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 | 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

```
Enable-UpsSSL.ps1 -Enable [-HTTPPort <port>] [-CGPPort <port>] [-
    HTTPSPort <port>] [-CGPSSLPort <port>] [-SSLMinVersion <version>] [-
    SSLCipherSuite <name>] [-CertificateThumbprint <thumbprint>] [-
    FIPSMode <Boolean>] [-ComplianceMode <mode>]
Enable-UpsSSL.ps1 -Disable [-HTTPPort <portnum>] [-CGPPort <portnum>]
```

| Parameter | Beschreibung |
|---|---|
| Aktivieren | 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. |
| SSLMinVersion "<version>" | Mindestversion des TLS-Protokolls zwischen Anführungszeichen. Gültige Werte: "TLS_1.2" und "TLS_1.3". Standard: TLS_1.2. |

| Parameter | Beschreibung |
| --- | --- |
| 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 in der Microsoft-Dokumentation.

### Aktivieren des FIPS-Modus auf dem Client

Führen Sie auf dem Delivery Controller Web 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

Legen Sie in Web Studio die Citrix Richtlinieneinstellung **SSL FIPS-Modus** auf **Aktiviert** 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.

> **Hinweis:**
>
> Der FIPS-Modus wird nicht unterstützt, wenn die SSL-Protokollversion auf TLS 1.3 eingestellt ist.

### Konfigurieren der SSL/TLS-Protokollversion

Die Standardversion des SSL/TLS-Protokolls ist TLS 1.2. TLS 1.2 und TLS 1.3 sind die empfohlenen SSL/TLS-Protokollversionen für den Produktionseinsatz. 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 oder TLS 1.3 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 1.2 oder TLS 1.3** 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 Datei (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.

## Positivliste für virtuelle Kanäle

June 27, 2024

Die Positivliste für virtuelle Kanäle ist ein Feature, mit dem Sie steuern können, welche virtuellen Kanäle, die nicht von Citrix stammen, in Ihrer Umgebung zulässig sind. Die Positivliste für virtuelle Kanäle ist standardmäßig aktiviert. Daher dürfen in Sitzungen von Citrix Virtual Apps and Desktops nur virtuelle Citrix Kanäle geöffnet werden. Ist die Verwendung benutzerdefinierter virtueller Kanäle erforderlich (eigener oder derer eines Dritten), müssen diese der Positivliste hinzugefügt werden.

### Konfiguration

Die Positivliste für virtuelle Kanäle ist standardmäßig deaktiviert. Sie können dieses Feature mithilfe der folgenden Einstellungen in der Citrix-Richtlinie konfigurieren:

- **Positivliste für virtuelle Kanäle**: um die Funktion zu aktivieren oder zu deaktivieren und virtuelle Kanäle zur Liste hinzuzufügen.
- **Protokolldrosselung für virtuelle Kanäle** –**Positivliste**: legt den Einschränkungszeitraum für die Protokollierung von Listenereignissen für virtuelle Kanäle fest.
- **Positivliste für die Protokollierung**: legt die Protokollierungsstufe für die Positivliste virtueller Kanäle fest.

### Hinzufügen virtueller Kanäle zur Positivliste

Sie benötigen die folgenden Informationen, um einen virtuellen Kanal zur Positivliste hinzuzufügen, benötigen:

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. Wenn es mehrere Prozesse gibt, können Sie diese Prozesse hinzufügen, indem Sie sie durch Kommas trennen.

#### Für einzelne Prozesse

Im Fall der o. g. Beispiele würden Sie der Liste den folgenden Eintrag hinzufügen:

```
CTXCVC1,C:\Program Files\Application\run.exe
```

#### Für mehrere Prozesse

Im Fall mehrerer Prozesse fügen Sie den folgenden Eintrag hinzu:

```
CTXCVC1,C:\Program Files\Application\run.exe,C:\Program Files\Application
\run2.exe
```

#### Platzhalter verwenden

Die Verwendung von Platzhaltern (*) wird unterstützt. Sie können Platzhalter verwenden, wenn sich die Namen von Verzeichnissen oder ausführbaren Dateien entsprechend der Version der Anwendung ändern oder wenn die Drittanbieterkomponente in den Benutzerprofilen installiert ist.

Sie können Platzhalter in den folgenden Szenarien verwenden:

- Um den vollständigen Verzeichnisnamen zu ersetzen.
  Beispiel:`C:\Program Files\Application\*\run1.exe`
- Um einen Teil des Verzeichnisnamens zu ersetzen.
  Beispiel:`C:\Program Files\Application\v*\run1.exe`
- Um den Namen der ausführbaren Datei zu ersetzen.
  Beispiel:`C:\Program Files\Application\v1.2\*.exe`
- Um einen Teil des Namens der ausführbaren Datei zu ersetzen.
  Beispiel:`C:\Program Files\Application\v1.2\run*.exe`

Es gelten die folgenden Einschränkungen:

- Der Platzhalter kann nur als Ersatz für ein einzelnes Verzeichnis verwendet werden. Beispiel: Die ausführbare Datei befindet sich in `C:\Program Files\Application\v1.2\run1.exe`
  - Zulässig: `C:\Program Files\Application\*\run1.exe`

  - Nicht zulässig: `C:\Program Files\*\run1.exe`

- Die Einträge müssen die Dateinamenserweiterung enthalten.
  - Zulässig: `C:\Program Files\Application\v1.2\*.exe`
  - Nicht zulässig: `C:\Program Files\Application\v1.2\*`
- Alle Pfade müssen lokale Pfade sein.

> **Hinweis:**
>
> - Netzwerkpfade sind nicht zulässig.
> - Wildcard-Unterstützung ist ab Citrix Virtual Apps and Desktops 2206 verfügbar.
> - Wildcard-Unterstützung ist in Citrix Virtual Apps and Desktops 2203 LTSR ab CU2 verfügbar.

#### Systemumgebungsvariablen verwenden

Sie können Systemumgebungsvariablen verwenden, um die Definition der vertrauenswürdigen Prozesse in Ihrer Positivliste zu vereinfachen. Sie können jede der vorbereiteten Variablen wie, %`programfiles`%, %`programfiles(x86)`%, %`systemdrive`% und %`systemroot`%.

Sie können auch benutzerdefinierte Umgebungsvariablen verwenden, sofern sie auf Systemebene definiert sind.

Die folgenden Beispiele zeigen sofort einsatzbereite Umgebungsvariablen:

- `%programfiles%\Application\v1.2\run.exe`
- `%programfiles%\Application\*\run.exe`
- `%programfiles(x86)%\Application\v1.*\run.exe`

Das folgende Beispiel zeigt eine benutzerdefinierte Systemumgebungsvariable:

- Name der benutzerdefinierten Variablen: `app`
- Wert der benutzerdefinierten Variablen: `%programfiles%\Application\`
- Eintrag in Positivliste: `CTXCVC1,%app%\run.exe`

> **Hinweis:**
>
> Benutzerumgebungsvariablen werden nicht unterstützt.
>
> Die Unterstützung von Umgebungsvariablen ist ab Version 2209 von Citrix Virtual Apps and Desktops verfügbar.

### Namen und Prozesse virtueller Kanäle erhalten

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 erhalten, indem Sie die Protokolle des Features anwenden und die folgenden Schritte einhalten:

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 und den Prozess, der ihn zu öffnen versucht: Weitere Informationen zu verfügbaren Ereignissen finden Sie unter Ereignisprotokolle.
3. Melden Sie sich von der Sitzung ab.
4. Fügen Sie in der Richtlinieneinstellung für die Positivliste virtueller Kanäle einen Eintrag für den gefundenen virtuellen Kanal und den Prozess hinzu.
5. Starten Sie die Maschine neu.
6. Sobald der VDA registriert ist, führen Sie die virtuelle Anwendung oder den virtuellen Desktop aus, um zu überprüfen, ob die benutzerdefinierten virtuellen Kanäle erfolgreich geöffnet werden.

## 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

Wenn Sie einen anderen Media Player als Windows Media Player als System-Media Player verwenden, müssen Sie ihn als vertrauenswürdigen Prozess zur Positivliste hinzufügen. Folgende Informationen sind für den Eintrag in der Positivliste erforderlich:

- Name des virtuellen Kanals: `CTXMM`
- Prozess: Pfad zu dem auf dem VDA verwendeten Media Player. Beispiel: `C:\Program Files (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 Positivliste 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:\Program Files\Microsoft Office\root\Office16\lync.exe`.
- Eintrag in Positivliste: `CTXRMEP,C:\Program Files\Microsoft Office\root\Office16\lync.exe`

## WebSocket-Kommunikation zwischen VDA und Delivery Controller

June 27, 2024

In diesem Artikel wird beschrieben, wie Sie eine WebSocket-Verbindung für die Kommunikation zwischen VDAs und Delivery Controllern einrichten.

### Übersicht

Das WebSocket-Protokoll funktioniert über das Citrix Brokering Protocol und ermöglicht eine stabile Kommunikation zwischen Delivery Controllern und VDAs.
Die Verwendung des WebSocket-Protokolls für die Kommunikation bietet die folgenden Vorteile:

- Erfordert nur den TLS-Port 443 für die Kommunikation vom VDA zum Delivery Controller.
- Bietet nahtlose und zuverlässige Kommunikationskanäle zwischen VDAs und Delivery Controllern.

### Funktionsweise

Im folgenden Abschnitt wird der Workflow für die WebSocket-Verbindung zwischen einem Delivery Controller und einem VDA beschrieben:

1. Administratoren von Citrix Virtual Apps and Desktops initiieren den Prozess, indem sie VDAs mithilfe des Machine Creation Service (MCS) bereitstellen.
2. Während des MCS-Bereitstellungsprozesses generiert MCS öffentlich-private Schlüsselpaare für jeden VDA und registriert die öffentlichen Schlüssel beim FMA-Vertrauensdienst auf dem Delivery Controller. MCS speichert das öffentlich-private Schlüsselpaar als Datei unter dem Identitätsdatenträger auf den VDAs.
3. Wenn die VDA-Maschine gestartet wird, liest der auf der VDA-Maschine installierte MCS-Agent das Schlüsselpaar vom Identitätsdatenträger und schreibt diese Informationen in den Speicherort der VDA-Registrierung.

4. Der auf dem VDA installierte Broker Agent liest die Schlüsselpaare aus der Registrierung und generiert eine SSL-fähige WebSocket-Anforderung an den Delivery Controller, wobei der Dienstschlüssel durch den privaten Schlüssel signiert ist.
5. Der Delivery Controller verifiziert den signierten Service Key Authorization Header mit dem öffentlichen Schlüssel des FMA Trust Service.
6. Sobald die Überprüfung abgeschlossen ist, stellt das System die WebSocket-Verbindung zwischen dem VDA und dem Delivery Controller her.

## WebSocket-Unterstützung für AD-verbundene VDAs

### Voraussetzungen

1. Konfigurieren Sie Ihre Site. Weitere Informationen finden Sie unter Site erstellen.
2. Installieren Sie TLS-Zertifikate auf den Delivery Controllern. Weitere Informationen finden Sie unter TLS-Serverzertifikaten auf Controllern installieren.
3. Installieren Sie die Stammzertifizierungsstelle und die Zwischenzertifizierungsstelle auf dem VDA, um dem Delivery Controller zu vertrauen.

### Verfahren

Folgen Sie den Anweisungen, um eine WebSocket-Verbindung einzurichten:

1. Aktivieren Sie die WebSocket-Verbindung auf dem Delivery Controller. Führen Sie den folgenden Befehl auf jedem Delivery Controller auf Ihrer Site aus:

   ```
   New-ItemProperty "HKLM:\SOFTWARE\Citrix\DesktopServer\WorkerProxy
   "-Name "WebSocket_Enabled"-PropertyType "DWord"-Value 1 -Force
   ```

   > **Hinweis:**
   >
   > Sie müssen die Delivery Controller neu starten, nachdem Sie den WebSocket aktiviert haben.

2. Erstellen Sie einen Maschinenkatalog für AD-verknüpfte VDAs mit MCS-Bereitstellung. Weitere Informationen finden Sie unter Erstellen des Maschinenkatalogs.
3. Erstellen Sie eine Bereitstellungsgruppe und fügen Sie Ihren VDA hinzu. Weitere Informationen finden Sie unter Bereitstellungsgruppen erstellen.
4. Aktivieren Sie die WebSocket-Verbindung auf dem VDA. Führen Sie den folgenden Befehl auf dem VDA aus:

```
New-ItemProperty "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
    Services\CitrixBrokerAgent\WebSocket" -Name "Enabled" -
    PropertyType "DWord" -Value 1 -Force
<!--NeedCopy-->
```

- Um zu überprüfen, ob der VDA über WebSocket mit dem Server verbunden ist, überprüfen Sie den folgenden Registrierungsschlüsselwert.

  Schlüssel:

  ```
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
      CitrixBrokerAgent\WebSocket
  <!--NeedCopy-->
  ```

  Name: Verbunden

  Typ: REG_DWORD

  Wert: 1 oder 0

  1: Der VDA ist über WebSocket mit dem Server verbunden.

  0: VDA kann den Server nicht über WebSocket erreichen oder WebSocket ist nicht aktiviert.

- Um zu überprüfen, ob WebSocket aktiviert ist, überprüfen Sie den folgenden Registrierungsschlüsselwert. Der Wert von `Enabled` muss 1 sein.

  Schlüssel:

  ```
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
      CitrixBrokerAgent\WebSocket
  <!--NeedCopy-->
  ```

  Name: Enabled

  Typ: REG_DWORD

  Wert: 1

## HDX-Konnektivität

June 27, 2024

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.

Das HDX-Angebot ermöglicht Ihnen den Verbindungsaufbau über ein einzigartiges, proprietäres Transportprotokoll, die Verwendung der maximalen Anzahl von Übertragungseinheiten beim Einrichten von Sitzungen und eine optimierte Konnektivität mit Citrix SD-WAN.

## Adaptiver Transport

June 27, 2024

Adaptiver Transport ist ein Mechanismus in Citrix Virtual Apps and Desktops, der es ermöglicht, Verbindungen für HDX-Sitzungen über ein bevorzugtes Transportprotokoll herzustellen und gleichzeitig ein Fallback auf TCP bereitzustellen, wenn die Konnektivität mit dem bevorzugten Protokoll nicht verfügbar ist.

Die folgenden Transportprotokolle werden unterstützt:

- Enlightened Data Transport (EDT)
- Übertragungssteuerungsprotokoll (TCP)

### Konfiguration

Der adaptive Transport ist standardmäßig aktiviert. Sie können den adaptiven Transport für folgende Modi konfigurieren:

- **Bevorzugt**: (Standard) Der Client versucht, eine Verbindung mit dem bevorzugten Protokoll herzustellen, und fällt auf TCP zurück, wenn die Konnektivität mit dem bevorzugten Protokoll nicht verfügbar ist.
- **Diagnosemodus**: Der Client versucht nur, eine Verbindung mit dem bevorzugten Protokoll herzustellen. Das Fallback auf TCP wird deaktiviert.
- **Aus**: Der Client versucht nur, eine Verbindung über TCP herzustellen.

### Funktionsweise

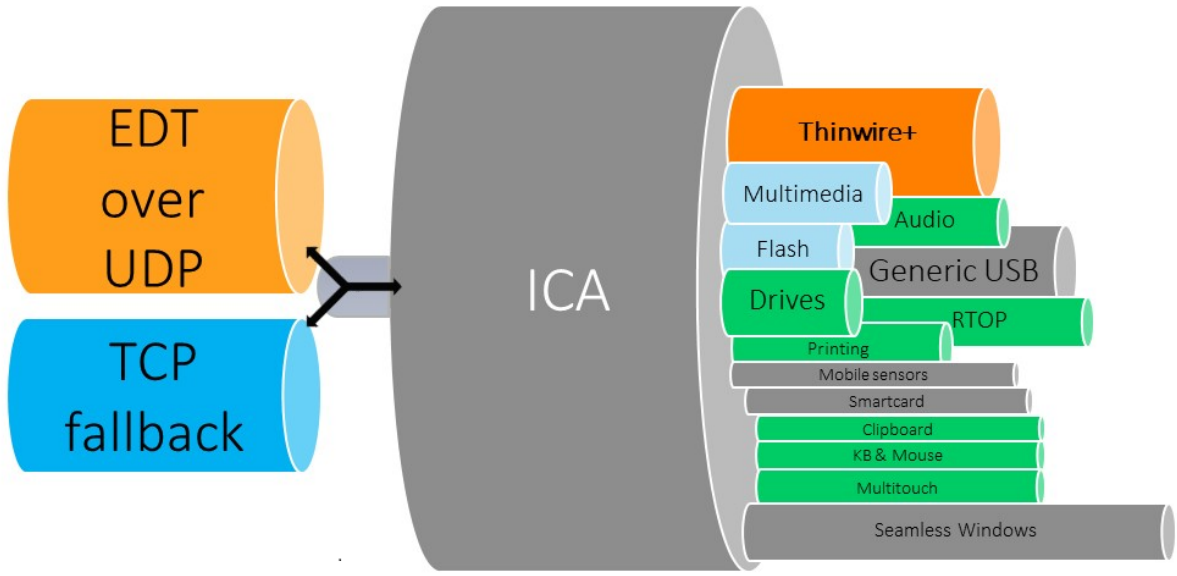
Wenn **Adaptiver Transport** auf `Preferred` eingestellt ist, versucht der Client, eine Verbindung zur Sitzung sowohl mit dem bevorzugten Protokoll als auch mit TCP parallel herzustellen. Auf diese

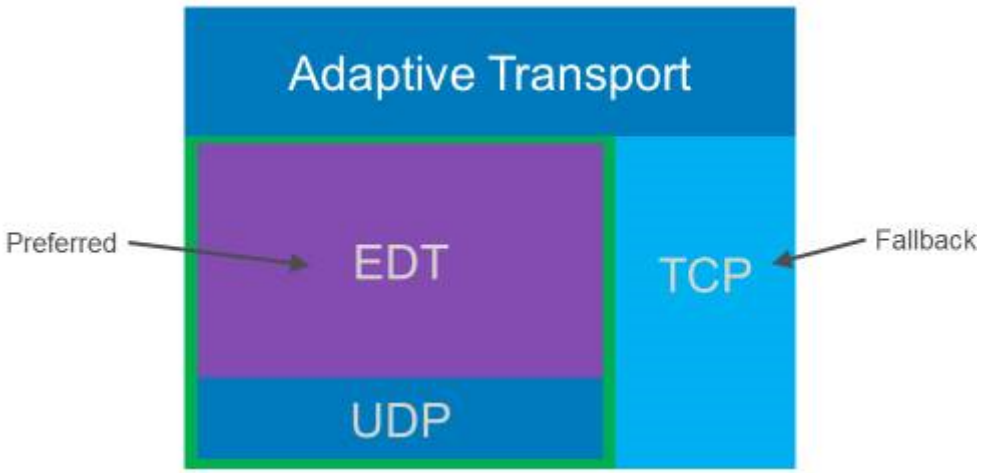
 

Weise kann die Verbindungszeit optimiert werden, wenn keine Verbindung mit dem bevorzugten Protokoll hergestellt werden kann und der Client auf TCP zurückgreifen muss. Wenn die Verbindung über TCP hergestellt wird, versucht der Client alle fünf Minuten, im Hintergrund eine Verbindung mit dem bevorzugten Protokoll herzustellen.

Wenn **Adaptiver Transport** auf `Diagnostic mode` eingestellt ist, stellt der Client nur mit dem bevorzugten Protokoll eine Verbindung zur Sitzung her. Wenn der Client keine Verbindung mit dem bevorzugten Protokoll herstellen kann, greift er nicht auf TCP zurück und die Verbindung schlägt fehl.

Wenn **Adaptiver Transport** auf `Off` eingestellt ist, ist **Adaptiver Transport** deaktiviert und der Client stellt nur über TCP eine Verbindung zur Sitzung her.



### Systemanforderungen

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

- Steuerungsebene
  - Citrix DaaS (früher Citrix Virtual Apps and Desktops Service)
  - Citrix Virtual Apps and Desktops: aktuell unterstützte Version
- Virtual Delivery Agent
  - Windows: aktuell unterstützte Version (2402 oder höher empfohlen)
  - Linux: aktuell unterstützte Version (2402 oder höher empfohlen)
- Citrix Workspace-App
  - Windows: aktuell unterstützte Version (2402 oder höher empfohlen)
  - Linux: aktuell unterstützte Version (2402 oder höher empfohlen)
  - Mac: aktuell unterstützte Version (2402 oder höher empfohlen)
  - iOS: aktuell verfügbare Version im Apple App Store
  - Android: aktuell verfügbare Version in Google Play
- Citrix NetScaler Gateway
  - 14.1.12.30 oder höher (empfohlen)
  - 13.1.17.42 oder höher (13.1-52.19 oder höher empfohlen)

> **Hinweis:**
>
> Einzelheiten zu Linux VDA finden Sie in der Dokumentation zu Linux Virtual Delivery Agent.

### Netzwerkanforderungen

In den folgenden Abschnitten sind die Netzwerkanforderungen für die Verwendung von EDT mit adaptivem Transport aufgeführt:

#### Sitzungshosts

Wenn Ihre Sitzungshosts über eine Firewall wie die Windows Defender-Firewall verfügen, müssen Sie den folgenden eingehenden Verkehr für interne Verbindungen zulassen.

| Beschreibung | Quelle | Protokoll | Port |
|---|---|---|---|
| Interne Verbindung — Sitzungszuverlässigkeit aktiviert | Client | UDP | 2598 |
| Interne Verbindung — Sitzungszuverlässigkeit deaktiviert | | | 1494 |
| Interne Verbindung — HDX Direct oder VDA SSL | | | 443 |

> **Hinweis:**
>
> Das VDA-Installationsprogramm fügt der Windows Defender-Firewall die entsprechenden Regeln für eingehenden Datenverkehr hinzu. Wenn Sie eine andere Firewall verwenden, müssen Sie die obigen Regeln hinzufügen.

**Internes Netzwerk**

Die folgende Tabelle zeigt die Firewallregeln, die für die Verwendung von EDT in Ihrem Netzwerk erforderlich sind:

| Beschreibung | Protokoll | Quelle | Ziel | Zielport |
|---|---|---|---|---|
| Direkte interne Verbindung — Sitzungszuverlässigkeit aktiviert | UDP | Clientnetzwerk | VDA-Netzwerk | 2598 |
| Direkte interne Verbindung — Sitzungszuverlässigkeit deaktiviert | | | | 1494 |
| Direkte interne Verbindung — HDX Direct oder VDA SSL | | | | 443 |
| NetScaler Gateway | | NetScaler-SNIP | | 2598 |

| Beschreibung | Protokoll | Quelle | Ziel | Zielport |
|---|---|---|---|---|
| NetScaler Gateway —VDA SSL | | | | 443 |

> **Hinweis:**
>
> Wenn Sie den Citrix Gateway Service verwenden, müssen Sie **Rendezvous** aktivieren, um EDT als Transportprotokoll zu verwenden. Die System- und Netzwerkanforderungen finden Sie in der Rendezvous-Dokumentation.

**Clientnetzwerk**

In der folgenden Tabelle sind die Konnektivitätsanforderungen für Clientgeräte aufgeführt:

| Beschreibung | Protokoll | Quelle | Ziel | Zielport |
|---|---|---|---|---|
| Interne Verbindung — Sitzungszuverlässigkeit aktiviert | UDP | Client IP | VDA-Netzwerk | 2598 |
| Interne Verbindung — Sitzungszuverlässigkeit deaktiviert | | | | 1494 |
| Interne Verbindung — HDX Direct oder SSL VDA | | | | 443 |
| Externe Verbindung — NetScaler Gateway | | | Öffentliche IP-Adresse von NetScaler Gateway | 443 |
| Externe Verbindung – Citrix Gateway Service | | | Citrix Gateway Service | 443 |

> **Hinweis:**
>
> Wenn Sie den Citrix Gateway Service verwenden, müssen die Clients https://*.*.nssvc.net erreichen können. Wenn Sie nicht alle Unterdomänen mit https://*.*.nssvc.net zulassen können, verwenden Sie stattdessen https://*.c.nssvc.net und https://*.g.nssvc.net. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX270584.

## Enlightened Data Transport (EDT)

June 27, 2024

EDT (Enlightened Data Transport) 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 **Adaptiver Transport** aktiviert ist, ist EDT das bevorzugte Protokoll.

### Nützliche Informationen

- Die **Sitzungszuverlässigkeit** muss aktiviert sein, um **MTU Discovery** und EDT mit NetScaler Gateway und Citrix Gateway Service verwenden zu können.
- Die Paketfragmentierung kann in einigen Fällen zu Leistungseinbußen oder sogar zum Versagen beim Öffnen von Sitzungen führen. Um dies zu verhindern, müssen Sie die EDT-MTU auf einen für Ihre Netzwerke angemessenen Wert einstellen. Sie können EDT MTU Discovery oder eine manuelle Problemumgehung verwenden, die unter So konfigurieren Sie MSS bei Verwendung von EDT in Netzwerken mitnicht stehender MTU beschrieben wird.
- Einzelheiten zur Aktivierung von EDT mit NetScaler Gateway finden Sie unter NetScaler Gateway zur Unterstützung von Enlightened Data Transport konfigurieren.

### 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.

Die MTU-Discovery ist standardmäßig aktiviert. Wenn Sie es deaktivieren müssen, finden Sie weitere Informationen unter HDX-Funktionen, die über die Registrierung verwaltet werden.

> **Hinweis:**
>
> - **Sitzungszuverlässigkeit** muss aktiviert sein, damit MTU-Discovery funktioniert.
> - MTU-Discovery mit Multistream-ICA ist mit VDA-Version 2209 und höher verfügbar.

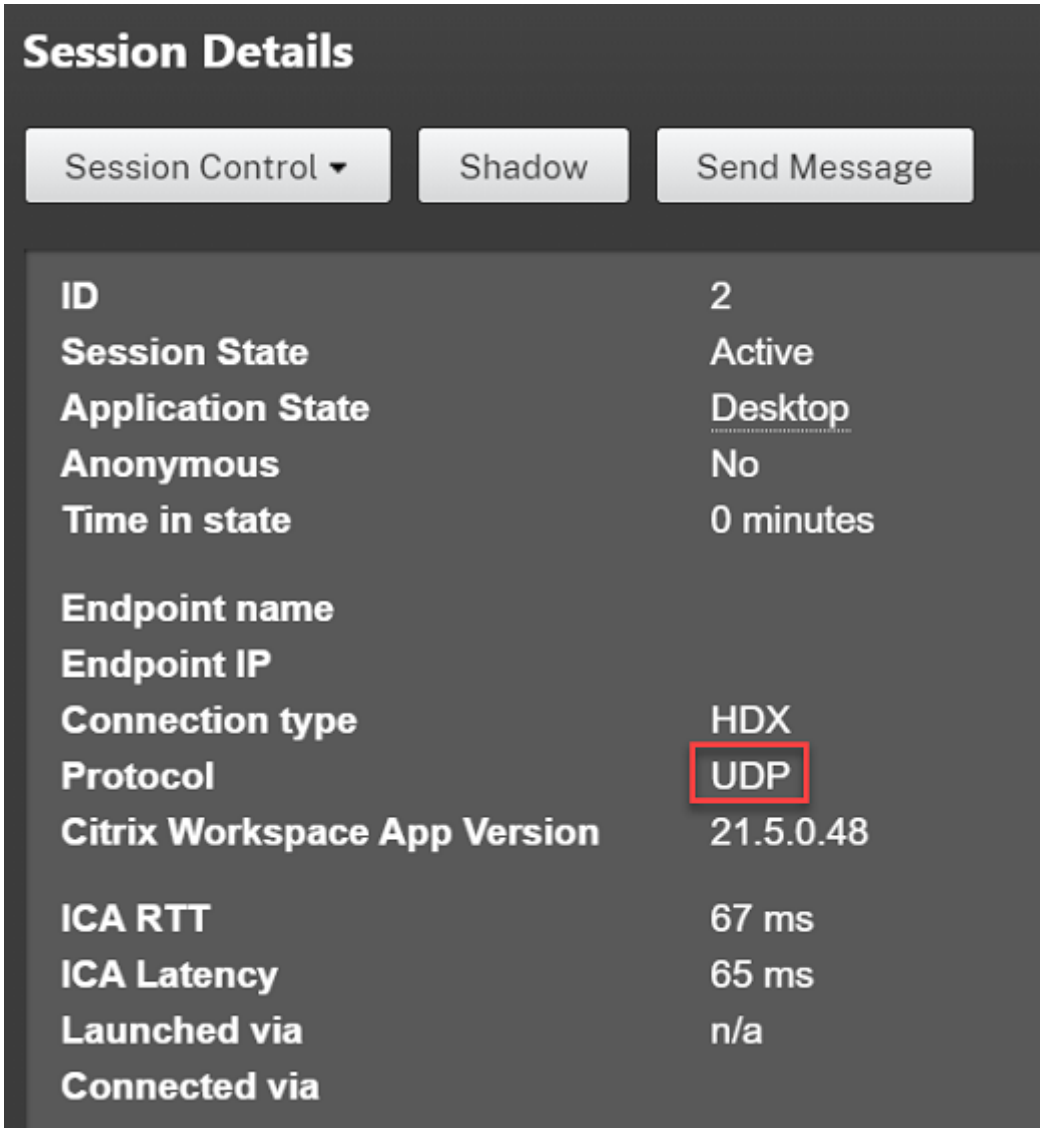
## Problembehandlung

June 27, 2024

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.

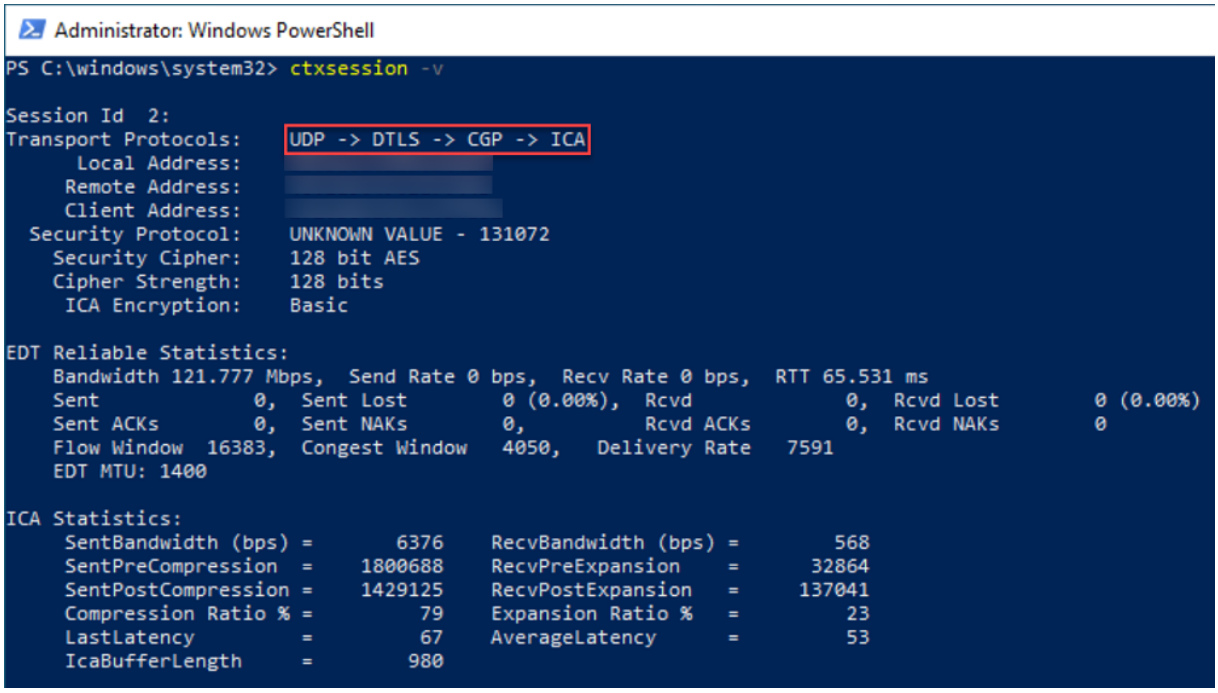
 




Um das Hilfsprogramm CtxSession.exe zu verwenden, starten Sie eine Eingabeaufforderung oder PowerShell in der Sitzung und führen `ctxsession.exe` aus. Zur Anzeige ausführlicher Statistiken führen Sie `ctxsession.exe -v` aus. Wenn EDT verwendet wird, wird eine der folgenden Optionen im Transportprotokoll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

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




### Wenn Sitzungen keine Verbindung mit EDT herstellen können

Folgendes wird zur Problembehandlung beim **adaptiven Transport** und **EDT** empfohlen:

1. Prüfen Sie die Systemanforderungen, Netzwerkanforderungen, Bekannten Probleme und Nützliche Informationen und achten Sie darauf, dass alle Punkte erfüllt sind.
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. Überprüfen Sie, ob die Firewallregeln in den Netzwerk-Firewalls und in den Firewalls, die auf den VDA-Maschinen ausgeführt werden, richtig konfiguriert sind.
6. Starten Sie intern eine direkte Sitzung unter Umgehung von NetScaler Gateway oder Citrix Gateway Service und überprüfen Sie das verwendete Protokoll. Wenn die Sitzung EDT verwendet, ist

der VDA in der Lage, EDT für externe Verbindungen über NetScaler Gateway oder Citrix Gateway Service zu verwenden.

7. Wenn EDT für direkte interne Verbindungen funktioniert und nicht für Sitzungen, die über NetScaler Gateway oder Citrix Gateway Service laufen:

   - Vergewissern Sie sich, dass die **Sitzungszuverlässigkeit** aktiviert ist.
   - Wenn Sie NetScaler Gateway verwenden, vergewissern Sie sich, dass Ihre Konfiguration der erforderlichen Konfiguration entspricht, die unter NetScaler Gateway zur Unterstützung von Enlightened Data Transport und HDX Insight konfigurieren beschrieben ist.

8. Wenn Sie den Citrix Gateway Service verwenden, vergewissern Sie sich, dass Rendezvous aktiviert ist und funktioniert.

9. 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 WLAN-Zugangspunkte und Mobilfunknetze wie 4G und 5G verwendet werden. Vergewissern Sie sich, dass Sie MTU Discovery aktiviert haben oder eine benutzerdefinierte MTU einrichten, wie unter So konfigurieren Sie MSS bei Verwendung von EDT in Netzwerken mitnicht stehender MTU beschrieben.

### Bekannte Probleme

- Bei asymmetrischen Netzwerkpfaden kann die MTU-Discovery bei Verbindungen fehlschlagen, die nicht über NetScaler 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 NetScaler Gateway 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 ab Firmware-Release 13.1 Build 17.42 verfügbar. Einzelheiten zur Aktivierung des Fixes finden Sie in der NetScaler Gateway-Dokumentation. [CGOP-18438]
- 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 **MTU Discovery** und verwenden Sie eine fest codierte MTU, wie unter So konfigurieren Sie MSS bei Verwendung von EDT in Netzwerken mitnicht stehender MTU 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.

## HDX Direct (Preview)

June 27, 2024

Beim Zugriff auf von Citrix bereitgestellte Ressourcen ermöglicht HDX Direct sowohl internen als auch externen Clientgeräten, eine sichere direkte Verbindung mit dem Sitzungshost herzustellen, sofern eine direkte Kommunikation möglich ist.

> **Wichtig:**
>
> HDX Direct ist derzeit in der Technical Preview. Dieses Feature wird ohne Unterstützung bereitgestellt und noch nicht für den Einsatz in Produktionsumgebungen empfohlen. Verwenden Sie dieses Formular, um Feedback einzureichen oder Probleme zu melden.

### Systemanforderungen

Für die Verwendung von HDX Direct gelten die folgenden Systemvoraussetzungen:

- Steuerungsebene
  - Citrix DaaS
  - Citrix Virtual Apps and Desktops 2402 oder höher
- Virtual Delivery Agent (VDA)
  - Windows: Version 2402 oder höher
- Workspace-App
  - Windows: Version 2402 oder höher
- Zugriffsebene
  - Citrix Workspace mit Citrix Gateway Service
  - Citrix Workspace mit NetScaler Gateway
- Sonstiges
  - Adaptive Transport muss für externe Direktverbindungen aktiviert sein

## Netzwerkanforderungen

Für die Verwendung von HDX Direct gelten die folgenden Netzwerkvoraussetzungen.

### Sitzungshosts

Wenn Ihre Sitzungshosts über eine Firewall wie die Windows Defender-Firewall verfügen, müssen Sie den folgenden eingehenden Verkehr für interne Verbindungen zulassen.

| Beschreibung | Quelle | Protokoll | Port |
|---|---|---|---|
| Direkte interne Verbindung | Client | TCP | 443 |
| Direkte interne Verbindung | Client | UDP | 443 |

> Hinweis:
>
> Das VDA-Installationsprogramm fügt der Windows Defender-Firewall die entsprechenden Regeln für eingehenden Datenverkehr hinzu. Wenn Sie eine andere Firewall verwenden, müssen Sie die obigen Regeln hinzufügen.

### Clientnetzwerk

In der folgenden Tabelle wird das Clientnetzwerk für interne und externe Benutzer beschrieben.

#### Interne Benutzer

| Beschreibung | Protokoll | Quelle | Quellport | Ziel | Zielport |
|---|---|---|---|---|---|
| Direkte interne Verbindung | TCP | Clientnetzwerk | 1024–65535 | VDA-Netzwerk | 443 |
| Direkte interne Verbindung | UDP | Clientnetzwerk | 1024–65535 | VDA-Netzwerk | 443 |

#### Externe Benutzer

| Beschreibung | Protokoll | Quelle | Quellport | Ziel | Zielport |
|---|---|---|---|---|---|
| STUN (nur für externe Benutzer) | UDP | Clientnetzwerk | 1024–65535 | Internet (siehe Hinweis unten) | 3478, 19302 |
| Externe Benutzerverbindung | UDP | Clientnetzwerk | 1024–65535 | Öffentliche IP-Adresse des Datencenters | 1024–65535 |

**Datencenternetzwerk**

In der folgenden Tabelle wird das Datencenternetzwerk für interne und externe Benutzer beschrieben.

**Interne Benutzer**

| Beschreibung | Protokoll | Quelle | Quellport | Ziel | Zielport |
|---|---|---|---|---|---|
| Direkte interne Verbindung | TCP | Clientnetzwerk | 1024–65535 | VDA-Netzwerk | 443 |
| Direkte interne Verbindung | UDP | Clientnetzwerk | 1024–65535 | VDA-Netzwerk | 443 |

**Externe Benutzer**

| Beschreibung | Protokoll | Quelle | Quellport | Ziel | Zielport |
|---|---|---|---|---|---|
| STUN (nur für externe Benutzer) | UDP | VDA-Netzwerk | 1024–65535 | Internet (siehe Hinweis unten) | 3478, 19302 |
| Externe Benutzerverbindung | UDP | DMZ / Internes Netzwerk | 1024–65535 | VDA-Netzwerk | 55000–55250 |
| Externe Benutzerverbindung | UDP | VDA-Netzwerk | 55000–55250 | Öffentliche IP des Clients | 1024–65535 |

> **Hinweis:**
>
> Sowohl der VDA als auch die Workspace-App versuchen, STUN-Anforderungen in derselben Reihenfolge an die folgenden Server zu senden:
>
> - stunserver.stunprotocol.org:3478
> - employees.org:3478
> - stun.l.google.com:19302
>
> Wenn Sie den Standardportbereich für externe Benutzerverbindungen mithilfe der Richtlinieneinstellung **HDX Direct-Portbereich** ändern, müssen die entsprechenden Firewallregeln Ihrem benutzerdefinierten Portbereich entsprechen.

### Konfiguration

HDX Direct ist standardmäßig deaktiviert. Sie können das Feature mithilfe der **HDX Direct**-Einstellung der Citrix Richtlinie konfigurieren.

- **HDX Direct**: Zum Aktivieren oder Deaktivieren eines Features.
- **HDX Direct-Modus**: Legt fest, ob **HDX Direct** nur für interne Clients oder sowohl für interne als auch für externe Clients verfügbar ist.
- **HDX Direct-Portbereich**: Definiert den Portbereich, den der VDA für Verbindungen von externen Clients verwendet.

### Überlegungen

Bei der Verwendung von HDX Direct ist Folgendes zu berücksichtigen:

- HDX Direct für externe Benutzer ist nur mit EDT (UDP) als Transportprotokoll verfügbar. Daher muss **Adaptiver Transport** aktiviert sein.
- Wenn Sie **HDX Insight** verwenden, beachten Sie, dass die Verwendung von **HDX Direct** die HDX Insight-Datenerfassung verhindert, weil die Sitzung nicht mehr über NetScaler Gateway als Proxy geleitet würde.
- Wenn Sie nicht persistente Maschinen für Ihre virtuellen Apps und Desktops verwenden, empfiehlt Citrix, **HDX Direct** auf den Sitzungshosts statt im Master-/Vorlagenimage zu aktivieren, damit jede Maschine ihre eigenen Zertifikate generiert.
- Die Verwendung Ihrer eigenen Zertifikate mit HDX Direct wird derzeit nicht unterstützt.

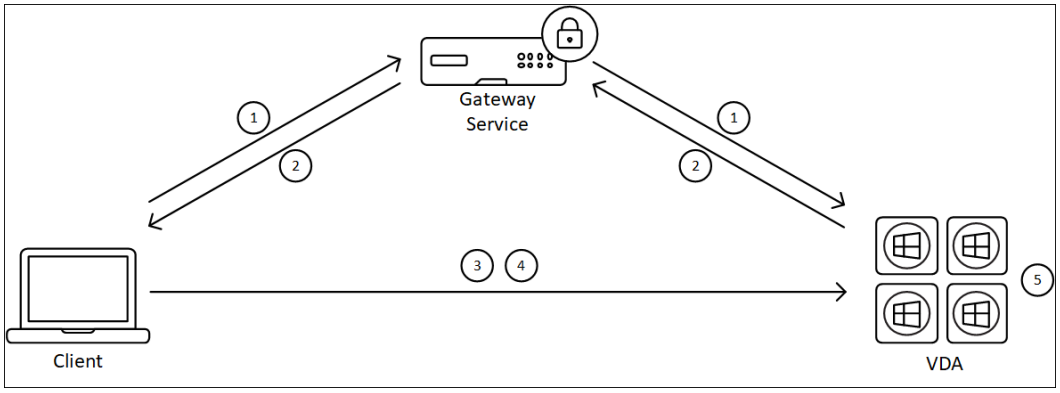
 

## Funktionsweise

HDX Direct ermöglicht es Clients, eine direkte Verbindung zum Sitzungshost herzustellen, wenn eine direkte Kommunikation verfügbar ist. Wenn direkte Verbindungen mit HDX Direct hergestellt werden, werden selbstsignierte Zertifikate verwendet, um die direkte Verbindung mit Verschlüsselung auf Netzwerkebene (TLS/DTLS) zu sichern.

### Interne Benutzer

Das folgende Diagramm zeigt den Überblick über den HDX Direct-Verbindungsprozess interner Benutzer.



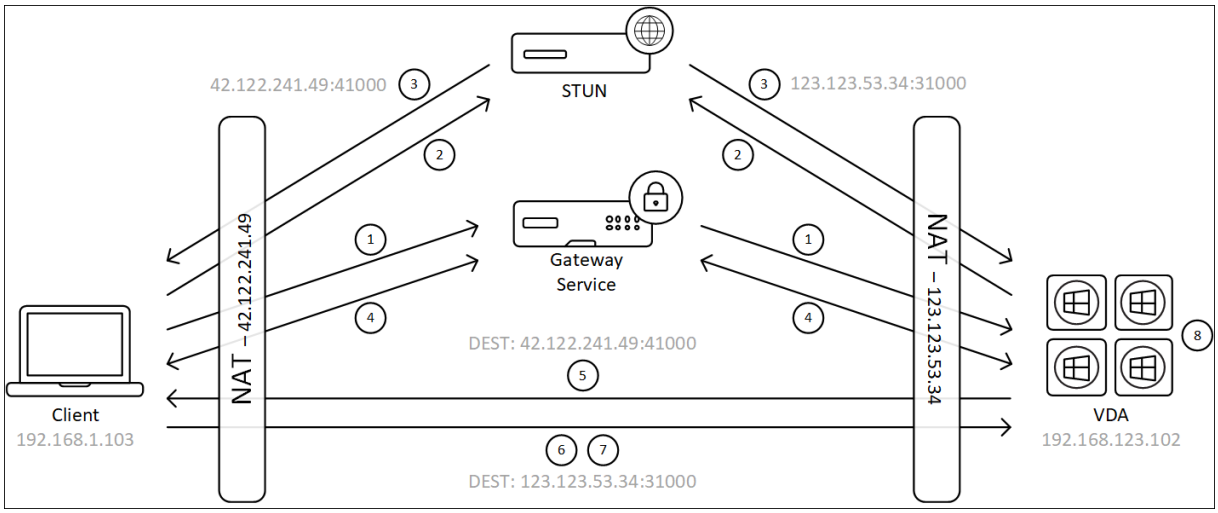

1. Der Client richtet eine HDX-Sitzung über den Gateway Service ein.
2. Nach einer erfolgreichen Verbindung sendet der VDA den FQDN der VDA-Maschine, eine Liste ihrer IP-Adressen und das Zertifikat der VDA-Maschine über die HDX-Verbindung an den Client.
3. Der Client überprüft die IP-Adressen, um festzustellen, ob er den VDA direkt erreichen kann.
4. Wenn der Client den VDA mit einer der gemeinsam genutzten IP-Adressen direkt erreichen kann, stellt der Client eine direkte Verbindung mit dem VDA her, die mit (D) TLS über ein Zertifikat gesichert ist, das dem in Schritt (2) ausgetauschten Zertifikat entspricht.
5. Sobald die direkte Verbindung hergestellt ist, wird die Sitzung an sie übertragen und die Verbindung zu Gateway Service wird beendet.

> **Hinweis:**
>
> Nach dem Herstellen der Verbindung in Schritt 2 oben ist die Sitzung aktiv. Die nachfolgenden Schritte verzögern oder beeinträchtigen nicht die Fähigkeit des Benutzers, die virtuelle Anwendung oder den Desktop zu verwenden. Wenn einer der nachfolgenden Schritte fehlschlägt, wird die Verbindung über das Gateway aufrechterhalten, ohne die Benutzersitzung zu unterbrechen.

**Externe Benutzer**

Das folgende Diagramm zeigt den Überblick über den HDX Direct-Verbindungsprozess für externe Benutzer:




1. Der Client richtet eine HDX-Sitzung über den Gateway Service ein.
2. Nach einer erfolgreichen Verbindung senden sowohl der Client als auch der VDA eine STUN-Anforderung, um ihre öffentlichen IP-Adressen und Ports zu ermitteln.
3. Der STUN-Server antwortet dem Client und dem VDA mit ihren entsprechenden öffentlichen IP-Adressen und Ports.
4. Über die HDX-Verbindung tauschen der Client und der VDA ihre öffentlichen IP-Adressen und UDP-Ports aus und der VDA sendet sein Zertifikat an den Client.
5. Der VDA sendet UDP-Pakete an die öffentliche IP-Adresse und den UDP-Port des Clients. Der Client sendet UDP-Pakete an die öffentliche IP-Adresse und den UDP-Port des VDA.
6. Nach Erhalt einer Nachricht vom VDA antwortet der Client mit einer sicheren Verbindungsanforderung.
7. Während des DTLS-Handshakes überprüft der Client, ob das Zertifikat mit dem in Schritt (4) ausgetauschten Zertifikat übereinstimmt. Nach der Validierung sendet der Client sein Autorisierungstoken. Eine sichere Direktverbindung ist jetzt hergestellt.
8. Sobald die direkte Verbindung hergestellt ist, wird die Sitzung an sie übertragen und die Verbindung zu Gateway Service wird beendet.

> **Hinweis:**
>
> Nach dem Herstellen der Verbindung in Schritt 2 oben ist die Sitzung aktiv. Die nachfolgenden Schritte verzögern oder beeinträchtigen nicht die Fähigkeit des Benutzers, die virtuelle Anwendung oder den Desktop zu verwenden. Wenn einer der nachfolgenden Schritte fehlschlägt, wird die Verbindung über das Gateway aufrechterhalten, ohne die Benutzersitzung zu unterbrechen.

## Zertifikatverwaltung

### Sitzungshost

Die folgenden beiden Dienste auf der VDA-Maschine übernehmen die Erstellung und Verwaltung von Zertifikaten. Beide sind so eingerichtet, dass sie beim Maschinenstart automatisch ausgeführt werden:

- Citrix ClxMtp Service: verantwortlich für die Generierung und Rotation von ZS-Zertifikaten.
- Citrix Certificate Manager Service: verantwortlich für die Generierung und Verwaltung des selbstsignierten Stamm-ZS-Zertifikats und der Maschinenzertifikate.

Die folgenden Schritte veranschaulichen den Prozess der Zertifikatsverwaltung:

1. Die Dienste werden beim Start der Maschine gestartet.
2. `Citrix ClxMtp Service` erstellt Schlüssel, falls noch keiner erstellt wurde.
3. Citrix Certificate Manager Service überprüft, ob **HDX Direct** aktiviert ist. Andernfalls stoppt der Dienst selbsttätig.
4. Wenn **HDX Direct** aktiviert ist, prüft Citrix Certificate Manager Service, ob ein selbstsigniertes Stamm-ZS-Zertifikat vorhanden ist. Ist dies nicht der Fall, wird ein selbstsigniertes Stammzertifikat erstellt.
5. Sobald ein Stamm-ZS-Zertifikat verfügbar ist, prüft Citrix Certificate Manager Service, ob ein selbstsigniertes Maschinenzertifikat vorhanden ist. Ist dies nicht der Fall, generiert der Dienst Schlüssel und erstellt mithilfe des Maschinen-FQDN ein Zertifikat.
6. Ist ein von Citrix Certificate Manager Service erstelltes Maschinenzertifikat vorhanden und der Antragstellername stimmt nicht mit dem Maschinen-FQDN überein, wird ein neues Zertifikat generiert.

> **Hinweis:**
>
> Citrix Certificate Manager Service generiert RSA-Zertifikate, die 2048-Bit-Schlüssel nutzen.

### Clientgerät

Damit eine sichere **HDX Direct**-Verbindung hergestellt werden kann, muss der Client den Zertifikaten vertrauen, die zum Schutz der Sitzung verwendet wurden. Um dies zu ermöglichen, erhält der Client das ZS-Zertifikat für die Sitzung über die ICA-Datei (von Workspace bereitgestellt), sodass es nicht erforderlich ist, ZS-Zertifikate an die Zertifikatsspeicher der Clientgeräte zu verteilen.

# NAT-Kompatibilität

June 27, 2024

Um eine direkte Verbindung zwischen einem externen Benutzergerät und dem Sitzungshost herzustellen, nutzt HDX Direct Hole Punching für NAT-Traversal und STUN, um den Austausch der öffentlichen IP-Adressen und Portzuordnungen für das Clientgerät und den Sitzungshost zu erleichtern. Dies ähnelt der Funktionsweise von VoIP-, Unified Communications- und P2P-Lösungen.

Solange Firewalls und andere Netzwerkkomponenten so konfiguriert sind, dass sie den UDP-Verkehr für die STUN-Anforderungen und die HDX-Sitzungen zulassen, wird erwartet, dass HDX Direct für externe Benutzer funktioniert. Es gibt jedoch bestimmte Szenarien, in denen die NAT-Typen der Benutzer- und Sitzungshostnetzwerke zu einer inkompatiblen Kombination führen, wodurch HDX Direct ausfällt.

## Validierungen

Sie können den NAT-Typ auf dem Client und dem Sitzungshost validieren, indem Sie das STUN-Clienthilfsprogramm von STUNTMAN verwenden:

1. Laden Sie das entsprechende Paket für die Zielplattform von stunprotocol.org herunter und extrahieren Sie den Inhalt.
2. Öffnen Sie eine Terminal-Eingabeaufforderung und navigieren Sie zu dem Verzeichnis, in das der Inhalt extrahiert wurde.
3. Führen Sie den folgenden Befehl aus:
   `.\stunclient.exe stunserver.stunprotocol.org --mode behavior`
4. Notieren Sie sich die Ausgabe.

Wenn die Bindungs- und Verhaltenstests erfolgreich sind, melden sowohl der **Bindungstest** als auch der **Verhaltenstest** den Erfolg und ein NAT-Verhalten wird angegeben:


Wenn die Tests fehlschlagen, melden sowohl der **Bindungstest** als auch der **Verhaltenstest** den Fehler.


Anhand der folgenden Tabelle können Sie ausgehend von den Testergebnissen des Clients und des Sitzungshosts ermitteln, ob HDX Direct für externe Benutzer voraussichtlich funktioniert:

| Clientgerät | Sitzungshost | Wird es voraussichtlich funktionieren? |
|---|---|---|
| Endpunktunabhängige Zuordnung | Endpunktunabhängige Zuordnung | Ja |
| Endpunktunabhängige Zuordnung | Endpunktabhängige Zuordnung | Ja |
| Endpunktabhängige Zuordnung | Endpunktunabhängige Zuordnung | Ja |
| Endpunktabhängige Zuordnung | Endpunktabhängige Zuordnung | Nein |
| Adress- und portabhängige Zuordnung | Beliebiger NAT-Typ | Nein |
| Beliebiger NAT-Typ | Adress- und portabhängige Zuordnung | Nein |
| Fehlschlag | Beliebiger NAT-Typ | Nein |
| Beliebiger NAT-Typ | Fehlschlag | Nein |
| Fehlschlag | Fehlschlag | Nein |

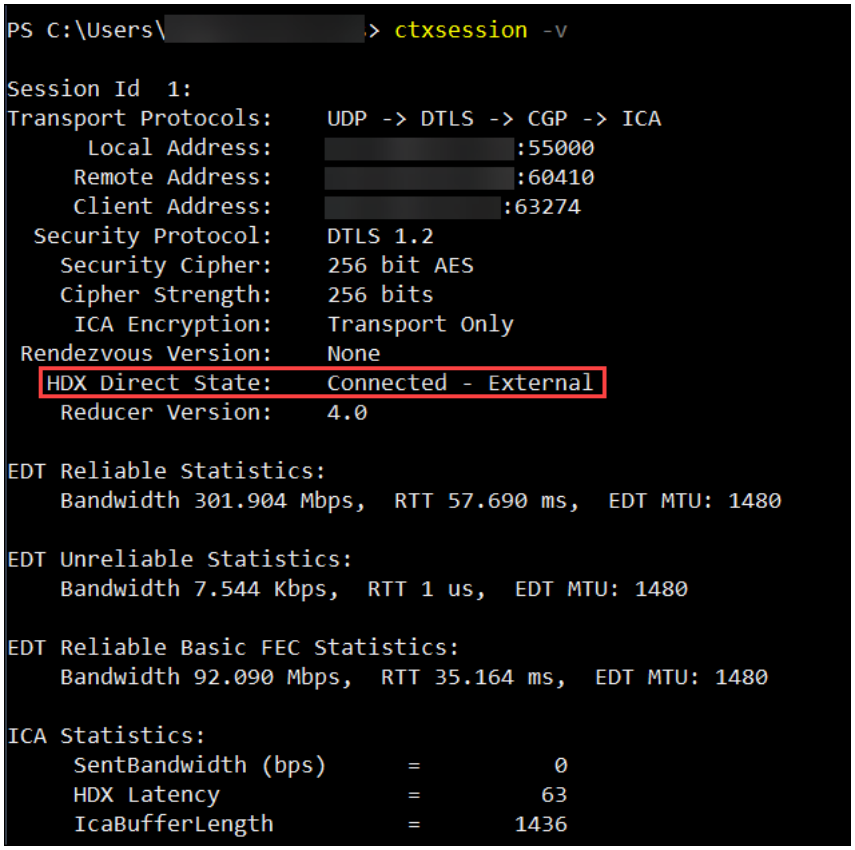
## Problembehandlung

June 27, 2024

Verwenden Sie das Hilfsprogramm `CtxSession.exe` auf der VDA-Maschine, um zu überprüfen, ob **HDX Direct** eine direkte Verbindung hergestellt hat.

Um das Hilfsprogramm `CtxSession.exe` zu verwenden, starten Sie eine Eingabeaufforderung oder PowerShell in der Sitzung und führen `ctxsession.exe -v` aus. Wenn die **HDX Direct**-Verbindung erfolgreich hergestellt wurde, lautet der **HDX Direct-Statu** `Connected`.




Sie können auch in den Ereignisprotokollen des Sitzungshosts nachlesen, ob die HDX Direct-Verbindung erfolgreich hergestellt wurde oder fehlgeschlagen ist. Einzelheiten finden Sie im Abschnitt **Ereignisprotokolle**.

> Hinweis:
>
> Je nach Umgebung und Anzahl der IP-Adressen, die den Sitzungshosts zur Verfügung stehen, kann es bis zu 5 Minuten dauern, bis die HDX Direct-Verbindung hergestellt ist.

### Wenn HDX Direct keine direkte Verbindung herstellen kann

Wenn HDX Direct keine direkte Verbindung herstellen kann, überprüfen Sie Folgendes:

1. Überprüfen Sie, ob die verwendete VDA-Version und die Workspace-App-Version das Feature gemäß den Systemanforderungen unterstützen.
2. Vergewissern Sie sich, dass auf den VDA eine Richtlinie angewendet wurde, die HDX Direct aktiviert, und keine anderen Richtlinien mit höherer Priorität vorhanden sind, die das Feature deaktivieren.
3. Vergewissern Sie sich, dass auf den VDA eine Richtlinie angewendet wurde, die den gewünschten HDX Direct-Modus festlegt, und keine anderen Richtlinien mit höherer Priorität die Konfiguration überschreiben.

4. Überprüfen Sie, ob der Citrix ClxMtp-Dienst auf dem Sitzungshost ausgeführt wird.
5. Überprüfen Sie, ob der Citrix Certificate Manager Service auf dem Sitzungshost ausgeführt wird. Wenn er nicht läuft, versuchen Sie, ihn manuell zu starten. Der Dienst wird automatisch beendet, wenn HDX Direct deaktiviert ist.
6. Prüfen Sie, ob der Sitzungshost über ein selbstsigniertes Stamm-ZS-Zertifikat verfügt:

    a) Ausgestellt an: CA-<hostname>(Zum Beispiel CA-FTLW11-001)
    b) Ausgestellt von: CA-<hostname>(Zum Beispiel CA-FTLW11-001)
    c) Angaben zum Aussteller: Die Organisation ist Citrix Systems, Inc.

7. Prüfen Sie, ob der Sitzungshost über ein selbstsigniertes Serverzertifikat verfügt:

    a) Ausgestellt an: <host FQDN> (Zum Beispiel FTLW11-001.ctxlab.net)
    b) Ausgestellt von: CA-<hostname>(Zum Beispiel CA-FTLW11-001)
    c) Angaben zum Aussteller: Die Organisation ist Citrix Systems, Inc.

8. Wenn die Zertifikate fehlen, wenden Sie sich an den technischen Support von Citrix.
9. Wenn die Zertifikate vorhanden sind:

    a) Stoppen Sie den Citrix Certificate Manager Service auf dem Sitzungshost.
    b) Löschen Sie sowohl das selbstsignierte Stamm-ZS-Zertifikat als auch das selbstsignierte Serverzertifikat.
    c) Starten Sie den Citrix Certificate Manager Service auf dem Sitzungshost. Der Dienst erstellt neue Zertifikate, sobald er gestartet wird.

10. Für interne Benutzer:

    a) Achten Sie darauf, dass die Firewall des Sitzungshosts den eingehenden Verkehr auf UDP 443 oder TCP 443 für HDX über EDT bzw. HDX über TCP nicht blockiert.
    b) Achten Sie darauf, dass Ihre Netzwerkfirewall den Verkehr auf UDP 443 und TCP 443 zwischen dem Netzwerk Ihrer Kunden und dem Netzwerk der Sitzungshosts nicht blockiert.

11. Für externe Nutzer:

    a) Überprüfen Sie den NAT-Typ für den Client und den Sitzungshost und stellen Sie sicher, dass die Kombination voraussichtlich funktioniert. Einzelheiten finden Sie im Abschnitt NAT-Kompatibilität.
    b) Wenn der NAT-Test entweder auf dem Client oder auf dem Sitzungshost fehlschlägt:
        i. Wenn auf dem System eine Firewall läuft, stellen Sie sicher, dass sie den ausgehenden Verkehr auf UDP 3478 nicht blockiert.
        ii. Stellen Sie sicher, dass Ihre Netzwerkfirewalls den ausgehenden Verkehr auf UDP 3478 nicht blockieren.
        iii. Stellen Sie sicher, dass die Firewalls die Antwort des STUN-Servers nicht blockieren.

c) Stellen Sie sicher, dass für Ihre Netzwerkfirewalls die entsprechenden Regeln konfiguriert sind, um den gesamten erforderlichen Datenverkehr zuzulassen. Einzelheiten finden Sie unter Netzwerkanforderungen.
d) Wenn Sie den Standardportbereich mithilfe der Richtlineineinstellung "HDX Direct-Portbereich"ändern, achten Sie darauf, dass Ihre Firewallregeln für den benutzerdefinierten Portbereich festgelegt sind.

### Ereignisprotokolle

Die folgenden Ereignisse werden im Ereignisprotokoll der VDA-Maschine protokolliert:

| Protokollierung | ID | Quelle | Ebene | Beschreibung |
|---|---|---|---|---|
| Anwendungs- und Dienstprotokolle > Citrix-HostCore-HDX Direct/Operational | 1 | HDX Direct | Informationen | HDX Direct-Verbindung für internen Benutzer <username> hergestellt. |
| Anwendungs- und Dienstprotokolle > Citrix-HostCore-HDX Direct/Operational | 2 | HDX Direct | Informationen | HDX Direct-Verbindung für externen Benutzer <username> hergestellt. |
| Anwendungs- und Dienstprotokolle > Citrix-HostCore-HDX Direct/Operational | 3 | HDX Direct | Informationen | Die HDX Direct-Verbindung für den Benutzer <username> ist fehlgeschlagen. |

### Bekannte Probleme

HDX Direct funktioniert möglicherweise nicht mehr, nachdem ein direktes Upgrade des VDA auf einer Maschine durchgeführt wurde, auf der **HDX Direct** bereits aktiviert ist.
Gehen Sie wie folgt vor, um das Problem zu beheben:

1. Stoppen Sie den Citrix Certificate Manager Service auf dem Sitzungshost.
2. Löschen Sie das selbstsignierte Stamm-ZS-Zertifikat und das selbstsignierte Serverzertifikat.
3. Öffnen Sie die Registrierung.
4. Löschen Sie den Schlüssel `HKLM\Software\Citrix\HDX-Direct`.
5. Gehen Sie zu `HKLM\SYSTEM\CurrentControlSet\Control\TerminalServer\Wds\icawd`.
6. Setzen Sie den **SSLEnabled**-Wert auf `0`.
7. Löschen Sie den Inhalt des **SSLThumbprint**-Werts.
8. Starten Sie den **Citrix Certificate Manager Service**.

## Secure HDX (Preview)

June 27, 2024

Secure HDX ist eine ALE-Lösung (Application Level Encryption), die verhindert, dass Netzwerkelemente im Datenverkehrspfad den HDX-Verkehr überprüfen können. Dazu wird echte Ende-zu-Ende-Verschlüsselung (E2EE) auf Anwendungsebene zwischen der Citrix Workspace-App (Client) und dem VDA (Sitzungshost) mithilfe der AES-256-GCM-Verschlüsselung bereitgestellt.

> **Wichtig:**
>
> Secure HDX befindet sich derzeit in der Previewversion. Dieses Feature wird ohne Unterstützung bereitgestellt und noch nicht für den Einsatz in Produktionsumgebungen empfohlen. Verwenden Sie dieses Formular, um Feedback einzureichen oder Probleme zu melden.

### Systemanforderungen

Die folgende Liste enthält die Systemanforderungen für die Verwendung von Secure HDX.

- Steuerungsebene
  - Citrix DaaS
  - Citrix Virtual Apps and Desktops 2402 oder höher
- Virtual Delivery Agent (VDA)
  - Windows: Version 2402 oder höher
- Workspace-App
  - Windows: Version 2402 oder höher
- Zugriffsebene

- Citrix Workspace
- Citrix StoreFront 2402 oder höher

### Konfiguration

Secure HDX ist standardmäßig deaktiviert. Sie können das Feature mit der Secure HDX-Einstellung der Citrix Richtlinie konfigurieren:

**Secure HDX**: Definiert, ob das Feature für alle Sitzungen, nur für direkte Verbindungen, aktiviert oder deaktiviert werden soll.

### Überlegungen

Im Folgenden finden Sie Überlegungen zur Verwendung von Secure HDX:

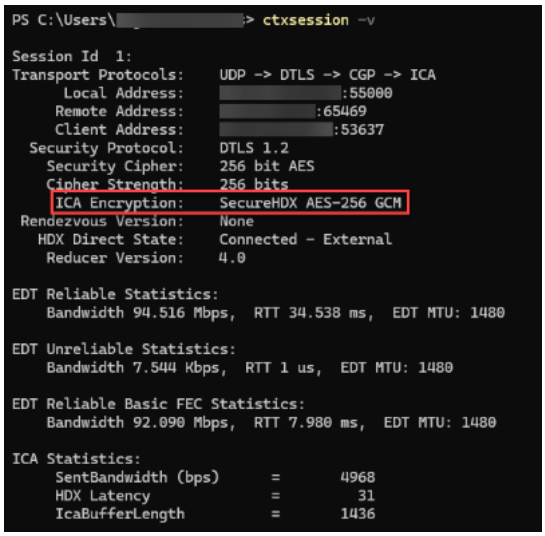
- Wenn ein Benutzer versucht, mit einem Client, der dieses Feature nicht unterstützt, eine Verbindung zu einem Sitzungshost herzustellen, bei dem Secure HDX aktiviert ist, wird die Verbindung verweigert.
- Servicekontinuität wird derzeit mit Secure HDX nicht unterstützt. Wenn Servicekontinuität in Ihrer Citrix Cloud-Umgebung aktiviert ist, kann bei einem Ausfall des Clouddienstes möglicherweise keine Verbindung zu Sitzungshosts hergestellt werden, auf denen Secure HDX aktiviert ist.
- Wenn Sie HDX Insight verwenden, beachten Sie, dass die Verwendung von Secure HDX die HDX Insight-Datenerfassung verhindert, da NetScaler den verschlüsselten HDX-Verkehr nicht überprüfen kann. Wenn Sie HDX Insight verwenden müssen, können Sie Secure HDX so einrichten, dass es nur für direkte Verbindungen aktiviert wird.
- Wenn Sie SmartControl verwenden, beachten Sie, dass die Verwendung von Secure HDX verhindert, dass SmartControl funktioniert, da der NetScaler den verschlüsselten HDX-Verkehr nicht überprüfen kann. Wenn Sie SmartControl verwenden müssen, können Sie Secure HDX so einrichten, dass es nur für direkte Verbindungen aktiviert wird.
- Multistream-ICA wird nicht unterstützt, wenn Secure HDX aktiviert ist.
- Bei Verwendung von Drittanbieterlösungen, die auf der Überprüfung des HDX-Datenverkehrs basieren, funktionieren diese nicht mehr, wenn Sie Secure HDX aktivieren, da der HDX-Verkehr verschlüsselt ist.

### Problembehandlung

Um zu bestätigen, dass Secure HDX aktiv ist, können Sie das Hilfsprogramm `ctxsession.exe` auf der VDA-Maschine verwenden.

Um das Hilfsprogramm `CtxSession.exe` zu verwenden, starten Sie eine Eingabeaufforderung oder PowerShell in der Sitzung und führen `ctxsession.exe -v` aus. Wenn Secure HDX verwendet wird, zeigt die ICA-Verschlüsselung `SecureHDX AES-256 GCM` an.




**Wenn Secure HDX in der Sitzung nicht aktiviert wird**

- Stellen Sie sicher, dass die verwendete VDA-Version das Feature gemäß den Systemanforderungen unterstützt.
- Vergewissern Sie sich, dass auf den VDA eine Richtlinie angewendet wurde, die HDX Direct aktiviert, und keine anderen Richtlinien mit höherer Priorität vorhanden sind, die das Feature deaktivieren.
- Wenn das Clientgerät eine Verbindung über NetScaler Gateway oder Gateway Service herstellt, stellen Sie sicher, dass Secure HDX nicht auf "Nur direkte Verbindungen"eingestellt ist.
- Wenn der Sitzungshost bereits lief, als Sie Secure HDX konfiguriert haben, starten Sie den Computer neu, um sicherzustellen, dass die Änderungen wirksam werden.

## Positivliste für virtuelle Kanäle

June 27, 2024

Die Positivliste für virtuelle Kanäle ist ein Feature, mit dem Sie steuern können, welche virtuellen Kanäle, die nicht von Citrix stammen, in Ihrer Umgebung zulässig sind. Die Positivliste für virtuelle Kanäle ist standardmäßig aktiviert. Daher dürfen in Sitzungen von Citrix Virtual Apps and Desktops nur virtuelle Citrix Kanäle geöffnet werden. Ist die Verwendung benutzerdefinierter virtueller Kanäle erforderlich (eigener oder derer eines Dritten), müssen diese der Positivliste hinzugefügt werden.

### Konfiguration

Die Positivliste für virtuelle Kanäle ist standardmäßig deaktiviert. Sie können dieses Feature mithilfe der folgenden Einstellungen in der Citrix-Richtlinie konfigurieren:

- **Positivliste für virtuelle Kanäle**: um die Funktion zu aktivieren oder zu deaktivieren und virtuelle Kanäle zur Liste hinzuzufügen.
- **Protokolldrosselung für virtuelle Kanäle –Positivliste**: legt den Einschränkungszeitraum für die Protokollierung von Listenereignissen für virtuelle Kanäle fest.
- **Positivliste für die Protokollierung**: legt die Protokollierungsstufe für die Positivliste virtueller Kanäle fest.

### Hinzufügen virtueller Kanäle zur Positivliste

Sie benötigen die folgenden Informationen, um einen virtuellen Kanal zur Positivliste hinzuzufügen, benötigen:

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. Wenn es mehrere Prozesse gibt, können Sie diese Prozesse hinzufügen, indem Sie sie durch Kommas trennen.

#### Für einzelne Prozesse

Im Fall der o. g. Beispiele würden Sie der Liste den folgenden Eintrag hinzufügen:

```
CTXCVC1,C:\Program Files\Application\run.exe
```

#### Für mehrere Prozesse

Im Fall mehrerer Prozesse fügen Sie den folgenden Eintrag hinzu:

```
CTXCVC1,C:\Program Files\Application\run.exe,C:\Program Files\Application
\run2.exe
```

### Platzhalter verwenden

Die Verwendung von Platzhaltern (*) wird unterstützt. Sie können Platzhalter verwenden, wenn sich die Namen von Verzeichnissen oder ausführbaren Dateien entsprechend der Version der Anwendung ändern oder wenn die Drittanbieterkomponente in den Benutzerprofilen installiert ist.

Sie können Platzhalter in den folgenden Szenarien verwenden:

- Um den vollständigen Verzeichnisnamen zu ersetzen.
  Beispiel:`C:\Program Files\Application\*\run1.exe`
- Um einen Teil des Verzeichnisnamens zu ersetzen.
  Beispiel:`C:\Program Files\Application\v*\run1.exe`
- Um den Namen der ausführbaren Datei zu ersetzen.
  Beispiel:`C:\Program Files\Application\v1.2\*.exe`
- Um einen Teil des Namens der ausführbaren Datei zu ersetzen.
  Beispiel:`C:\Program Files\Application\v1.2\run*.exe`

Es gelten die folgenden Einschränkungen:

- Der Platzhalter kann nur als Ersatz für ein einzelnes Verzeichnis verwendet werden. Beispiel: Die ausführbare Datei befindet sich in `C:\Program Files\Application\v1.2\run1.exe`
  - Zulässig: `C:\Program Files\Application\*\run1.exe`
  - Nicht zulässig: `C:\Program Files\*\run1.exe`
- Die Einträge müssen die Dateinamenserweiterung enthalten.
  - Zulässig: `C:\Program Files\Application\v1.2\*.exe`
  - Nicht zulässig: `C:\Program Files\Application\v1.2\*`
- Alle Pfade müssen lokale Pfade sein.

> **Hinweis:**
>
> - Netzwerkpfade sind nicht zulässig.
> - Wildcard-Unterstützung ist ab Citrix Virtual Apps and Desktops 2206 verfügbar.
> - Wildcard-Unterstützung ist in Citrix Virtual Apps and Desktops 2203 LTSR ab CU2 verfügbar.

### Systemumgebungsvariablen verwenden

Sie können Systemumgebungsvariablen verwenden, um die Definition der vertrauenswürdigen Prozesse in Ihrer Positivliste zu vereinfachen. Sie können jede der vorbereiteten Variablen wie, `%programfiles%`, `%programfiles(x86)%`, `%systemdrive%` und `%systemroot%`.

Sie können auch benutzerdefinierte Umgebungsvariablen verwenden, sofern sie auf Systemebene definiert sind.

Die folgenden Beispiele zeigen sofort einsatzbereite Umgebungsvariablen:

- `%programfiles%\Application\v1.2\run.exe`
- `%programfiles%\Application\*\run.exe`
- `%programfiles(x86)%\Application\v1.*\run.exe`

Das folgende Beispiel zeigt eine benutzerdefinierte Systemumgebungsvariable:

- Name der benutzerdefinierten Variablen: `app`
- Wert der benutzerdefinierten Variablen: `%programfiles%\Application\`
- Eintrag in Positivliste: `CTXCVC1,%app%\run.exe`

> **Hinweis:**
>
> Benutzerumgebungsvariablen werden nicht unterstützt.
>
> Die Unterstützung von Umgebungsvariablen ist ab Version 2209 von Citrix Virtual Apps and Desktops verfügbar.

### Namen und Prozesse virtueller Kanäle erhalten

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 erhalten, indem Sie die Protokolle des Features anwenden und die folgenden Schritte einhalten:

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 und den Prozess, der ihn zu öffnen versucht: Weitere Informationen zu verfügbaren Ereignissen finden Sie unter Ereignisprotokolle.
3. Melden Sie sich von der Sitzung ab.
4. Fügen Sie in der Richtlinieneinstellung für die Positivliste virtueller Kanäle einen Eintrag für den gefundenen virtuellen Kanal und den Prozess hinzu.
5. Starten Sie die Maschine neu.
6. Sobald der VDA registriert ist, führen Sie die virtuelle Anwendung oder den virtuellen Desktop aus, um zu überprüfen, ob die benutzerdefinierten virtuellen Kanäle erfolgreich geöffnet werden.

### 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

Wenn Sie einen anderen Media Player als Windows Media Player als System-Media Player verwenden, müssen Sie ihn als vertrauenswürdigen Prozess zur Positivliste hinzufügen. Folgende Informationen sind für den Eintrag in der Positivliste erforderlich:

- Name des virtuellen Kanals: `CTXMM`
- Prozess: Pfad zu dem auf dem VDA verwendeten Media Player. Beispiel: `C:\Program Files (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 Positivliste 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:\Program Files\Microsoft Office\root\Office16\lync.exe`.
- Eintrag in Positivliste: `CTXRMEP,C:\Program Files\Microsoft Office\root\Office16\lync.exe`

## Problembehandlung

June 27, 2024

Wenn der benutzerdefinierte virtuelle Kanal nicht geöffnet werden kann, gehen Sie die folgenden Schritte durch:

1. Vergewissern Sie sich, dass Sie die richtige VDA-Version verwenden.

2. Vergewissern Sie sich, dass auf den VDA eine Richtlinie mit dem benutzerdefinierten virtuellen Kanal in der Positivliste für virtuelle Kanäle angewendet wurde und keine anderen Richtlinien mit höherer Priorität diese Konfiguration überschreiben.
3. Überprüfen Sie das Ereignisprotokoll im VDA und vergewissern Sie sich, dass der gemeldete virtuelle Kanalname mit dem Namen übereinstimmt, der in der Positivliste definiert ist.

    a) Wenn Sie mehrere Prozesse haben, vergewissern Sie sich, dass diese korrekt definiert sind, wie unter Virtuelle Kanäle zur Positivliste hinzufügen beschrieben.
    b) Wenn Sie Platzhalter im definierten Prozesspfad verwenden, achten Sie darauf, dass Sie die Richtlinien für die Verwendung von Platzhaltern einhalten.
    c) Wenn Sie Umgebungsvariablen im definierten Prozesspfad verwenden, achten Sie darauf, dass Sie die Richtlinien unter Systemumgebungsvariablen verwenden einhalten.

## Ereignisprotokolle

Die folgenden Ereignisse werden im Ereignisprotokoll der VDA-Maschine protokolliert:

### Einzelsitzungs-VDA

Die folgenden Ereignisse werden im Ereignisprotokoll eines Einzelsitzungs-VDAs protokolliert:

| Protokolldateiname | ID | Quelle | Ebene | Beschreibung |
|---|---|---|---|---|
| System | 2001 | `Picadd` | Informationen | Der benutzerdefinierte virtuelle Kanal <`vcName`> wurde von Prozess < `processName`> geöffnet |
| System | 2002 | `Picadd` | Warnung | Der benutzerdefinierte virtuelle Kanal <`vcName`> kann von Prozess < `processName`> nicht geöffnet werden |

| Protokolldateiname | ID | Quelle | Ebene | Beschreibung |
|---|---|---|---|---|
| System | 2003 | Picadd | Informationen | <username> hat den benutzerdefinierten Kanal <vcName> geöffnet |
| System | 2004 | Picadd | Warnung | <username> hat versucht, den benutzerdefinierten virtuellen Kanal <vcName> zu öffnen |
| System | 2005 | Picadd | Fehler | Der in Richtlinie <pathInPolicy> angegebene Pfad kann nicht in den Prozesspfad aufgelöst werden |
| System | 2007 | Picadd | Informationen | Der geladene Prozesspfad ist <processPath> |
| System | 2008 | Picadd | Fehler | Umgebungsvariable <varName> wurde nicht im VC-Richtlinienpfad gefunden |

**Multisitzungs-VDA**

Die folgenden Ereignisse werden im Ereignisprotokoll eines Multisitzungs-VDAs protokolliert:

| Protokolldateiname | ID | Quelle | Ebene | Beschreibung |
|---|---|---|---|---|
| System | 13 | Rpm | Informationen | Der benutzerdefinierte virtuelle Kanal <vcName> wurde von Prozess <processName> geöffnet |
| System | 14 | Rpm | Warnung | Der benutzerdefinierte virtuelle Kanal <vcName> kann von Prozess <processName> nicht geöffnet werden |
| System | 15 | Rpm | Informationen | <username> hat den benutzerdefinierten Kanal <vcName> geöffnet |
| System | 16 | Rpm | Warnung | <username> hat versucht, den benutzerdefinierten virtuellen Kanal <vcName> zu öffnen |
| System | 17 | Rpm | Fehler | Der in Richtlinie <pathInPolicy> angegebene Pfad kann nicht in den Prozesspfad aufgelöst werden |
| System | 18 | Rpm | Informationen | Der geladene Prozesspfad ist <processPath> |

| Protokolldateiname | ID | Quelle | Ebene | Beschreibung |
|---|---|---|---|---|
| System | 19 | Rpm | Fehler | Umgebungsvariable <varName> wurde nicht im VC-Richtlinienpfad gefunden |

## Bekannte virtuelle Kanäle von Drittanbietern

June 27, 2024

Die folgenden Drittanbieterlösungen verwenden bekanntermaßen benutzerdefinierte virtuelle Citrix Kanäle. Diese Liste enthält nicht jede Lösung, die einen benutzerdefinierten virtuellen Citrix Kanal verwendet.

- Cerner
- ControlUp
- Cisco WebEx Teams
- Cisco WebEx Meetings Virtual Desktop-Software
- deviceTrust
- Epic Warp Drive
- Epic Slingshot
- Imprivata OneSign
- Midmark IQPath-Clienterweiterungen
- Nuance PowerMic-Clienterweiterungen
- Nuance Dragon Medical Network Edition 360 vSync
- Zoom Meetings für VDI
- Ultima IA-Connect

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

June 27, 2024

HDX bietet eine High Definition-Benutzererfahrung auf jedem Gerät an jedem Ort. Im Abschnitt "Geräte"werden folgende Geräte behandelt:

- Scannen
- Generische USB-Geräte
- Clientlaufwerkszuordnung
- Mobile und Touchscreengeräte
- Serielle Geräte
- Spezialtastaturen
- 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 | 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 in der virtuellen Sitzung entsperrt wird | Nur Citrix Virtual Desktops |

## Scannen

June 27, 2024

Ein Scanner ist ein Gerät, das Bilder, gedruckten Text, Handschrift oder ein Objekt optisch scannt und in ein digitales Bild umwandelt.

Wenn Sie einen Scanner verwenden und auf Ihrem Computer Windows ausgeführt wird, verwenden Sie wahrscheinlich den WIA-Scannertreiber. Dieser Treiber ist für die Kommunikation zwischen Ihrem Computer und dem Scanner verantwortlich.

- **Windows Image Acquisition** (WIA) ist das Treibermodell und die Anwendungsprogrammierschnittstelle (API) von Microsoft, über die Software mit Bildverarbeitungshardware wie Scannern kommunizieren kann.
- **TWAIN** (Windows und Mac) ist ein weiteres Protokoll, bei dem es sich um ein Scanprotokoll handelt, das Scanner und Anwendungen über eine Standardschnittstelle miteinander verbindet. Mit TWAIN können Anwendungen Bilder von TWAIN-kompatiblen Geräten (Scannern, Digitalkameras usw.) erfassen.

## TWAIN-Umleitung

June 27, 2024

## Einführung

TWAIN ist ein Scanprotokoll, das verwendet wird, um Bildsoftware mit Scannern oder Digitalkameras zu verbinden.

### So funktioniert TWAIN

- Scannen Sie Ihre Dokumente mit einer der 32-Bit-Anwendungen in Ihrer Citrix-Sitzung.

  > **Hinweis:**
  >
  > Verwenden Sie einen lokal angeschlossenen TWAIN-kompatiblen Scanner, um die Dokumente zu scannen.

- Das Citrix-Scanmodul leitet die TWAIN-Anfrage an den Scanner des Clients weiter.
- Sobald der Scan abgeschlossen ist, wird der Sitzungshost benachrichtigt.

## Anforderungen

### Citrix Steuerungsebene

- Citrix Virtual Apps and Desktops 1912 oder höher
- Citrix DaaS

### Sitzungshost

- Betriebssystem
  - Windows 10 1809 oder höher
  - Windows 11
  - Windows Server 2022 oder später
- VDA
  - Version 1912 oder höher
- Anwendung
  - 32-Bit-Anwendung

#### Clientgerät

- Betriebssystem
  - Windows 10 1809 oder höher
  - Windows 11
- Workspace-App
  - Windows: Version 1912 oder höher
- Scanner
  - TWAIN-kompatibler Scanner

### Konfiguration

- Installieren Sie die TWAIN-Treiber auf dem Clientendpunkt.
- Richten Sie Geräte oder Anwendungen so ein, dass sie das erforderliche Scanprotokoll auswählen, wenn sie sowohl TWAIN als auch WIA unterstützen.
- Schließen Sie den Scanner lokal (über USB) an den Clientendpunkt an.
- Leiten Sie TWAIN-Geräte bei Bedarf per USB-Umleitung zur Sitzung um.

> **Hinweis:**
>
> TWAIN-Geräte funktionieren mit USB-Umleitung nicht gut, was zu einer schlechten Scanqualität führt.

#### Richtlinieneinstellungen

Richtlinieneinstellungen zur Einrichtung der TWAIN-Umleitung und zur Verbesserung des Scannens.

- **Client-TWAIN-Geräteumleitung:** um die TWAIN-Umleitung zu aktivieren oder zu deaktivieren.

  > **Hinweis:**
  >
  > Die TWAIN-Umleitung ist standardmäßig aktiviert.

- **TWAIN-Komprimierungsgrad:** Damit wird der Komprimierungsgrad für die Übertragung von Bildern vom Client zum Host festgelegt.

Weitere Informationen finden Sie unter TWAIN-Geräte - Richtlinieneinstellungen.

### Problembehandlung

Testen Sie TWAIN mit der öffentlichen Test-App Twacker, die unter dieser URL heruntergeladen werden kann.

Gehen Sie wie folgt vor, um TWAIN in einer Sitzung des veröffentlichten Desktops zu überprüfen:

1. Installieren Sie **Twacker** auf dem VDA.
2. Starten Sie **Twacker** (32-Bit-Version).
3. Klicken Sie auf **File > Select Source** und wählen Sie Ihren Scanner aus der Liste aus.
4. Klicken Sie auf **File > Acquire**.
5. Klicken Sie auf die Schaltfläche **Scan**, um Ihren Scanner zu testen.

Wenn **Twacker** erfolgreich scannen kann, wird für das **Citrix Virtual Apps and Desktops**-Setup bestätigt:

- Configured for USB redirection
- TWAIN-Geräte verwenden
- Erfüllung aller lokalen Clientgeräteanforderungen

Wenn Sie in einer bestimmten Anwendung immer noch Probleme mit dem Scannen haben, handelt es sich wahrscheinlich um ein Softwareproblem.

## WIA-Geräte

June 27, 2024

### Anforderungen

- Der Scanner muss WIA-kompatibel sein.
- Installieren Sie die WIA-Treiber auf dem lokalen Gerät. Auf dem Server sind sie nicht erforderlich.
- Schließen Sie den Scanner lokal an (z. B. über USB).
- Vergewissern Sie sich, dass der Scanner den lokalen Windows-Bilderfassungsdienst (Windows Image Acquisition, WIA) und nicht den TWAIN-Treiber verwendet.
- Vergewissern Sie sich, 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.

#### Positivliste für WIA-Anwendungen

Mit einer Positivliste können Sie festlegen, welche Anwendungen auf dem VDA auf die WIA-Scannerumleitung zugreifen können. Der Registrierungs-Editor verwendet Angaben aus der eingestellten Positivliste auf jedem VDA mit Windows-Bilderfassung (WIA). Standardmäßig kann keine Anwendung auf die WIA-Schnittstelle zugreifen.

Informationen zum Anpassen der Windows-Bilderfassung für Anwendungen auf dem VDA finden Sie unter Positivliste für WIA-Anwendungen in der Liste der über die Registrierung verwalteten Features.

Informationen zu Richtlinieneinstellungen finden Sie unter Einstellungen der Richtlinie "WIA-Geräte" .

## Generische USB-Geräte

June 27, 2024

### Einführung

Das generische USB-Umleitungsfeature ermöglicht die Umleitung von USB-Geräten von Clientmaschinen zu HDX-Sitzungen, sodass Endbenutzer in ihrer HDX-Sitzung mit einer großen Auswahl generischer USB-Geräte interagieren können. Dies ist in Szenarien hilfreich, in denen Benutzer spezielle Geräte verwenden müssen, die keinen optimierten Support bieten oder in denen diese ungeeignet sind.

> **Hinweis:** USB-Geräte, die nicht für die Unterstützung virtueller Kanäle optimiert sind, greifen mithilfe der Raw-USB-Umleitung auf den generischen virtuellen USB-Kanal zurück.

### Funktionsweise

Die generische USB-Umleitung funktioniert auf niedriger Ebene und leitet USB-Anforderungs- und Antwortmeldungen zwischen Clientmaschinen und virtuellen XenDesktop-Desktops um.

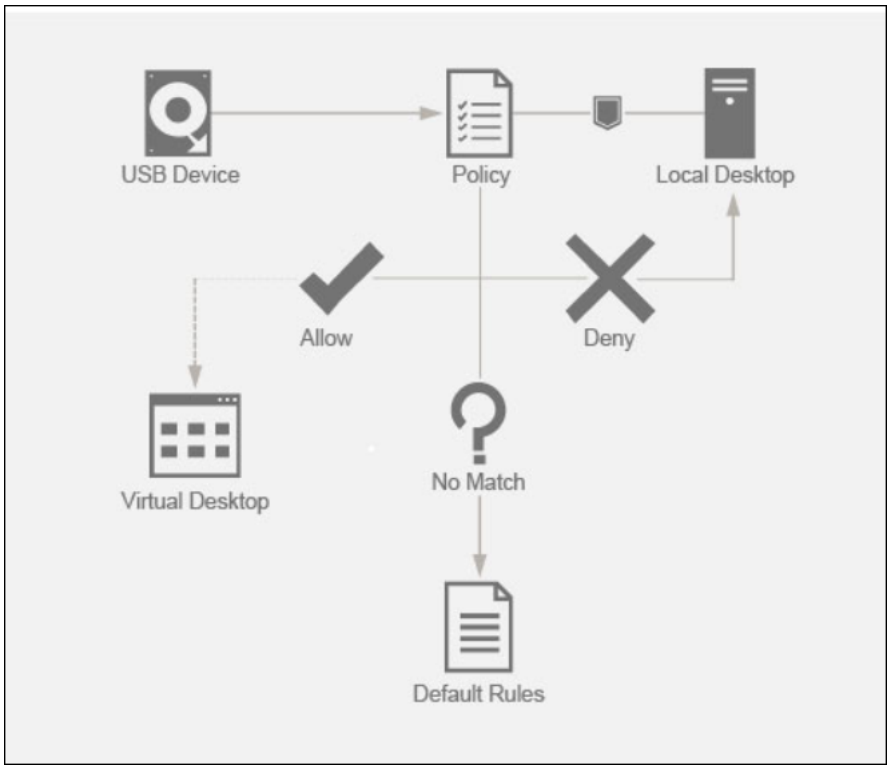
Auf der Clientmaschine sind keine kompatiblen Gerätetreiber erforderlich, der Treiber muss nur auf dem virtuellen Desktop unterstützt werden. Die Regeln für USB-Umleitungsrichtlinien folgen einer bestimmten Rangfolge, sodass clientseitige Richtlinien und Standardregeln eingehalten werden können, nachdem die DDC-Richtlinienregeln evaluiert und durchgesetzt wurden. Auf diese Weise können Citrix-Administratoren verhindern, dass nicht autorisierte/gefälschte Geräte innerhalb einer Sitzung umgeleitet werden.

Darüber hinaus kann die Ereignisprotokollierung von nicht autorisierten Geräten, die versuchen, auf die Remotesitzung zuzugreifen, überwacht und gekennzeichnet werden, und Administratoren können zusätzliche Maßnahmen ergreifen, um Datenexfiltration zu verhindern.

Wenn ein Benutzer ein USB-Gerät anschließt, überprüft der Sitzungshost es nacheinander anhand jeder Richtlinienregel, bis eine Übereinstimmung gefunden wird. Die erste Übereinstimmung für ein beliebiges Gerät ist entscheidend.

- Handelt es sich um eine Allow-Regel, wird das Gerät an den virtuellen Desktop weitergeleitet.
- Handelt es sich bei der ersten Übereinstimmung um eine Deny-Regel, wird das Gerät nicht zur Sitzung umgeleitet und kann nur auf dem lokalen Benutzergerät verwendet werden. Wenn keine Übereinstimmung gefunden wird, werden die Standardregeln verwendet.




## Konfiguration

June 27, 2024

USB-Umleitung ist standardmäßig deaktiviert. Sie können die generische USB-Umleitung mit den folgenden Einstellungen in der Citrix-Richtlinie konfigurieren:

- **Client-USB-Geräteumleitung**: um die USB-Umleitung zu aktivieren oder zu deaktivieren

- **Regeln für die Client-USB-Geräteumleitung**: um eine bestimmte Geräteaktion festzulegen, d. h. um den Zugriff auf ein bestimmtes Gerät zuzulassen oder zu verweigern
- **Regeln für die Client-USB-Geräteumleitung (Version 2)**: zur Angabe von Regeln für das Filtern, Teilen und automatische Verbinden von USB-Geräten
- **Regeln für die Client-USB-Geräteoptimierung**: um die Optimierung zu deaktivieren oder den Optimierungsmodus zu ändern.
- **Zulassen, dass vorhandene USB-Geräte automatisch verbunden werden**: um die automatische Verbindung vorhandener USB-Geräte zu ermöglichen oder zu verhindern, die zu Beginn einer HDX-Sitzung mit einem Clientendpunkt verbunden sind
- **Zulassen, dass neu angeschlossene USB-Geräte automatisch verbunden werden**: um die automatische Verbindung von USB-Geräten zu ermöglichen oder zu verhindern, die während einer HDX-Sitzung mit einem Clientendpunkt verbunden sind

Weitere Informationen finden Sie unter USB-Richtlinieneinstellungen.

## So konfigurieren Sie die USB-Umleitung

Standardmäßig ist die Konfiguration der USB-Umleitung deaktiviert. Um sie verwenden zu können, müssen die USB-Umleitungsrichtlinie und spezifische Umleitungsregeln auf dem DDC aktiviert und konfiguriert werden.

> **Hinweis:**
>
> Wenn Sie Komponenten verwenden, die älter als Version 2212 sind, oder wenn Sie die Workspace-App für Linux/Mac verwenden, finden Sie unter Konfiguration der veralteten USB-Umleitung Informationen zur USB-Umleitung.

### Generische USB-Umleitung aktivieren

1. Öffnen Sie die **Citrix Web Studio-Richtlinien** und klicken Sie auf die Registerkarte **Richtlinien**.
2. Klicken Sie auf **Richtlinie erstellen** und erweitern Sie **ICA > USB-Geräterichtlinien**.
3. Bearbeiten Sie die **Richtlinie für die Client-USB-Geräteumleitung**.
4. Wählen Sie **Zugelassen** aus und klicken Sie auf **Speichern**.

### Richtlinienregeln für die USB-Umleitung erstellen

Wenn der Benutzer versucht, ein USB-Gerät an den virtuellen Desktop umzuleiten, wird es nacheinander mit jeder USB-Richtlinienregel verglichen, bis eine Übereinstimmung gefunden wird. Die erste

Übereinstimmung für ein beliebiges Gerät gilt als endgültig. Wenn es sich bei der ersten Übereinstimmung um eine **Allow**-Regel handelt, darf das übereinstimmende Gerät auf den virtuellen Desktop umgeleitet werden. Handelt es sich um eine **Deny**-Regel, kann das Gerät nur auf dem lokalen Desktop verwendet werden. Wenn keine Übereinstimmung gefunden wird, werden die Standardregeln verwendet.

**Geräteregeln** Wie bei USB-Standardgeräten werden die Verbundgeräte von Geräteregeln, die in der Richtlinie oder der Citrix Workspace-App auf dem Clientendpunkt konfiguriert sind, für die Weiterleitung ausgewählt. Die Citrix Workspace-App entscheidet dann anhand dieser Regeln, welche USB-Geräte an die Remotesitzung weitergeleitet werden dürfen.

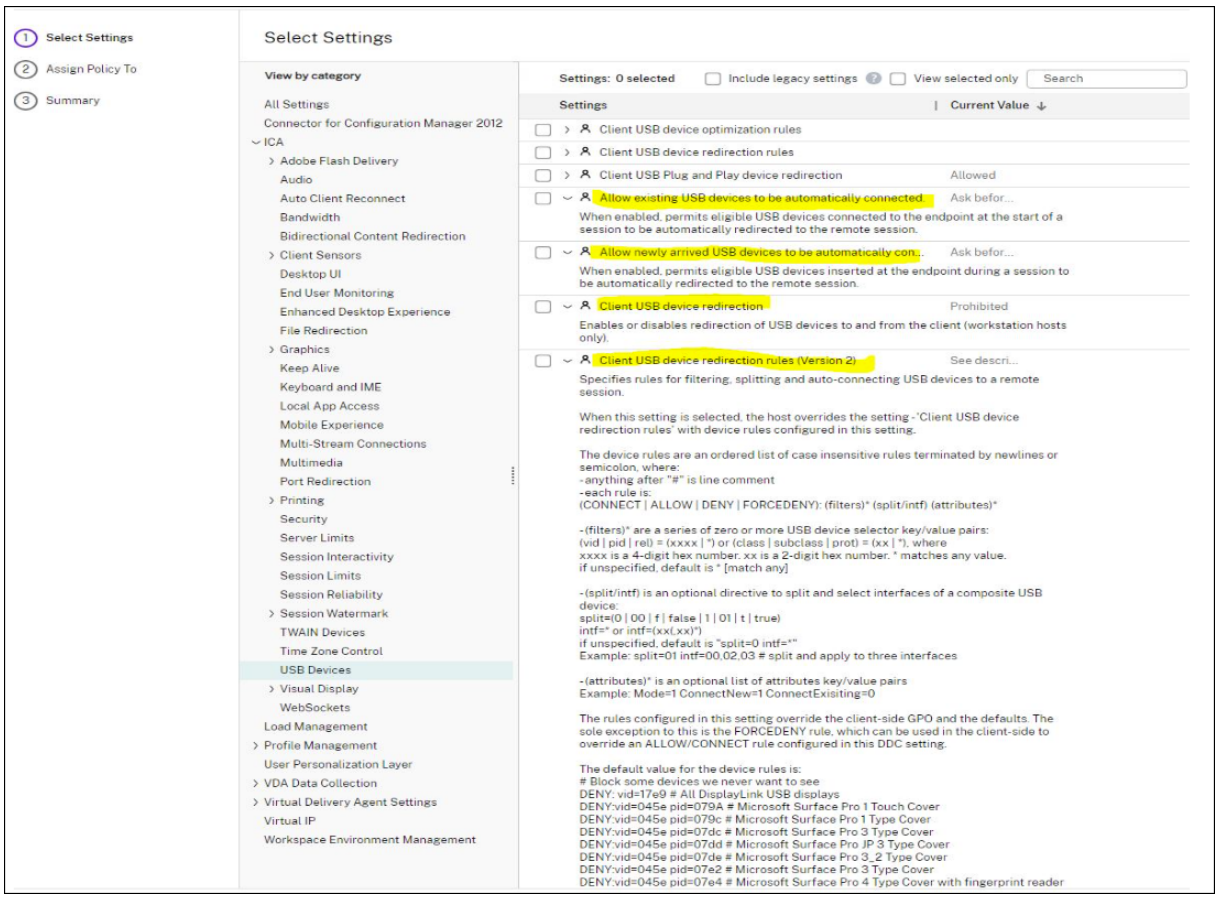
Jede Regel besteht aus einem Aktionsschlüsselwort (**Allow, Connect oder Deny**), einem Doppelpunkt (:) und null oder mehr Filterparametern, die den tatsächlichen Geräten am USB-Subsystem des Endpunkts entsprechen. Diese Filterparameter entsprechen den Metadaten des USB-Gerätedeskriptors, die von jedem USB-Gerät zur Identifizierung verwendet werden.

Geräteregeln sind als Klartext angegeben, mit einer Regel pro Zeile und einem optionalen Kommentar nach dem #-Zeichen. Regeln werden von oben nach unten (in absteigender Prioritätsreihenfolge) zugeordnet. Die erste Regel, die dem Gerät oder der untergeordneten Schnittstelle entspricht, wird angewendet. Nachfolgende Regeln, die dasselbe Gerät oder dieselbe Schnittstelle auswählen, werden ignoriert.

**Beispiel:** ALLOW VID=1050 PID=0421 #Device1
**Beispiel:** CONNECT VID=xxxx PID=yyyy Class=03 #Device2

| Schlüsselwort | Beschreibung |
|---|---|
| CONNECT | Verwenden Sie dieses Schlüsselwort, um zu zuzulassen, dass Geräte über den virtuellen USB-Kanal umgeleitet werden, und zu aktivieren, dass sie beim Sitzungsstart sowie beim Anschließen automatisch umgeleitet werden. |
| ALLOW | Verwenden Sie dieses Schlüsselwort, um zuzulassen, dass Geräte über den virtuellen USB-Kanal umgeleitet werden. |
| DENY | Verwenden Sie dieses Schlüsselwort, um zu verhindern, dass Geräte über den virtuellen USB-Kanal umgeleitet werden |




**Richtlinie auf dem Desktop Delivery Controller einstellen**:

1. Öffnen Sie die **Citrix Web Studio-Richtlinien** und klicken Sie auf die Registerkarte **Richtlinien**.
2. Klicken Sie auf **Richtlinie erstellen** und erweitern Sie **ICA > USB-Geräterichtlinien**.
3. Bearbeiten Sie die **Regeln für die Client-USB-Geräteumleitung** (**Version 2**).
4. Stellen Sie den Wert anhand der Beispiele in der Beschreibung für jedes USB-Gerät ein, das umgeleitet werden muss, und klicken Sie auf "Speichern".

   Beispiel: Allow: VID=056A PID=00A4 #STU-430
   Deny: Class=08 subclass=05 # Mass Storage

   > **Hinweis:**
   >
   > Wenn ein Citrix-Administrator die Option **Standardwert verwenden** aktiviert und auf **Speichern** klickt, sind die Standardregeln in der folgenden Registrierung im VDA zu finden.
   >
   > **Achtung:**

> Lesen Sie den Haftungsausschluss am Ende dieses Artikels, bevor Sie den Registrierungs-Editor verwenden.

`HKLM\SOFTWARE\Wow6432Node\Citrix\PortICA\GenericUSB\DeviceRules`

> **Hinweis:**
>
> Richtlinien können auf dem Clientgerät weiterhin mit Gruppenrichtlinien für Geräteregeln festgelegt werden, aber das ist in neueren Versionen von CVAD und CWA nicht mehr erforderlich.
>
> Informationen zur Legacy-Konfiguration von USB-Geräten finden Sie unter Legacy-USB-Umleitungskonfiguration.

**Konfigurieren der automatischen Umleitung von USB-Geräten (optional)**

USB-Geräte werden automatisch umgeleitet, wenn die USB-Unterstützung aktiviert ist. Außerdem sind die USB-Benutzereinstellungen für eine automatische Verbindung der USB-Geräte konfiguriert. 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 entweder auf dem Clientendpunkt oder in der DDC-Richtlinie DeviceRules.
Diese Richtlinie kann auf dem DDC, dem Client über ein GPO, über Citrix Workspace-Einstellungen oder auf der Registerkarte “Verbindungen”unter CDViewer festgelegt werden. Alle diese Methoden werden im Folgenden beschrieben:

**Richtlinie auf dem Desktop Delivery Controller einstellen:**

Auf dem DDC gibt es zwei Richtlinien, die so eingestellt werden können, dass sie die automatische Umleitung von USB-Geräten zulassen:

- Zulassen, dass vorhandene USB-Geräte automatisch verbunden werden
- Zulassen, dass neu angeschlossene USB-Geräte automatisch verbunden werden

1. Öffnen Sie die **Citrix Web Studio-Richtlinien** und klicken Sie auf die Registerkarte **Richtlinien**.
2. Klicken Sie auf **Richtlinie erstellen** und erweitern Sie **ICA > USB-Geräterichtlinien**.
3. Bearbeiten Sie die Einstellung **Zulassen**, dass vorhandene USB-Geräte automatisch verbunden werden.
4. Deaktivieren Sie das Kontrollkästchen **Standardwert verwenden**, wählen Sie im Dropddownmenü **Verfügbare USB-Geräte automatisch umleiten** aus und klicken Sie auf **Speichern**.

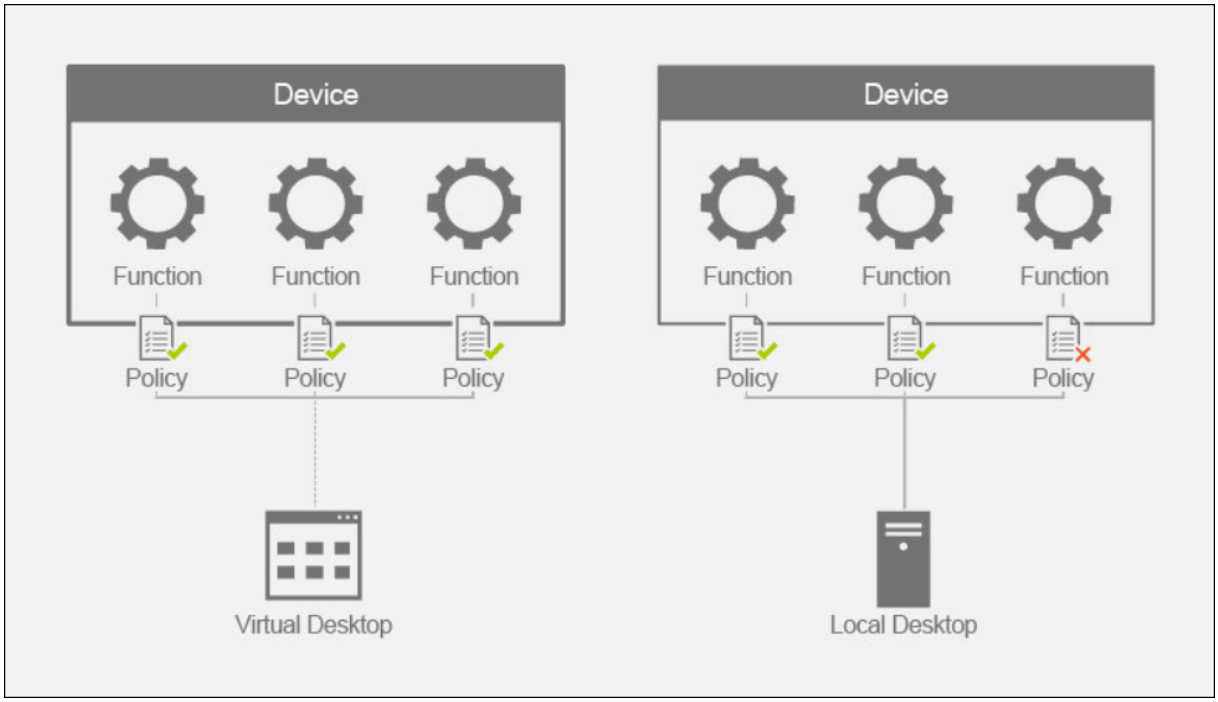
5. Bearbeiten Sie die Einstellung **Zulassen**, dass neu angeschlossene USB-Geräte automatisch verbunden werden.
6. Deaktivieren Sie das Kontrollkästchen **Standardwert verwenden**, wählen Sie im Dropddownmenü **Verfügbare USB-Geräte automatisch umleiten** aus und klicken Sie auf **Speichern**.

## Verbundgeräte und Geräteaufteilung

June 27, 2024

Ein USB-Verbundgerät ist ein einzelnes Gerät, das sich wie mehrere unabhängige USB-Geräte verhält, die an einen Computer angeschlossen sind. Es hat einen einzigen USB-Anschluss, kann jedoch mehrere Schnittstellen zum Computer bereitstellen, von denen jede über ihre eigenen Funktionen verfügt. Wenn ein Benutzer ein USB-Verbundgerät anschließt, überprüft das Hostgerät anhand jeder Richtlinienregel, ob alle Funktionen (Schnittstellen) vorhanden sind. Wenn die erste Übereinstimmung für eine Funktion (Schnittstelle) eine Deny-Regel ist, gilt die Regel für das Verbundgerät als endgültig und das Gerät wird verweigert. Wenn die erste Übereinstimmung für eine Funktion (Schnittstelle) eine Zulassungsregel ist, gleicht das Hostgerät die Regeln weiterhin mit der nächsten Funktion (Schnittstelle) ab. Das Verbundgerät ist zulässig, wenn keine Funktion (Schnittstelle) durch eine Richtlinienregel verweigert wird. Wenn die endgültige Übereinstimmung für das Verbundgerät eine Deny-Regel ist, ist das Gerät nur für den lokalen Desktop verfügbar, andernfalls wird das Gerät auf den virtuellen Desktop übertragen. Wenn keine Übereinstimmung gefunden wird, werden die Standardregeln verwendet.




Wir können das Verbundgerät mithilfe der entsprechenden Regeln in der Richtlinie für Geräteumleitungsregeln (Version 2) aufteilen, um nur bestimmte Funktionen eines Verbundgeräts zuzulassen. Zum Beispiel sollen nur die HID-Funktionen eines FIDO2-Schlüssels verwendet werden, nicht aber die Smartcardfunktionen. In diesem Fall würden die Regeln wie folgt festgelegt:

1. Connect: VID=1050 PID=0407 class=03 split=01 intf=00,01 #Yubikey series 5 lässt FIDO2 HID-Funktionen zu.
2. Deny: VID=1050 PID=0407 split=01 intf=02 # Yubikey series 5 Smartcardfunktion blockiert.

> **Tipp:**
>
> Beachten Sie beim Erstellen neuer Richtlinienregeln die USB-Klassencodes, die auf der USB-Website verfügbar sind.

### Konfiguration eines Unterschriftenfelds

1. Installieren Sie den entsprechenden Gerätetreiber auf dem VDA-Host.
2. Aktivieren Sie die **Richtlinie für die Client-USB-Geräteumleitung** in **Citrix Web Studio**.
3. Bearbeiten Sie die Richtlinie **Regeln für die Client-USB-Geräteumleitung** (**Version 2**).
    a) Stellen Sie die **VID**- und **PID**-Informationen für das Unterschriftenfeld ein, das umgeleitet werden muss, und klicken Sie auf **Speichern**. Zum Beispiel: **Connect**: VID=056A PID=00A4 #STU -430

4. Bearbeiten Sie die **Regeln für die USB-Clientgeräteoptimierung**.
    a) Stellen Sie den Modus zusammen mit anderen Geräteinformationen ein. Zum Beispiel: Mode=00000004 VID=056A PID=00A4 class=03 #Eingabegerät, das im Refassungsmodus arbeitet
5. Bearbeiten Sie die Richtlinie **Zulassen, dass vorhandene USB-Geräte automatisch verbunden werden**.
6. Deaktivieren Sie das Kontrollkästchen **Standardwert verwenden**, wählen Sie im Dropddownmenü **Verfügbare USB-Geräte automatisch umleiten** aus und klicken Sie auf **Speichern**.
7. Bearbeiten Sie die Richtlinie **Zulassen, dass neu angeschlossene USB-Geräte automatisch verbunden werden**.
8. Deaktivieren Sie das Kontrollkästchen **Standardwert verwenden**, wählen Sie im Dropddownmenü **Verfügbare USB-Geräte automatisch umleiten** aus und klicken Sie auf **Speichern**.

Sobald diese Richtlinien in der Studio-Konsole festgelegt sind, wird das Gerät bei nachfolgenden Sitzungsstarts automatisch umgeleitet, sodass keine zusätzliche Aktion des Endbenutzers erforderlich ist.

> **Hinweis:**
>
> Ersetzen Sie VID und PID durch die tatsächliche VID und PID des Geräts, das umgeleitet werden soll.

### Bloomberg-Tastatur mit der USB-Umleitung konfigurieren

1. Aktivieren Sie die **Richtlinie für die Client-USB-Geräteumleitung** in **Citrix Web Studio**.
2. Bloomberg 5-Tastaturen sind standardmäßig in der Richtlinie für Client-USB-Geräteumleitungsregeln (Version 2) festgelegt, und es sind keine zusätzlichen Administratormaßnahmen erforderlich.
3. Bearbeiten Sie die Richtlinie **Zulassen, dass vorhandene USB-Geräte automatisch verbunden werden**.
4. Deaktivieren Sie das Kontrollkästchen **Standardwert verwenden**, wählen Sie im Dropddownmenü **Verfügbare USB-Geräte automatisch umleiten** aus und klicken Sie auf **Speichern**.
5. Bearbeiten Sie die Richtlinie **Zulassen, dass neu angeschlossene USB-Geräte automatisch verbunden werden**.
6. Deaktivieren Sie das Kontrollkästchen **Standardwert verwenden**, wählen Sie im Dropddownmenü **Verfügbare USB-Geräte automatisch umleiten** aus und klicken Sie auf **Speichern**.

Sobald diese Richtlinien in der Studio-Konsole festgelegt sind, werden Bloomberg-Schlüssel in nachfolgenden HDX-Sitzungen automatisch angezeigt, sodass keine zusätzliche Aktion des Endbenutzers erforderlich ist.

### FIDO2-Schlüssel mit der USB-Umleitung konfigurieren

Citrix empfiehlt die FIDO2-Umleitung, wenn Sie FIDO2-Schlüssel in Ihren HDX-Sitzungen verwenden. Es kann jedoch Situationen geben, in denen Sie FIDO2-Schlüssel stattdessen mit der USB-Umleitung umleiten müssen. Dazu gehören Szenarien, in denen die FIDO2-Umleitung nicht verfügbar ist, weil die Funktion vom Client, dem VDA oder dem Betriebssystem (z. B. Windows Server 2016) nicht unterstützt wird.

Es kann auch Situationen geben, in denen für den Schlüssel mehrere Modi aktiviert sind, Sie jedoch nur eine Teilmenge davon in Ihren HDX-Sitzungen zulassen möchten. Beispielsweise möchten Sie FIDO2 und OTP zulassen, aber die Smartcard blockieren.

Die folgenden Schritte veranschaulichen, wie Sie einen FIDO2-Schlüssel mit der USB-Umleitung konfigurieren können (Yubikey vid=1050, pid=0407).

1. Aktivieren Sie die **Richtlinie für die Client-USB-Geräteumleitung** in **Citrix Web Studio**.
2. Bearbeiten Sie die Richtlinie **Regeln für die Client-USB-Geräteumleitung** (Version 2).
    a) Stellen Sie die **VID**- und **PID**-Informationen sowie die Konfiguration für Geräteaufteilung für den FIDO2-Schlüssel ein, der in der Sitzung umgeleitet werden soll, und klicken Sie auf **Speichern**.
    b) **Connect**: VID=1050 PID=0407 class=03 split=01 intf=00,01 #Yubikey series 5 lässt FIDO2 HID-Funktionen zu.
    c) **Deny**: VID=1050 PID=0407 split=01 intf=02 # Yubikey series 5 Smartcardfunktion blockiert.
3. Bearbeiten Sie die Richtlinie **Zulassen, dass vorhandene USB-Geräte automatisch verbunden werden**.
4. Deaktivieren Sie das Kontrollkästchen **Standardwert verwenden**, wählen Sie im Dropddownmenü **Verfügbare USB-Geräte automatisch umleiten** aus und klicken Sie auf **Speichern**.
5. Bearbeiten Sie die Richtlinie **Zulassen, dass neu angeschlossene USB-Geräte automatisch verbunden werden**.
6. Deaktivieren Sie das Kontrollkästchen **Standardwert verwenden**, wählen Sie im Dropddownmenü **Verfügbare USB-Geräte automatisch umleiten** aus und klicken Sie auf **Speichern**.

Sobald diese Richtlinien in der Studio-Konsole festgelegt sind, werden FIDO2-Tastaturen in nachfolgenden HDX-Sitzungen automatisch angezeigt, sodass keine zusätzliche Aktion des Endbenutzers erforderlich ist.

### 3D-Maus mit der USB-Umleitung konfigurieren

Heute werden die 3DConnexion SpaceMouse-Treiber nur auf Arbeitsstationsbetriebssystemen (Win 10 und Win 11) unterstützt. Sie funktionieren nicht auf dem Serverbetriebssystem. Im Folgenden finden Sie die Schritte zur Konfiguration einer SpaceMouse Enterprise auf einem Workstationbetriebssystem (vid=046D, pid=C016).

1. Installieren Sie den neuesten Windows-Treiber auf dem VDA-Host.
2. Aktivieren Sie die **Richtlinie für die Client-USB-Geräteumleitung** in **Citrix Web Studio**.
3. Bearbeiten Sie die Richtlinie **Regeln für die Client-USB-Geräteumleitung** (**Version 2**).
    a) Stellen Sie die **VID**- und **PID**-Informationen für das Unterschriftenfeld ein, das umgeleitet werden muss, und klicken Sie auf **Speichern**. Zum Beispiel: **Connect**: VID=046D PID=C016 #SpaceMouse Enterprise
4. Bearbeiten Sie die **Regeln für die USB-Clientgeräteoptimierung**.
    a) Stellen Sie den Modus zusammen mit anderen Geräteinformationen ein. Zum Beispiel: Mode=00000004 VID=046D PID=C016 class=03 #Input Gerät, das im Aufnahmemodus arbeitet
5. Bearbeiten Sie die Richtlinie **Zulassen, dass vorhandene USB-Geräte automatisch verbunden werden**.
6. Deaktivieren Sie das Kontrollkästchen **Standardwert verwenden**, wählen Sie im Dropddownmenü **Verfügbare USB-Geräte automatisch umleiten** aus und klicken Sie auf **Speichern**.
7. Bearbeiten Sie die Richtlinie **Zulassen, dass neu angeschlossene USB-Geräte automatisch verbunden werden**.
8. Deaktivieren Sie das Kontrollkästchen **Standardwert verwenden**, wählen Sie im Dropddownmenü **Verfügbare USB-Geräte automatisch umleiten** aus und klicken Sie auf **Speichern**.

## Problembehandlung

June 27, 2024

Die folgenden Schritte müssen befolgt werden, um Probleme im Zusammenhang mit der USB-Umleitung zu lösen:

1. Achten Sie darauf, dass die Systemanforderungen für die USB-Umleitung erfüllt sind. Dazu gehören korrekte CVAD- und CWA-Versionen sowie unterstützte Geräte und Gerätetreiber auf der betrachteten Betriebssystemplattform.

2. Achten Sie darauf, dass die Konfiguration auf der Grundlage der Versionen und Plattformen der Komponenten, die in Ihrer Umgebung verwendet werden, angemessen ist. Einzelheiten zu Komponenten, für die Legacy-Konfigurationseinstellungen erforderlich sind, finden Sie im Hinweis unter "Konfiguration der Legacy-USB-Umleitung".
3. Vergewissern Sie sich, dass das Gerät unter "Geräte"aufgeführt ist, die der Client aufgelistet hat.

    a) Symbolleiste für Workspace-Einstellungen: Sehen Sie sich die Geräte an, die auf der Registerkarte "Geräte"der Symbolleiste für die Einstellungen der Workspace-App aufgeführt sind (Rechtsklick auf das **CWA-Symbol > Connection Center > Einstellungen**…Klicken Sie auf die Registerkarte **Geräte**).

    b) `CtxUsbDiagnostics.exe` (Empfohlen): Führen Sie dieses Tool in einem Befehlszeilenfenster aus. Die Ausgabe enthält gerätespezifische Informationen für eine bestimmte Sitzung. Den Informationen können Sie entnehmen, ob ein Gerät umgeleitet wird oder nicht. Außerdem erfahren Sie, ob ein Geräteregelsatz dazu führt, dass das Gerät nicht umgeleitet wird. Weitere Informationen finden Sie unter Diagnosetool.

    c) USBView oder andere Tools von Drittanbietern: Führen Sie ein Drittanbietertool wie USBView auf dem Endpunkt bzw. der Clientmaschine aus, um sicherzustellen, dass das Gerät am Endpunkt erkannt wird.

4. Wenn Sie sehen, dass das Gerät aufgelistet wird:

    a) Wenn Sie in der Ausgabe des CtxUsbDiagnostics-Tools eine Deny-Regel für ein bestimmtes Gerät sehen, überprüfen Sie die in Studio konfigurierten Richtlinien und vergewissern Sie sich, dass die Regeln in der Version 2-Richtlinie korrekt festgelegt sind. Wenn die Deny-Regel nicht in der Studio-Richtlinie erscheint, überprüfen Sie die clientseitige Richtlinie und schließlich die clientseitigen Standardeinstellungen in dieser Reihenfolge, um die passende Deny-Regel zu finden.

    b) Wenn in der Ausgabe von CtxUsbDiagnostics keine Deny-Regel vorhanden ist, erlaubt CWA die Umleitung des Geräts, indem Sie die entsprechende Schaltfläche auf der Registerkarte "Geräte"des Fensters "Einstellungen"(Geräte > Geräte verwalten) aktivieren/anklicken. Wenn das Gerät einmal umgeleitet wurde, ist es in der Sitzung verfügbar. Dies kann überprüft werden, indem Sie den Gerätemanager/USBView oder eine ähnliche Anwendung in der HDX-Sitzung überprüfen.

5. Wenn Sie das Gerät in der Sitzung nicht sehen, gehen Sie wie folgt vor:

    a) Es ist möglich, dass der richtige Gerätetreiber nicht korrekt auf dem VDA-Host installiert ist. Vergewissern Sie sich, dass die neuesten Versionen der Gerätetreiber korrekt auf dem VDA-Host installiert sind. Einige Gerätetreiber werden auf Terminalservermaschinen nicht unterstützt. Vergewissern Sie sich daher, dass dies bei dem Gerät, das Sie umleiten möchten, nicht der Fall ist.

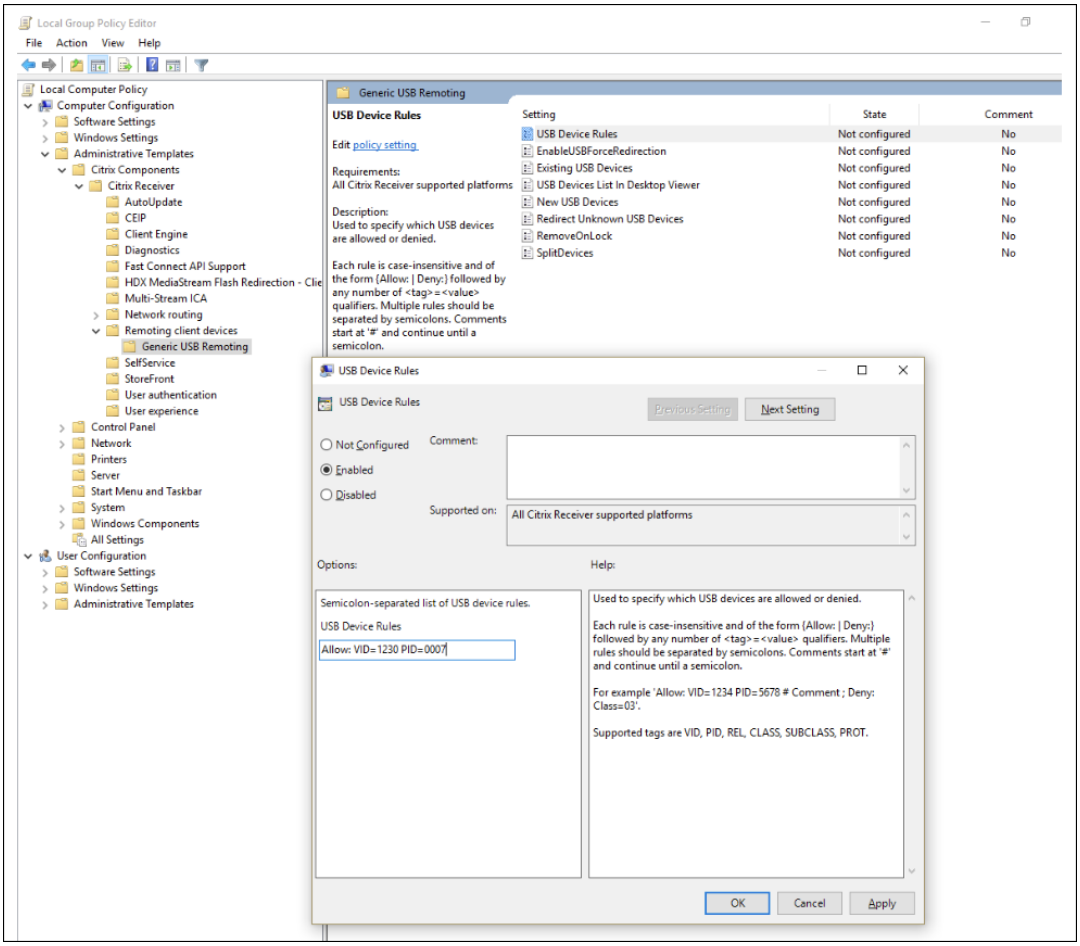
b) Vergewissern Sie sich, dass das Gerät nicht auf dem Clientendpunkt verwendet wird. Bei einigen Geräten müssen Treiber auch auf dem Clientendpunkt installiert werden. Dies könnte verhindern, dass sie in der Sitzung umgeleitet werden.

6. Vergewissern Sie sich, dass USB-bezogene Regeln auf dem Clientendpunkt korrekt festgelegt sind:

   a) **Citrix Workspace-App für Windows**:

      i. Vergewissern Sie sich, dass die Gruppenrichtlinie auf dem Client (fügen Sie weitere Details und SS hinzu) ordnungsgemäß festgelegt ist und nicht mit den in Studio festgelegten Regeln in Konflikt steht.

      ii. Überprüfen Sie diese Standardregeln in der Registrierung des Clients.




(`HKLM\SOFTWARE\Wow6432Node\Citrix\PortICA\GenericUSB\DeviceRules`)are appropriately set and not in conflict with the rules set in Studio and client group policy.

b) Citrix Workspace-App für Linux —Informationen zur Prüfung von Citrix Workspace-App für Linux-Problemen finden Sie in der USB-Dokumentation für Citrix Workspace-App für Linux

c) CWA für Mac: Informationen zur Behebung von Problemen mit CWA für Mac finden Sie unter CWA für Mac

**Hinweis:**

- Auf TSVDA werden Audiogeräte standardmäßig daran gehindert, die USB-Umleitung zu verwenden. Zur Verwendung dieser Geräte wird optimierter Audio VC empfohlen.
- Manchmal werden USB-Verbundgeräte möglicherweise nicht automatisch aufgeteilt, obwohl eine korrekte Geräteumleitungsregel festgelegt ist, um das Gerät aufzuteilen. Dieses Problem tritt auf, weil sich das Gerät im Energiesparmodus befindet. In diesen Fällen ist das untergeordnete Gerät, das in den Energiesparmodus wechselt, möglicherweise nicht in der Geräteliste enthalten. Sie können die folgenden Problemumgehungen verwenden, um dieses Problem zu lösen:

  - Trennen Sie die Sitzung, schließen Sie das USB-Gerät an und stellen Sie erneut eine Verbindung zur Sitzung her.

  - Trennen Sie das USB-Gerät und schließen Sie es wieder an. Diese Aktion führt dazu, dass das Gerät den Energiesparmodus verlässt.
- Manchmal können die USB-Akkuspareinstellungen aktiviert werden, um die Akkulaufzeit zu optimieren. Wenn der Clientendpunkt in den Ruhezustand wechselt, wird das USB-Gerät möglicherweise getrennt. In einem solchen Szenario müssen Sie das Gerät möglicherweise trennen und erneut verbinden, um es erneut in der Sitzung zu präsentieren.

### Ereignisprotokolle

Administratoren können jetzt nach nicht autorisierten Geräten suchen, die Benutzer möglicherweise umleiten möchten, und die entsprechenden Maßnahmen ergreifen. Im Folgenden finden Sie einige Ereignismeldungen, die in der Ereignisanzeige auf dem VDA-Host für Geräte, die umgeleitet werden dürfen und für Geräte, die nicht umgeleitet werden dürfen, protokolliert werden.

| | |
|---|---|
| **Id** | 1000 |
| **Name** | UsbEventAcceptDevice |
| **Severity** | Informational |
| **Facility** | System |
| **Text** | The Citrix USB Service allows the USB Device with Product ID: %2, Vendor ID: %3, and Device ID: %4 to be remoted. |
| **Comment** | This message logs the device info of a device redirected in an HDX session |

| | |
|---|---|
| **Id** | 1001 |
| **Name** | UsbEventPolicyRejectsDeviceV1 |
| **Severity** | Warning |
| **Facility** | System |
| **Text** | The USB device with Product ID: 0x%2, Vendor ID: 0x%3, and Device ID: 0x%4 is not being redirected because the Citrix USB policy, "DENY: ...%5..." is in effect. If you wish to redirect the device, please set an allow rule that matches the device in the "Client USB device redirection rules" policy in Citrix Studio. |
| **Comment** | This message displays a message of the device not getting redirected if a DENY rule is being enforced by the legacy “Client USB device redirection rules” policy rule. |
| **Arguments** | |

| | |
|---|---|
| **Id** | 1002 |
| **Name** | UsbEventPolicyRejectsDeviceV2 |
| **Severity** | Warning |
| **Facility** | System |
| **Text** | The USB device with Product ID: 0x%2, Vendor ID: 0x%3, and Device ID: 0x%4 is not being redirected because the Citrix USB policy, "DENY: ...%5..." is in effect. If you wish to redirect the device, please set an allow rule that matches the device in the "Client USB device redirection rules (Version 2)" policy in Citrix Studio. |
| **Comment** | This message displays a message of the device not getting redirected if a DENY rule is being enforced by the "Client USB device redirection rules (Version 2)" policy rule. For instance, if the studio policy rule allows an approved set of devices and denies all other devices and an end user tries to create a new rule on the client endpoint via group policy, this event will get logged. This message would be indicative of an unauthorized device redirection attempt. |
| **Arguments** | |

## USB-Diagnosetool

June 27, 2024

`CtxUsbDiagnostics.exe` ist ein Befehlszeilentool auf dem VDA, mit dem Citrix-Administratoren Probleme mit der USB-Geräteumleitung auf dem Client schneller diagnostizieren und lösen können. Dieses Hilfsprogramm sammelt wichtige Informationen, die zur Priorisierung von Konfigurationsproblemen im Zusammenhang mit an den Client angeschlossenen USB-Geräten erforderlich sind, die innerhalb einer HDX-Sitzung nicht umgeleitet werden können.

## Anforderungen

### Sitzungshost

- Betriebssystem
  - Windows 10 1809 oder höher
  - Windows 11 21H2 oder höher
  - Windows Server 2016 oder höher
- VDA
  - Windows: Citrix Virtual Apps and Desktops Version 2311 oder höher

### Clientgerät

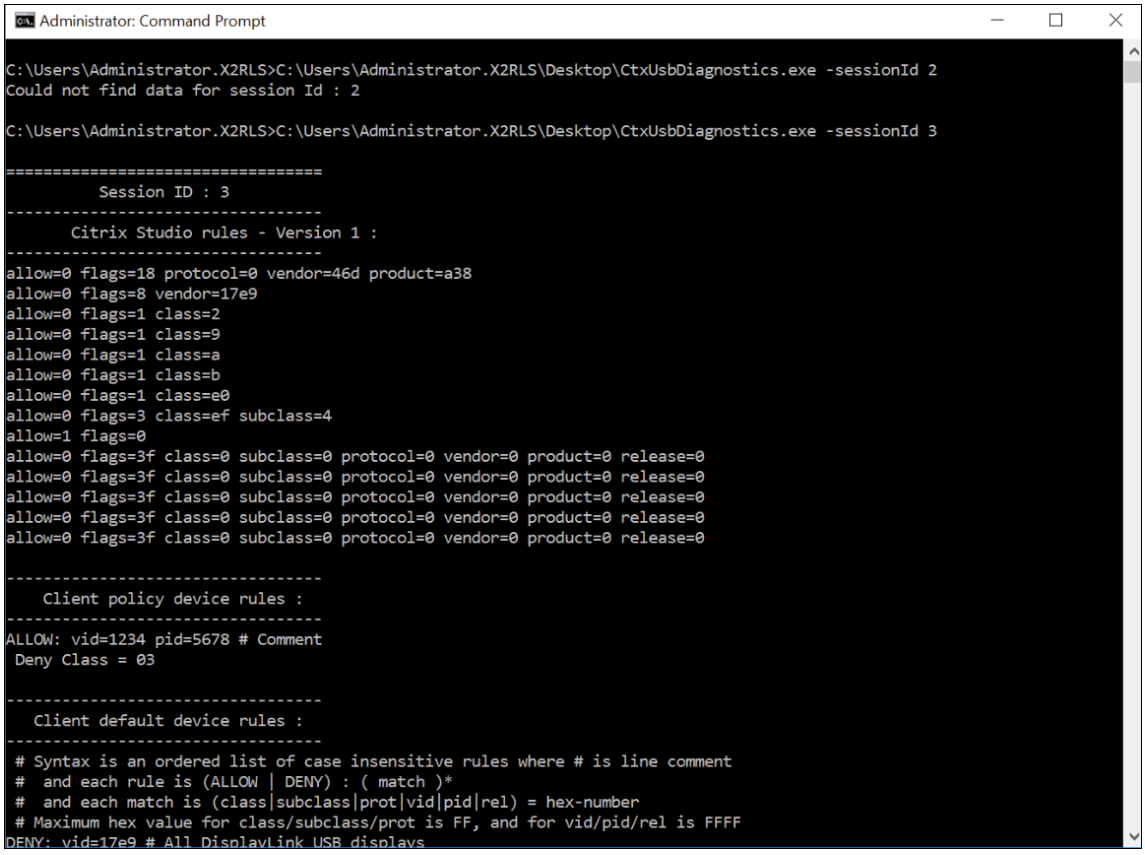
- Betriebssystem
  - Windows 10 1809 oder höher
- Workspace-App
  - Windows: Version 2311 oder höher

## Was macht das Tool?

Das Tool bietet derzeit:

- SessionID
- VDA-Geräterichtlinien (in Studio festgelegte Geräteregeln)
- Clientgeräte und Clientgeräterichtlinien (Geräteregeln)
- Liste der Geräte, deren Umleitungsstatus und warum sie zugelassen oder verweigert wurden




> **Hinweis:**
>
> Der Administrator kann Geräteinformationen für alle aktiven Sitzungen einsehen.

### Angezeigte Informationen

- **Citrix Studio-Regeln – Version 1/2**
  - Die DDC-Regeln geben die Verwendung der veralteten Richtlinie "**Regeln für die Client-USB-Geräteumleitung**"oder "**Regeln für die Client-USB-Geräteumleitung (Version 2)**" in Studio an. Die in diesem Abschnitt aufgeführten Informationen enthalten alle Regeln, die vom Citrix-Administrator konfiguriert wurden.

```
C:\Program Files\Citrix\HDX\bin>CtxUsbDiagnostics.exe

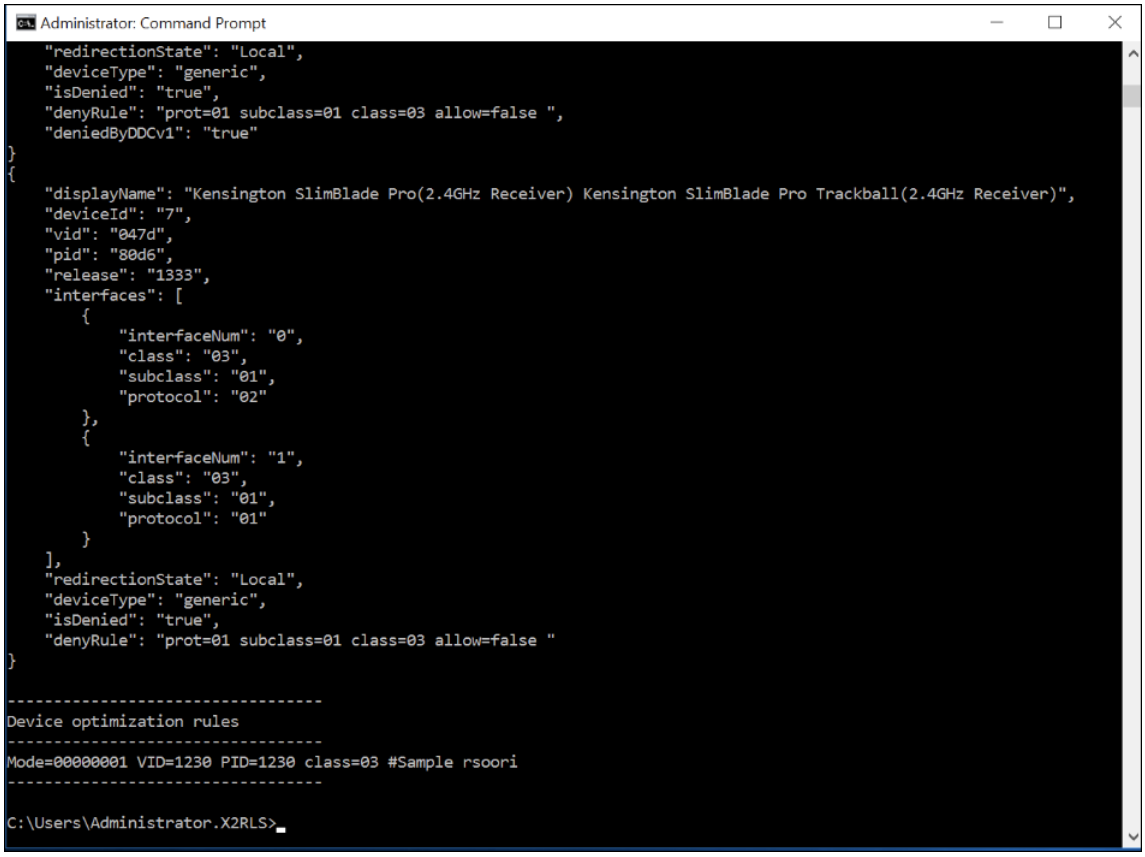
---------------------------------
          Session ID : 1
---------------------------------
       Citrix Studio rules - Version 2 :
---------------------------------
DENY: vid=046D pid=0A38
# Block some devices we never want to see
DENY: vid=17e9 # All DisplayLink USB displays
```

- **Standardgeräteregeln für Clients**
  - In diesem Abschnitt werden die Regeln aufgeführt, die in der Registrierung auf dem Client festgelegt sind.

```
---------------------------------
  Client default device rules :
---------------------------------
 # Syntax is an ordered list of case insensitive rules where # is line comment
 #  and each rule is (ALLOW | DENY) : ( match )*
 #  and each match is (class|subclass|prot|vid|pid|rel) = hex-number
 # Maximum hex value for class/subclass/prot is FF, and for vid/pid/rel is FFFF
DENY: vid=17e9 # All DisplayLink USB displays
CONNECT: vid=1188 pid=A101 # Bloomberg 5 Biometric module
DENY: vid=1188 pid=A001 split=01 intf=00 # Bloomberg 5 Primary keyboard
CONNECT: vid=1188 pid=A001 split=01 intf=01 # Bloomberg 5 Keyboard HID
DENY: vid=1188 pid=A301 split=01 intf=02 # Bloomberg 5 Keyboard Audio Channel
CONNECT: vid=1188 pid=A301 split=01 intf=00,01 # Bloomberg 5 Keyboard Audio HID
DENY: class=02 # Communications and CDC-Control
DENY: class=09 # Hub devices
DENY:vid=045e pid=079A # Microsoft Surface Pro 1 Touch Cover
DENY:vid=045e pid=079c # Microsoft Surface Pro 1 Type Cover
DENY:vid=045e pid=07dc # Microsoft Surface Pro 3 Type Cover
DENY:vid=045e pid=07dd # Microsoft Surface Pro JP 3 Type Cover
DENY:vid=045e pid=07de # Microsoft Surface Pro 3_2 Type Cover
DENY:vid=045e pid=07e2 # Microsoft Surface Pro 3 Type Cover
DENY:vid=045e pid=07e4 # Microsoft Surface Pro 4 Type Cover with fingerprint reader
DENY:vid=045e pid=07e8 # Microsoft Surface Pro 4_2 Type Cover
DENY:vid=03eb pid=8209 # Surface Pro Atmel maXTouch Digitizer
ALLOW:vid=056a pid=0315 class=03 # Wacom Intuos tablet
ALLOW:vid=056a pid=0314 class=03 # Wacom Intuos tablet
ALLOW:vid=056a pid=00fb class=03 # Wacom DTU tablet
DENY: class=03 subclass=01 prot=01 # HID Boot keyboards
DENY: class=03 subclass=01 prot=02 # HID Boot mice
DENY: class=0a # CDC-Data
DENY: class=0b # Smartcard
DENY: class=e0 # Wireless controller
DENY: class=ef subclass=04 # Miscellaneous network devices
ALLOW: # Otherwise allow everything else
```

- **Regeln zur Geräteoptimierung**
  - In diesem Abschnitt werden die Regeln zur Geräteoptimierung aufgeführt, wie sie unter “Regeln zur Optimierung von Client-USB-Geräten”festgelegt sind.




### Geräteliste

Dieser Abschnitt enthält wichtige Informationen zu jedem mit dem Clientendpunkt verbundenen Gerät, zur Hardware, zu eventuell vorhandenen Umleitungen, zur Einhaltung einer gegebenenfalls festgelegten Geräteumleitungsregel und so weiter.

| Tagname | Beschreibung |
|---|---|
| displayName | Listet den allgemeinen Namen des Geräts auf. |
| vid | Anbieter-ID |
| pid | Produkt-ID |
| Interfaces | In diesem Unterabschnitt werden alle Schnittstellen für den Fall aufgeführt, dass das Verbundgerät in mehrere untergeordnete Geräte aufgeteilt wurde. |
| InterfaceNum | Gibt den Index des Schnittstellendeskriptors an |
| class | Klassencode |

| Tagname | Beschreibung |
| --- | --- |
| subclass | Unterklassencode |
| Protokoll | Protokoll |
| redirectionState | **Local** gibt an, dass das Gerät in der ICA-Sitzung nicht umgeleitet wird. **ThisSession** gibt an, dass das Gerät in der ICA-Sitzung umgeleitet wird. **OtherSession** gibt an, dass das Gerät in einer anderen ICA-Sitzung umgeleitet wird. |
| optiEnabled | **true** gibt an, dass das Gerät optimiert ist. **false** bedeutet, dass das Gerät nicht optimiert ist und die Datenübertragung über den virtuellen USB-Kanal erfolgt. |
| deviceType | **generic** gibt an, dass das Gerät keinen optimierten virtuellen Kanal hat und der Datenverkehr über den virtuellen USB-Kanal fließt. **optimized** bedeutet, dass die mit dem Gerät verbundene Datenübertragung über einen dedizierten virtuellen Kanal erfolgt. |
| isDenied | **true** gibt an, dass das Gerät aufgrund einer vom Administrator festgelegten Richtlinienregel nicht umgeleitet wird. **false** bedeutet, dass das Gerät aufgrund einer angewendeten Richtlinie umgeleitet wurde. |
| denyRule | Dieses Feld ist nützlich, wenn isDenied auf **true** gesetzt ist. Es teilt dem Administrator die spezifische Regel mit, die in der Richtlinie festgelegt ist und dazu führt, dass das Gerät nicht umgeleitet wird. |

## Konfiguration der Legacy-USB-Umleitung

June 27, 2024

Wenn Sie Komponenten verwenden, die älter als Version 2212 sind, oder wenn Sie CWA für Linux verwenden, folgen Sie dieser Anleitung zur Konfiguration der USB-Umleitung in Ihrer Umgebung.

### Generische USB-Umleitung aktivieren

1. Öffnen Sie die **Citrix Web Studio-Richtlinien** und klicken Sie auf die Registerkarte **Richtlinien**.
2. Klicken Sie auf **Richtlinie erstellen** und erweitern Sie **ICA > USB-Geräterichtlinien**.
3. Bearbeiten Sie die **Richtlinie für die Client-USB-Geräteumleitung**.
4. Wählen Sie **Zugelassen** aus und klicken Sie auf **Speichern**.

### Richtlinienregeln für die USB-Umleitung erstellen

Wenn der Benutzer versucht, ein USB-Gerät an den virtuellen Desktop umzuleiten, wird es nacheinander mit jeder USB-Richtlinienregel verglichen, bis eine Übereinstimmung gefunden wird. Die erste Übereinstimmung für ein beliebiges Gerät gilt als endgültig. Wenn es sich bei der ersten Übereinstimmung um eine Allow-Regel handelt, darf das übereinstimmende Gerät auf den virtuellen Desktop umgeleitet werden. Handelt es sich um eine Deny-Regel, kann das Gerät nur auf dem lokalen Desktop verwendet werden. Wenn keine Übereinstimmung gefunden wird, werden die Standardregeln verwendet.

**Richtlinie auf dem Desktop Delivery Controller einstellen:**

1. Öffnen Sie die **Citrix Web Studio-Richtlinien** und klicken Sie auf die Registerkarte **Richtlinien**.
2. Klicken Sie auf **Richtlinie erstellen** und erweitern Sie **ICA > USB-Geräterichtlinien**.
3. Bearbeiten Sie die **Regeln für die Client-USB-Geräteumleitung**.
4. Stellen Sie den Wert anhand der Beispiele in der Beschreibung für jedes USB-Gerät ein, das umgeleitet werden muss, und klicken Sie auf “Speichern”.
   Beispiel:
   Allow: VID=056A PID=00A4 #STU-430
   Deny: Class=08 subclass=05 # Mass Storage

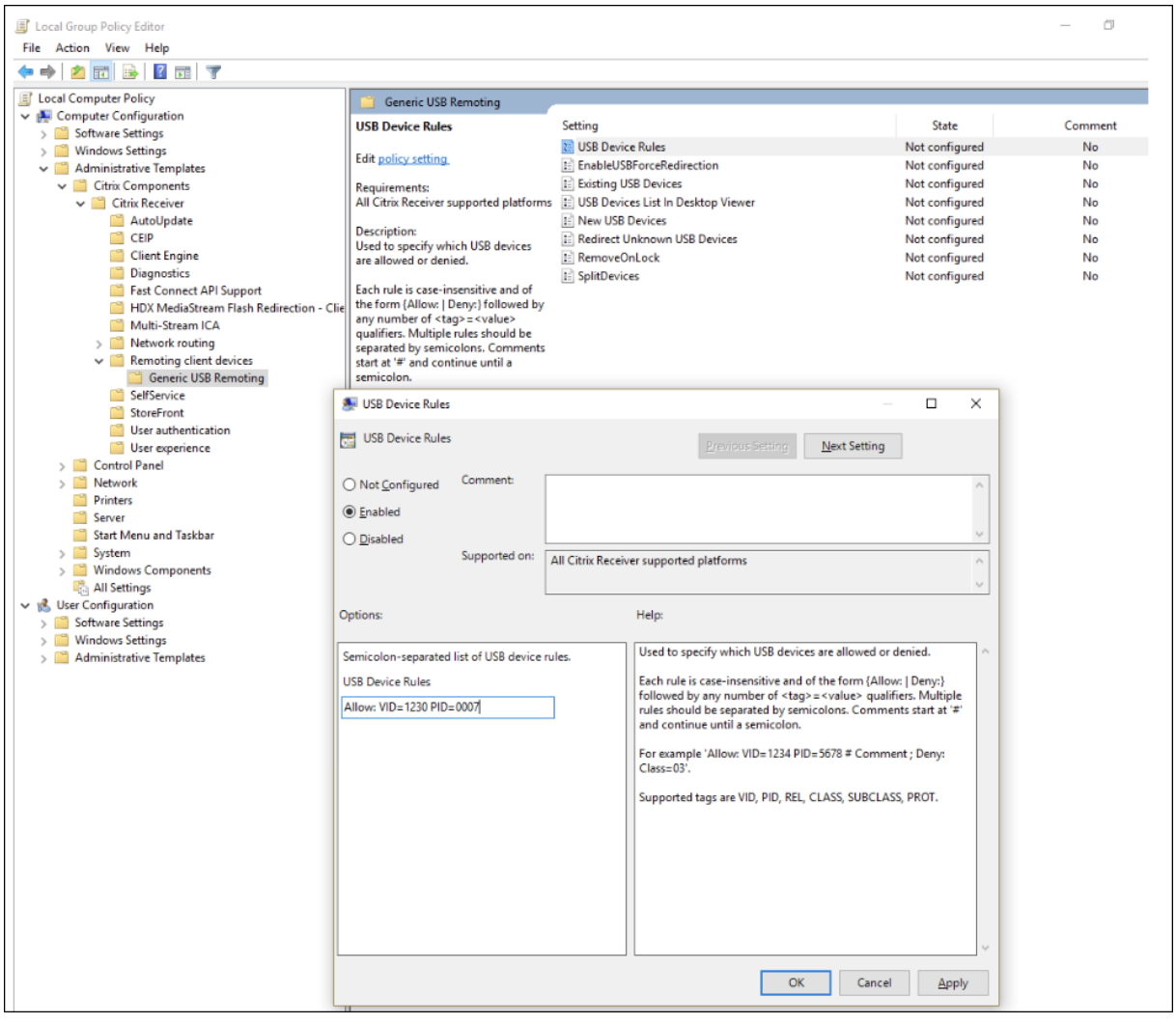
   > **Hinweis:**
   >
   > Wenn ein Citrix-Administrator die Option Standardwert verwenden aktiviert und auf Speichern klickt, sind die Standardregeln in der folgenden Registrierung im VDA zu finden.
   >
   > **Achtung:**
   >
   > Lesen Sie den Haftungsausschluss am Ende dieses Artikels, bevor Sie den Registrierungs-Editor verwenden.
   > `HKLM\SOFTWARE\Wow6432Node\Citrix\PortICA\GenericUSB\DeviceRules`

**GPOs auf dem Client verwenden:**

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 die Einstellung **USB-Geräteregeln** und aktivieren Sie sie. Fügen Sie die USB-Geräteregel wie in diesem Beispiel hinzu.
   Die Regel Allow: VID=1230 PID=0007 lässt das Gerät mit der Vendor-ID 1230 und der Produkt-ID 0007 zu.

> **Hinweis:**
>
> Verwenden Sie die Regel Allow: VID=xxxx PID=xxxx„ wenn ein bestimmtes Gerät ganz oben auf der Liste der Geräteregeln stehen muss.




> **Hinweis:**
>
> Ein Tool wie USBView oder sogar die Verbindungssymbolleiste können verwendet werden, um

> die Gerätedetails wie VID und PID zu ermitteln (SS hier einbeziehen).

### Konfigurieren der automatischen Umleitung von USB-Geräten

USB-Geräte werden automatisch umgeleitet, wenn die USB-Unterstützung aktiviert ist. Außerdem sind die USB-Benutzereinstellungen für eine automatische Verbindung der USB-Geräte konfiguriert. 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 entweder auf dem Clientendpunkt oder in der DDC-Richtlinie DeviceRules.

Diese Richtlinie kann auf dem DDC, dem Client über ein GPO, über Citrix Workspace-Einstellungen oder auf der Registerkarte "Verbindungen"unter CDViewer festgelegt werden. Alle diese Methoden werden im Folgenden beschrieben:

**Richtlinie auf dem Desktop Delivery Controller einstellen:**

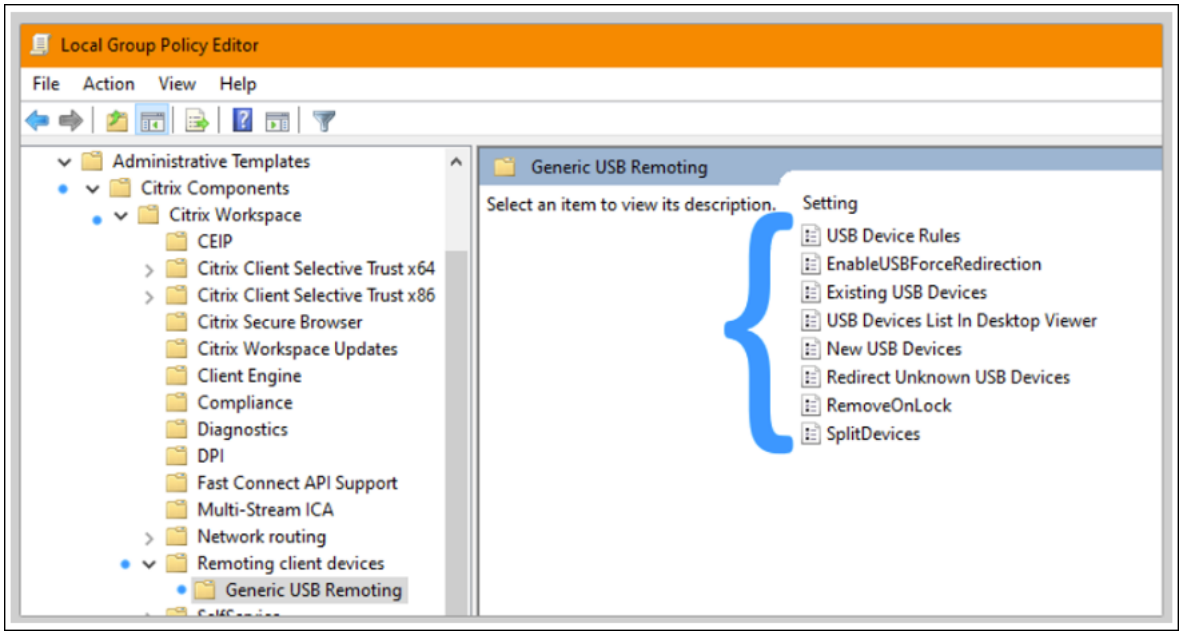
Auf dem DDC gibt es zwei Richtlinien, die so eingestellt werden können, dass die automatische Umleitung von USB-Geräten zulässig ist: "Zulassen, dass vorhandene USB-Geräte automatisch verbunden werden, Zulassen, dass neu angeschlossene USB-Geräte automatisch verbunden werden".

1. Öffnen Sie die **Citrix Web Studio-Richtlinien** und klicken Sie auf die Registerkarte **Richtlinien**.
2. Klicken Sie auf **Richtlinie erstellen** und erweitern Sie **ICA > USB-Geräterichtlinien**.
3. Bearbeiten Sie die Einstellung **Zulassen, dass vorhandene USB-Geräte automatisch verbunden werden**.
4. Deaktivieren Sie das Kontrollkästchen **Standardwert verwenden**, wählen Sie im Dropddownmenü **Verfügbare USB-Geräte automatisch umleiten** aus und klicken Sie auf **Speichern**.
5. Bearbeiten Sie die Einstellung **Zulassen, dass neu angeschlossene USB-Geräte automatisch verbunden werden**.
6. Deaktivieren Sie das Kontrollkästchen **Standardwert verwenden**, wählen Sie im Dropddownmenü **Verfügbare USB-Geräte automatisch umleiten** aus und klicken Sie auf **Speichern**.

**GPOs auf dem Client verwenden:**

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**.




**Mit Citrix Connection Center:**

1. Gehen Sie zu **Citrix Workspace-Einstellungen > Verbindungen**.
2. Vergewissern Sie sich, dass die folgenden Optionen ausgewählt sind:

    a) Geräte beim Start einer Sitzung automatisch verbinden
    b) Wenn ein neues Gerät angeschlossen wird, während eine Sitzung ausgeführt wird, wird das Gerät automatisch verbunden

3. Klicken Sie auf **OK**.

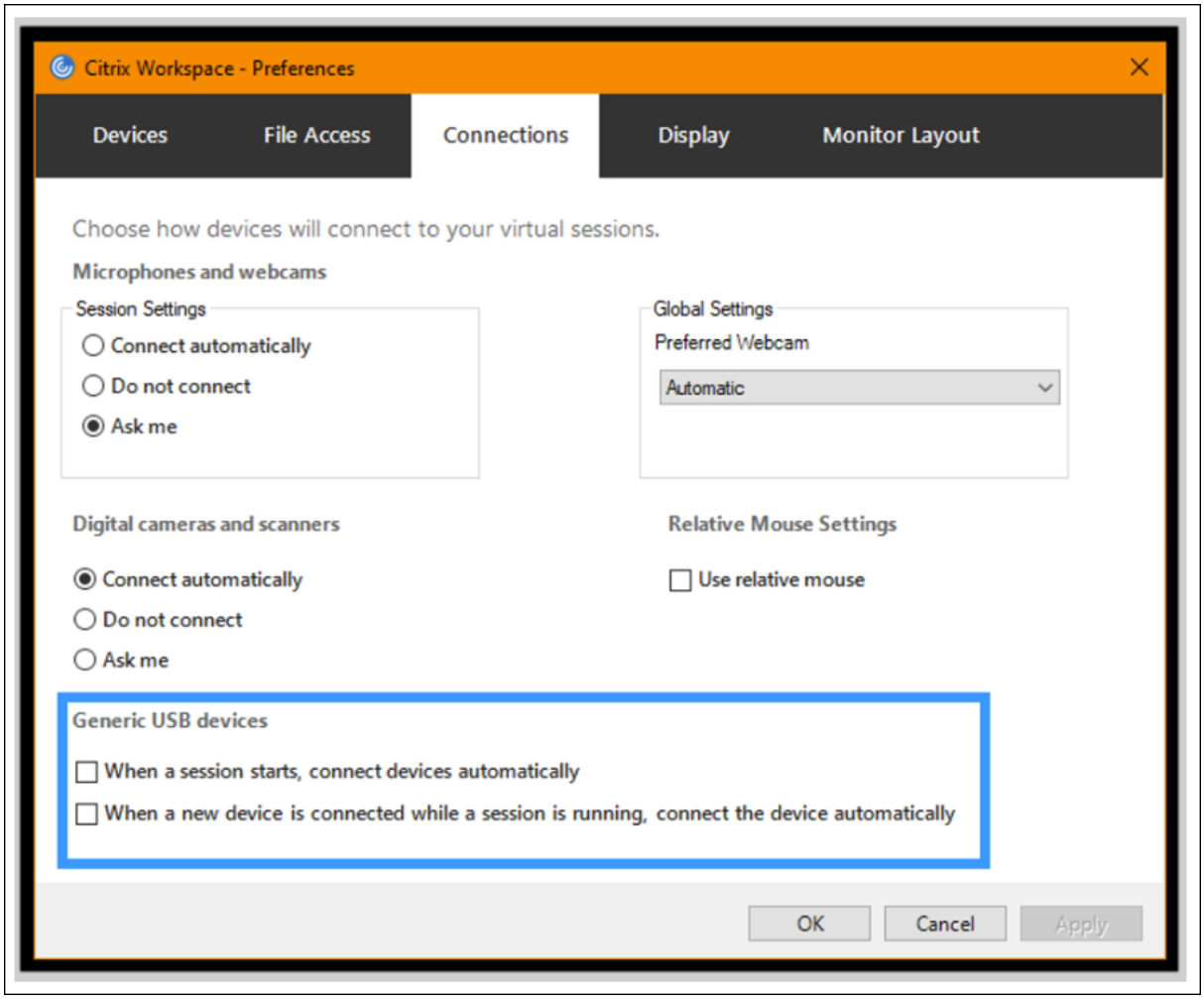
**Mit CDViewer-Verbindungssymbolleiste:**

1. Klicken Sie nach dem Start einer Sitzung auf das Dropdownmenü **CDViewer** und wählen Sie die Registerkarte **Citrix Workspace-Einstellungen > Verbindungen** aus.
2. Vergewissern Sie sich, dass die folgenden Optionen ausgewählt sind:

    a) Geräte beim Start einer Sitzung automatisch verbinden
    b) Wenn ein neues Gerät angeschlossen wird, während eine Sitzung ausgeführt wird, wird das Gerät automatisch verbunden

3. Klicken Sie auf **Übernehmen** und auf **OK**, um die Richtlinie zu speichern.




Für die clientbasierten Konfigurationen werden die Registrierungsschlüssel auf das Clientgerät an der folgenden Stelle gesetzt:

> **Achtung:**
>
> Lesen Sie den Haftungsausschluss am Ende dieses Artikels, bevor Sie den Registrierungs-Editor verwenden.
>
> `HKLM\SOFTWARE\Wow6432Node\Citrix\ICA Client\GenericUSB`

## Clientlaufwerkzuordnung (Clientlaufwerkzuordnung)

June 27, 2024

Die Clientlaufwerkzuordnung stellt Speicherlaufwerke auf dem Clientendpunkt innerhalb einer Citrix HDX-Sitzung zur Verfügung, sodass Dateien und Ordner zwischen Client und Sitzungshost übertragen werden können. Das Feature ist standardmäßig mit Lese- und Schreibrechten aktiviert. 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 sich vergewissern, dass die Einstellung **"Clientlaufwerkumleitung"** auf **Zugelassen** festgelegt und zur Richtlinie hinzugefügt ist.

Aus Sicherheitsgründen werden Endpunktlaufwerke standardmäßig ohne Ausführungsberechtigung zugeordnet. Damit Benutzer ausführbare Dateien direkt von den zugeordneten Clientlaufwerken ausführen können, bearbeiten Sie den Registrierungswert **ExecuteFromMappedDrive** auf dem Sitzungshost. Weitere Informationen finden Sie unter Zugeordnete Clientlaufwerke in der Liste **Über die Registrierung verwaltete HDX-Features**.

## Anforderungen

Die folgenden Anforderungen gelten für die Verwendung der Clientlaufwerkzuordnung:

### Citrix Steuerungsebene

- Citrix Virtual Apps and Desktops 1912 oder höher
- Citrix DaaS

### Sitzungshost

- Betriebssystem
  - Windows 10 1809 oder höher
  - Windows Server 2016 oder höher
  - Linux: Siehe Linux VDA-Systemanforderungen.
- VDA
  - Windows: Citrix Virtual Apps and Desktops 1912 oder höher
  - Linux: Siehe Linux VDA-Dokumentation.

### Clientgerät

- Betriebssystem
  - Windows 10 1809 oder höher
  - Linux: Siehe Systemanforderungen der Workspace-App für Linux.

### Relevante Richtlinien

Informationen zu den Einstellungen für die Clientlaufwerkzuordnung finden Sie unter Referenz für Richtlinieneinstellungen.

### Double-Hop-Szenarien

Die Clientlaufwerkzuordnung wird in Double-Hop-Szenarien unterstützt. Standardmäßig wird das Laufwerk des Clientendpunkts in der zweiten Hop-Sitzung zugeordnet und die Laufwerke des ersten Hop sind nicht verfügbar. Dies kann jedoch so konfiguriert werden, dass die Laufwerke der ersten Hop-Sitzung in der zweiten Hop-Sitzung anstelle der Laufwerke des Clientendpunkts zugeordnet werden.

Um diese Funktion zu konfigurieren, bearbeiten Sie den folgenden Registrierungswert:

- Schlüssel: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Adva
- Wertname: NativeDriveMapping
- Werttyp: REG_SZ
- Wertdaten:
  - True: Ordnet die Laufwerke der ersten Hop-Sitzung der zweiten Hop-Sitzung zu.
  - False: Ordnet die Laufwerke des Clientendpunkts in der zweiten Hop-Sitzung zu.

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

## Unterstützung für mobile Clientgeräte und Clientgeräte mit Touchscreen

June 27, 2024

Mit Citrix Virtual Apps and Desktops können Benutzer von mobilen Clientgeräten und Clientgeräten mit Touchscreen aus auf ihre veröffentlichten Anwendungen und Desktops zugreifen.

## Anforderungen

### Citrix Steuerungsebene

- Citrix Virtual Apps and Desktops 1912 oder höher
- Citrix DaaS

### Sitzungshost

- Betriebssystem
  - Windows 10 1903 oder höher
  - Windows 11 21H2 oder höher
  - Windows Server 2016 oder höher
- VDA
  - Windows: Citrix Virtual Apps and Desktops Version 7.15 oder höher

### Clientgerät

- Betriebssystem
  - Windows 10 1809 oder höher
  - Windows 11 21H2 oder höher
- Citrix Workspace-App für Windows Version 1808 oder höher

## Tabletmodus für Touchscreengeräte mit Windows Continuum

Continuum ist ein Windows 10-Feature, das sich an die Art und Weise der Verwendung des Clientgeräts anpasst. Wenn der VDA erkennt, dass eine Tastatur oder Maus an einen Client mit Touchscreen angeschlossen ist, versetzt er den Client in den Desktopmodus. Ist keine Tastatur oder Maus vorhanden, versetzt der VDA den Client in den Tablet-/Mobilgerätemodus. Diese Erkennung erfolgt bei der Verbindung und Wiederverbindung der Sitzung sowie während der Sitzung, wenn eine Tastatur oder Maus angeschlossen oder getrennt wird.

Das Feature ist in der Standardeinstellung aktiviert. Um diese Funktion zu deaktivieren, konfigurieren Sie die Richtlinieneinstellung Tabletmodus ein/aus.

Zusätzlich zu den oben genannten Anforderungen für Touchscreengeräte müssen für Windows Continuum die folgenden Anforderungen erfüllt sein:

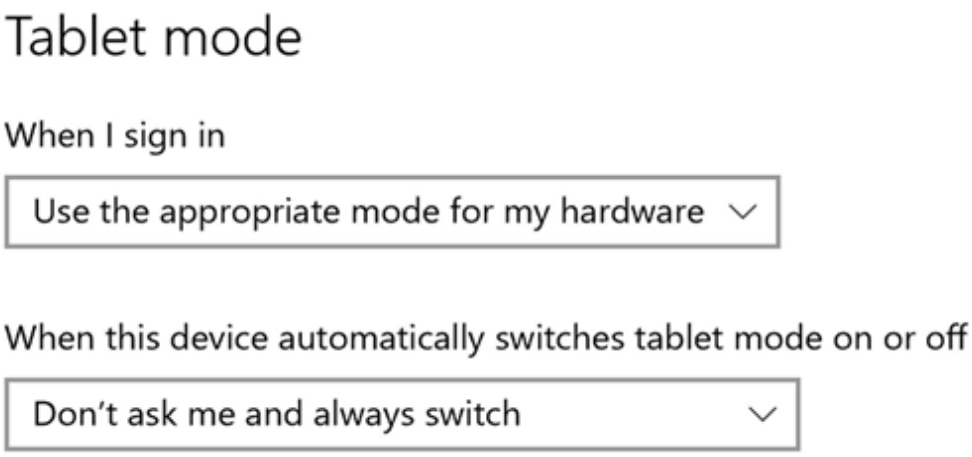
**XenServer (ehemals Citrix Hypervisor)**

- Citrix Hypervisor 8.2 oder höher
- 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 Basisimage 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.

**Sitzungshost**

- Betriebssystem
  - Windows 10 1903 oder höher
  - Windows 11 21H2 oder höher
- VDA
  - Windows: Version 7.16 oder höher
  - **Aufgrund der aktuellen Einschränkungen in den Betriebssystemkonfigurationen muss der Benutzer nach dem Start der ersten ICA-Sitzung die folgenden Optionen in den Dropdownmenüs festlegen und dann den VDA neu starten:**
    - **Einstellungen > System > Tabletmodus**
      - Passenden Modus für meine Hardware verwenden
      - Nicht fragen und immer wechseln




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.

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 unterstützt keine Windows Continuum-Features.

Der **Desktopmodus** ist die klassische Benutzeroberfläche, bei der die Interaktion wie bei einem PC mit Tastatur und Maus erfolgt.

### Microsoft Surface Pro und Surface Book-Stifte

Standardstiftfunktionen bei Windows Ink-basierten Anwendungen werden unterstützt. 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. Dieses Feature ist standardmäßig aktiviert.

Im Folgenden sind die Anforderungen für die Unterstützung der Stiftfunktionalität aufgeführt:

#### Citrix Steuerungsebene

- Citrix Virtual Apps and Desktops 1903 und höher
- Citrix DaaS

**Sitzungshost**

- Betriebssystem
  - Windows 10 1809 oder höher
  - Windows 11 21H2 oder höher
  - Windows Server 2016 oder höher
- VDA
  - Windows: Citrix Virtual Apps and Desktops 1903 oder höher

**Clientgerät**

- Betriebssystem
  - Windows 10 1809 oder höher
  - Windows 11 21H2 oder höher
- Citrix Workspace-App für Windows Version 1902 oder später

Für eine Demonstration von Windows Ink und der Stiftfunktionalität klicken Sie auf folgende Grafik:


Informationen zum Deaktivieren oder Aktivieren dieses Features finden Sie unter Microsoft Surface Pro und Surface Book-Stifte in der Liste der über die Registrierung verwalteten Features.

### Bekannte Probleme

Die folgenden Probleme mit der Stiftunterstützung sind bekannt:

- Aufgrund von Betriebssystembeschränkungen in Windows Server 2k22 können Benutzer keine Stiftverknüpfungen einrichten oder Stift-/Tinteneinstellungen in der Systemsteuerung anpassen, wenn sie eine Verbindung zu 2k22-Serveranwendungen oder Desktops herstellen.
- Stiftverknüpfungen werden von einem für Stifte aktivierten Windows 11-Client aufgrund von Betriebssystemeinschränkungen nicht beachtet.

## Serielle Ports

June 27, 2024

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 Unterschriftenpad) nur dann zuverlässig, wenn es über COM1 oder COM2 an der Clientarbeitsstation angeschlossen ist.

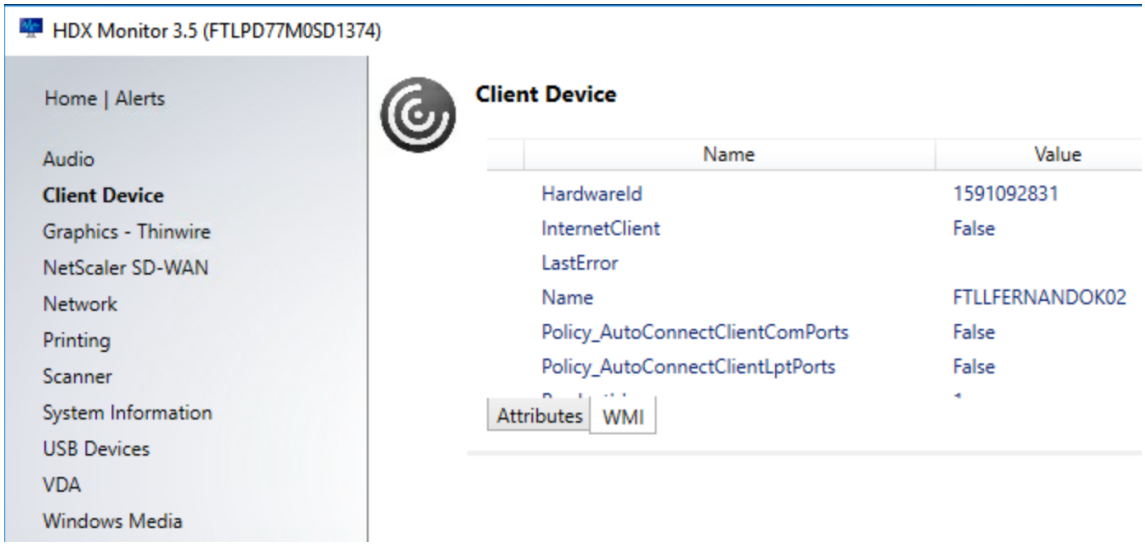
 

### Zuordnen eines COM-Ports für Clients zu einem Server-COM-Port

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.

```
C:\Windows\system32>net use
New connections will be remembered.


Status       Local     Remote                    Network

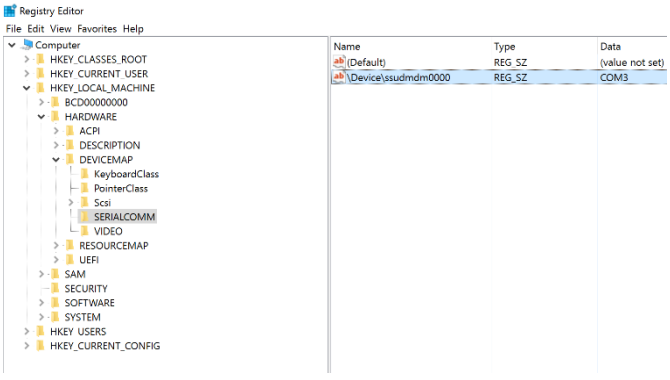
-------------------------------------------------------------------------------
             COM3      \\Client\COM3:            Citrix Client Network
```

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.

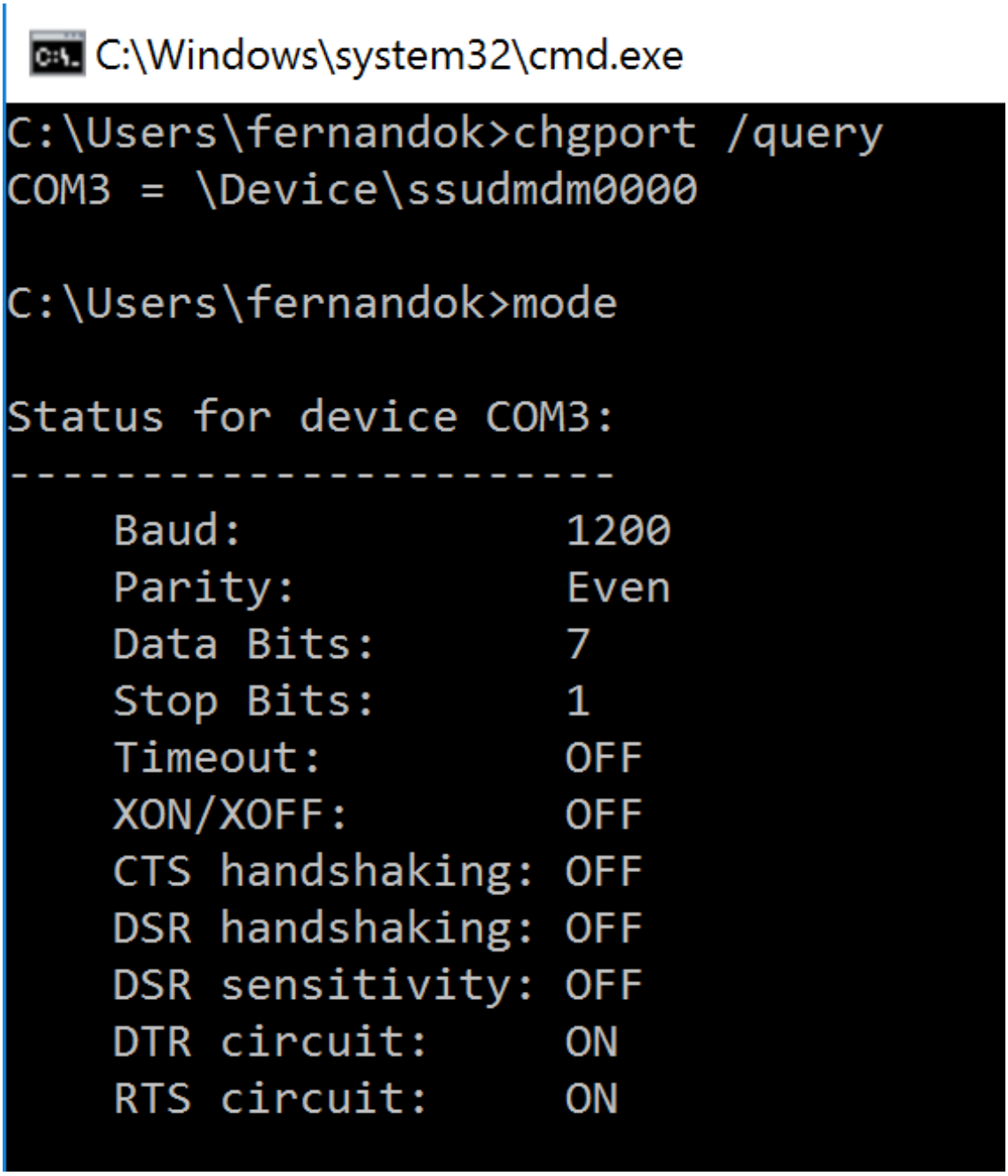
## Problembehandlung

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:



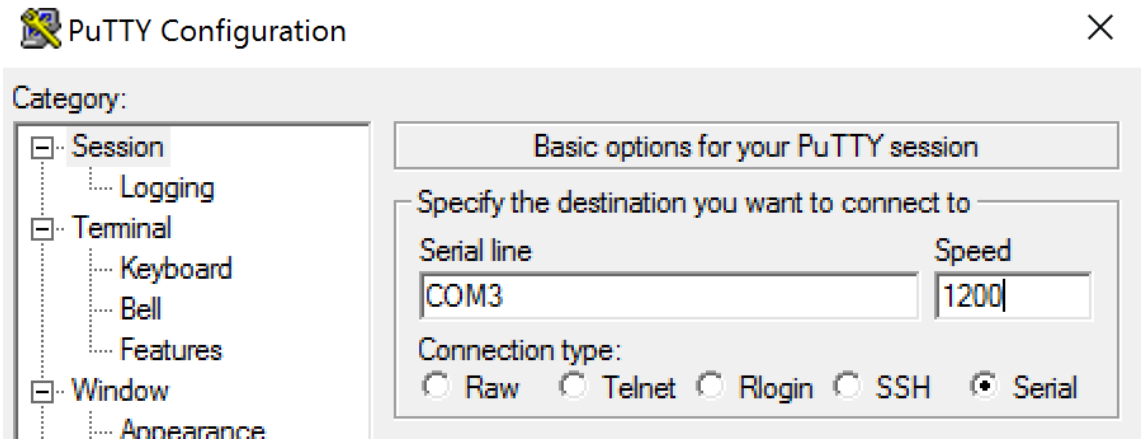

   Sie finden diese Informationen auch durch Ausführen von chgport **/query** an der Eingabeaufforderung.




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.

## Spezialtastaturen

June 27, 2024

### Bloomberg-Tastaturen

> **Warnung:**
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übern-

> immt 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.

Citrix Virtual Apps and Desktops unterstützt die Bloomberg-Tastatur 5 und 4 (Starboard) und das ältere Modell 3. Mithilfe der Spezialfunktionen dieser Tastatur können Benutzer im Finanzsektor schnell auf Finanzmarktdaten zugreifen und handeln.

> **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 umfasst als USB-Verbundgerät mehrere 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 2207 für Linux zur Unterstützung des Bloomberg-Tastaturmodells 5.
- Mindestens Citrix Workspace App 2109 für Windows zur Unterstützung des Bloomberg-Tastaturmodells 5.
- 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.

Informationen zum Aktivieren der Bloomberg-Tastaturunterstützung finden Sie unter Bloomberg-Tastaturen in der Liste der über die Registrierung verwalteten Features.

**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:

Für Bloomberg-Tastatur 5:

- Bloomberg LP Bloomberg Biometric Module
- Bloomberg LP Keyboard (Verbundgerät mit zwei Schnittstellen)
- Bloomberg LP Keyboard Audio (Verbundgerät mit drei Schnittstellen)

Für Bloomberg-Tastaturen 3 und 4:

- 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.

## Webcams

June 27, 2024

### 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.

Sie können das Feature über einen Registrierungsschlüssel aktivieren und deaktivieren und dann eine spezifische Auflösung konfigurieren. Weitere Informationen finden Sie unter HD-Webcamstreaming und HD-Webcamauflösung in der Liste der Features, die über die Registrierung verwaltet werden.

## Grafik

June 27, 2024

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 Host-

computer (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.

### Textbasierte 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.

### Angepasste Aktualisierungsrate

Mit den neuen Skalierbarkeitsverbesserungen passt HDX die Aktualisierungsrate virtueller Monitore an die festgelegte FPS-Zielrichtlinie an. Adaptive Refresh Rate (ARR) ist sowohl für Einzel- als auch für Multisession-VDAs verfügbar und funktioniert sowohl für GPU-beschleunigte als auch für Nicht-GPU-Szenarien.

### Verlusttoleranzmodus

Der Verlusttoleranzmodus wurde gründlich überarbeitet, um sicherzustellen, dass die Sitzung interaktiv bleibt, wenn ein Paketverlust erkannt wird.

### Verwandte Informationen

- HDX 3D Pro
- GPU-Beschleunigung für Windows-Einzelsitzungs-OS
- GPU-Beschleunigung für Windows-Multisitzungs-OS
- Framehawk
- Thinwire
- Textbasierte Sitzungswasserzeichen

## 10-Bit High Dynamic Range (HDR)

June 27, 2024

Mit 10-Bit HDR-Sitzungen für virtuelle Desktops können Sie erweiterte Codierungs- und Decodierungsfunktionen für das Rendern hochwertiger Bilder und Videos mit einem erweiterten Farbbereich sowie größerem Kontrast und größerer Helligkeit nutzen. Außerdem können Sie die Weißleuchtdichte, EDID (Extended Display Identification Data) und die visuelle Qualität anpassen, um die Benutzererfahrung zu verbessern.

### Systemanforderungen

Endpunkt

- Citrix Workspace-App für Windows 2209 oder höher für NVIDIA GPUs
- NVIDIA-GPUs mit Unterstützung für 10-Bit-HEVC-(H.265)-444-Decodierung auf dem Endpunkt
- 10-Bit-HDR-unterstützte Monitore, 10-Bit-HDR muss über die Anzeigeeinstellungen auf allen Monitoren aktiviert sein.

Server:

- Windows-Einzelsitzungs-OS VDA 2209 oder höher für NVIDIA-GPUs und VDA 2308 oder höher für Intel-GPUs
- NVIDIA-GPUs mit Unterstützung für 10-Bit-HEVC 444-Codierung auf dem Endpunkt

## Erforderliche Richtlinien

Endpunkt

- H.265-Decodierung für Grafiken aktivieren

Server:

- Optimierung für 3D-Grafikworkload
- Grafikstatusanzeige (optional)

## Serverkonfigurationen

Wenn Sie eine Citrix-Sitzung auf einem 10-Bit-HDR-fähigen Endpunktmonitor starten, wird die HDR-Sitzung standardmäßig aktiviert. In HDR-Sitzungen mit mehreren Monitoren muss auf allen Endpunktmonitoren 10-Bit-HDR aktiviert sein. HDR-Sitzungen werden sowohl im Fenster- als auch im Vollbildmodus unterstützt.

### Referenzweißwert

Diese Einstellung definiert die weiße Leuchtdichte anhand des Nit-Werts. Der Wert steuert die relative HDR-Bildschirmhelligkeit innerhalb der Sitzung. Der Standardwert ist 80 Nits. Legen Sie den folgenden Registrierungsschlüssel fest, um einen anderen Nit-Wert zu definieren:

- HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics
- Typ: REG_DWORD
- Name: RefWhiteLevel

Um die Einstellung zu aktivieren, müssen Sie entweder die Größe Ihrer Sitzung ändern oder die Sitzung trennen und neu starten.

### EDID überschreiben

Sie können den VDA so konfigurieren, dass er die EDID des Endpunktmonitors für Ihre HDR-Sitzungen verwendet. Auf diese Weise können Sie die Anzeigefunktionen des Monitors voll ausnutzen, indem Sie die Farbskala und den Leuchtdichtenbereich anpassen. Standardmäßig wird für HDR-Sitzungen ein HDR1000-fähiges Display vorausgesetzt.
Sie können die Endpunktmonitor-EDID mit NVIDIA oder anderen Tools exportieren. Wenden Sie den Wert mit dem folgenden Registrierungsschlüssel auf den VDA an:

- HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics
- Typ: REG_BINARY

- Name: EDIDOverride

Wenn Sie die EDID in der Registrierung speichern, darf sie keine Kommas, Leerzeichen oder Sonderzeichen enthalten. Um die EDID außer Kraft zu setzen, melden Sie sich ab und starten Sie eine neue Sitzung.

#### Visuell verlustfreies Erlebnis

Aktivieren Sie die folgenden Richtlinien für ein visuell verlustfreies Erlebnis:

- Visuell verlustfreie Komprimierung zulassen
- Bildqualität: "Immer verlustfrei"oder "Zu verlustfrei verbessern"

Nachdem die Richtlinien festgelegt wurden, können Sie die HDR-Sitzungsqualität über die Grafikstatusanzeige steuern, indem Sie den Schieberegler für die Bildqualität verwenden oder in den pixelgenauen Modus wechseln.

#### Windows-Bildschirmsperre zulassen

Mit dieser Richtlinie können Sie zulassen, dass alle Windows-Anzeigetimeouts, einschließlich der Bildschirmsperre, für eine Citrix Virtual Desktop-Sitzung auf Workstation OS gelten. Diese Einstellung kann mit einem Citrix Gruppenrichtlinienobjekt in Citrix Studio festgelegt werden.

Wenn diese Einstellung nicht aktiviert ist, reagiert ein Citrix Virtual Desktop standardmäßig nicht auf Timeouts für Sitzungssperre, Bildschirmschoner oder Display Off während einer aktiven Sitzung.

Wenn ein kennwortgeschützter Bildschirmschoner auf einem Workstation-VDA konfiguriert ist, muss diese Einstellung aktiviert sein, damit die Citrix Virtual Desktop-Sitzung automatisch gesperrt wird, sobald das Bildschirmschoner-Timeout erreicht wurde.

Wenn Sie diese Einstellung aktivieren und auf dem VDA ein Display-Off-Timeout konfiguriert ist, führt der Ablauf dieses Timeouts zu einer Sitzung, die erst aktualisiert wird, wenn der Benutzer die Interaktion mit der Sitzung wieder aufnimmt. Beispielsweise wird jede angezeigte Uhrzeit nicht aktualisiert und neue Benachrichtigungen werden nicht angezeigt.

#### Andere Überlegungen

- Auf virtuellen GPUs können Sie 10-Bit-HDR-Sitzungen auf bis zu vier Monitoren starten.
- Die Citrix-Sitzung wird in den folgenden Fällen auf den 8-Bit-Nicht-HDR-Modus zurückgesetzt:
  - Auf einem der Endpunktmonitore ist 10-Bit-HDR nicht aktiviert
  - Bildschirmfreigabe aktivieren.
  - Virtuelles Anzeigelayout auf dem VDA einstellen.

- In den pixelgenauen Modus wechseln, ohne die Richtlinie **Visuell verlustfreie Komprimierung zulassen** festzulegen.

## HDX 3D Pro

June 27, 2024

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.

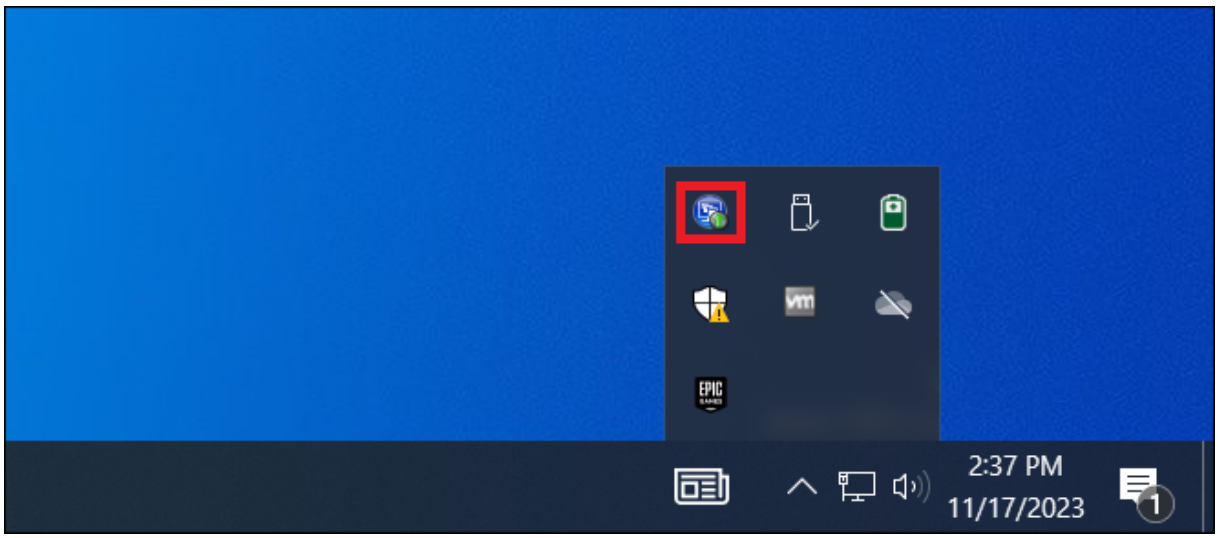
 

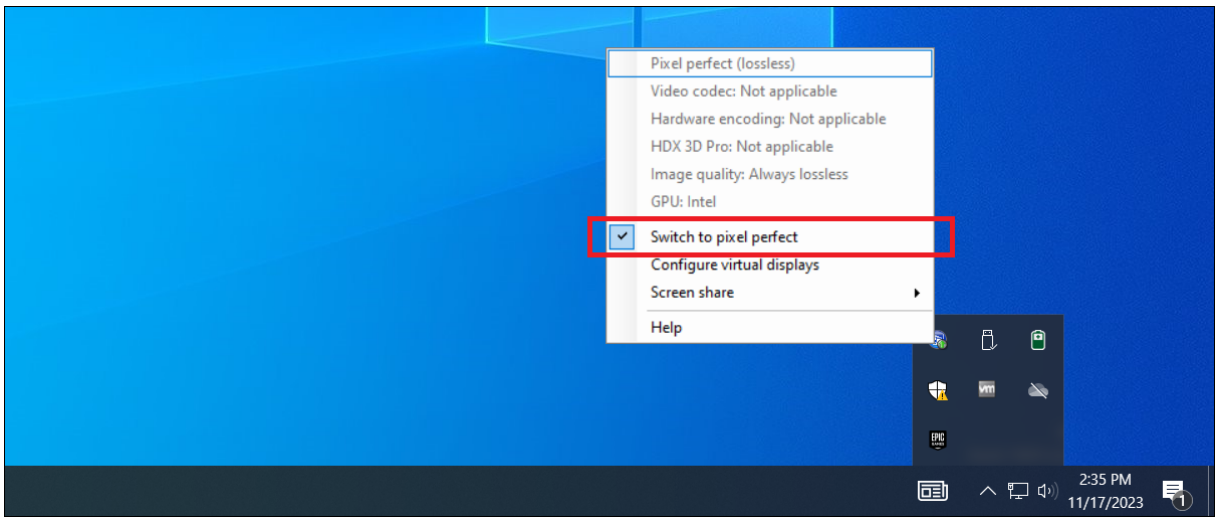
### Verlustfreie Komprimierung für besondere Anwendungsfälle

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 in der Grafikstatusanzeige 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 Modus **Immer verlustfrei** wechseln. Zum Aktivieren von **Verlustfrei** in einer Sitzung

klicken Sie mit der rechten Maustaste auf das Symbol und dann auf **Zu pixelgenau wechseln** 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 für die Konfiguration 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:
  Für F10 setzen Sie K=0x79
  Für Strg + F10 setzen Sie C=1, K=0x79
  Für Alt + A setzen Sie A=1, K=a or A=1, K=A or K=A, A=1
  Für Strg + Alt + 5 setzen Sie C=1, A=1, K=5 oder A=1, K=5, C=1
  Für Strg + Umschaltt + F5 setzen Sie A=1, S=1, K=0x74

### Optimierung der HDX 3D Pro-Benutzererfahrung

Wenn mehrere Benutzer eine Verbindung mit beschränkter Bandbreite gemeinsam verwenden, z. B. in einer Zweigstelle, empfiehlt Citrix, die Richtlinieneinstellung Bandbreitenlimit für Sitzung insgesamt zu verwenden, um die für die einzelnen Benutzer verfügbare Bandbreite zu beschränken.

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 vergewissern Sie sich, 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.
Mit dem HDX Monitor können Sie den Betrieb und die Konfiguration von HDX-Visualisierungstechnologien überprüfen und HDX-Probleme diagnostizieren und beheben. Das Tool ist im Ordner **Support** auf dem Citrix Virtual Apps and Desktops-Installationsmedium verfügbar.

## GPU-Beschleunigung für Windows-Multisitzungs-OS

June 27, 2024

Citrix Virtual Apps and Desktops unterstützen grafikintensive Anwendungen, die in Windows-Multisitzungs-OS-Sitzungen ausgeführt und auf dem Grafikprozessor (GPU) des Servers gerendert werden. Beim Verlagern von OpenGL-, DirectX-, Direct3D- und Windows Presentation Foundation-(WPF)-Rendering auf die GPU des Servers kann die CPU des Servers effizienter genutzt werden.

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. Erstellen 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 XenServer 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:

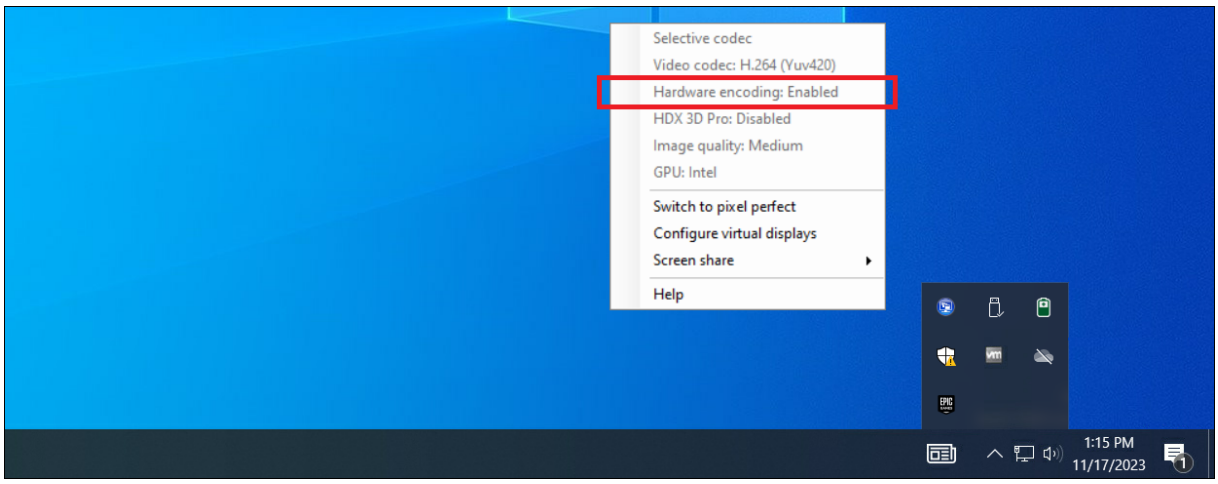
- Ausgeführte Anwendungen
- Verbrauchter Videospeicher
- Verarbeitungsleistung der Grafikkarte

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.

- 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".

Um zu bestätigen, dass die GPU-Beschleunigung stattfindet, kann die Grafikstatusanzeige verwendet werden:




### 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 2016 und später verwenden Remotedesktopdienste-Sitzungen auf dem RD-Sitzungshostserver als Standardadapter den Microsoft Basic Render-Treiber. Um die GPU in RDS-Sitzungen unter Windows Server 2016 und später 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 WPF-Anwendungen mithilfe der Server-GPU zu rendern, erstellen Sie die Einstellungen in der Registrierung des Servers, der die Sitzungen mit Windows-Multisitzungs-OS ausführt. Weitere Informationen zur Registrierungseinstellung finden Sie unter Rendering mit Windows Presentation Foundation (WPF) in der Liste der über die Registrierung verwalteten Features.

### 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 Registrierungseinstellungen, um die verfügbaren CUDA-Beschleunigungsfeatures zu verwenden. Weitere Informationen finden Sie unter GPU-Beschleunigung für CUDA- oder OpenCL-Anwendungen in der Liste der über die Registrierung verwalteten Features.

# GPU-Beschleunigung für Windows-Einzelsitzungs-OS

June 27, 2024

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, Nutanix und Hyper-V (nur Passthrough).

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.

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

- Unterstützung für mehrere Monitore und hochauflösende Monitore. Für Maschinen mit Einzelsitzungs-OS werden bis zu 8 4K-Monitore unterstützt. 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.
- 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.
- Unterstützung von Microsoft HyperV mit Discrete Device Assignment in Windows Server 2016:
- Unterstützung von Datencenter-Grafikplattformen der Serie Intel Xeon Processor E3 und Intel Data Center GPU Flex-Serie. Weitere Informationen finden Sie unter https://www.intel.com/content/www/us/en/products/details/discrete-gpus/data-center-gpu/flex-series.html.
- Unterstützung für AMD-GPUs.

> Hinweis:
>
> 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 https://www.amd.com/en/graphics/workstation-virtual-graphics.

- Zugriff auf einen leistungsstarken Videocodierer für NVIDIA-GPUs, AMD-GPUs und Intel-GPUs. Das Feature wird durch eine standardmäßig aktivierte Richtlinieneinstellung gesteuert. Das Feature ermöglicht die Verwendung der H.264-, H.265- oder AV1-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".

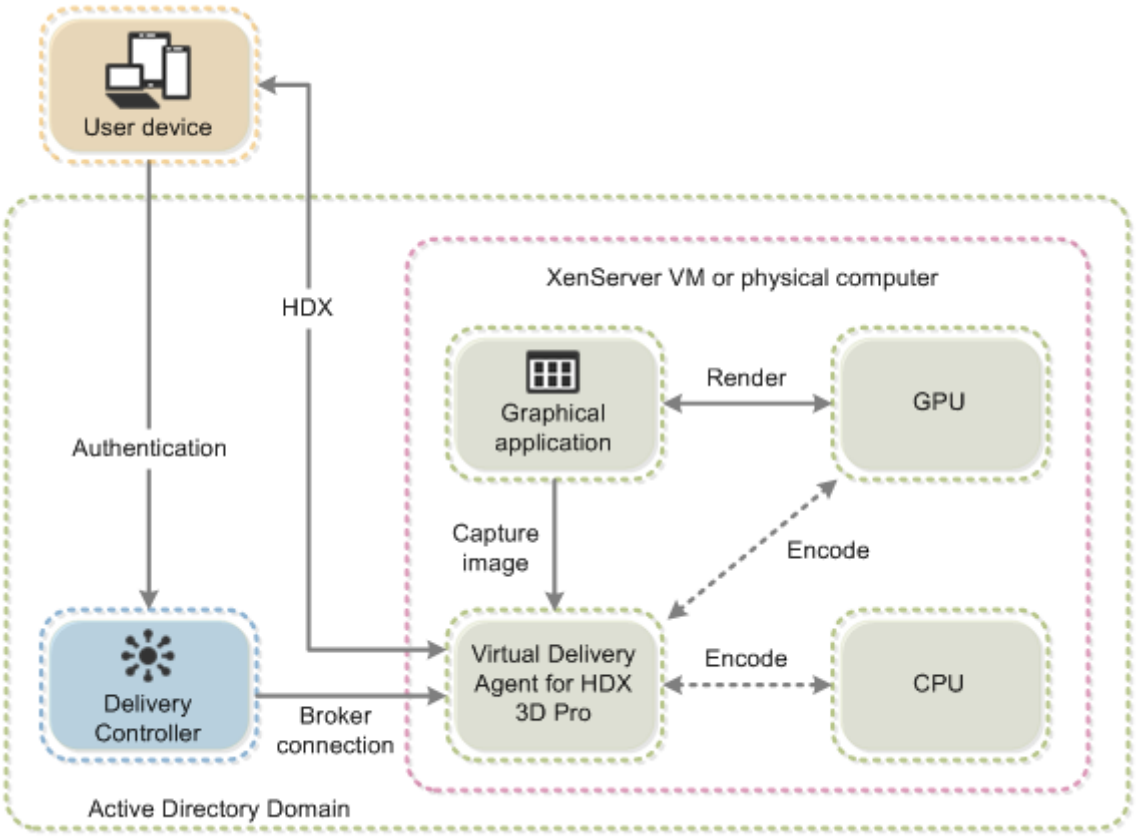
Wie in der folgenden Abbildung dargestellt:

- 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

Wenn mehrere Benutzer eine Verbindung mit beschränkter Bandbreite gemeinsam verwenden, z. B. in einer Zweigstelle, empfiehlt Citrix, die Richtlinieneinstellung **Bandbreitenlimit für Sitzung insgesamt** zu verwenden, um die für die einzelnen Benutzer verfügbare Bandbreite zu beschränken. 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 vergewissern Sie sich, 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.

### Verlustfreie Komprimierung

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 klicken Sie mit der rechten Maustaste auf das Symbol und dann auf **Zu pixelgenau wechseln** 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.

### Tastenkombination für Verlustfreiheit

Sie können jederzeit innerhalb einer Sitzung die Standardtastenkombination **ALT+SHIFT+1** verwenden, um **Verlustfrei** auszuwählen oder zu deaktivieren.

Sie können die Standardtastenkombination **ALT+SHIFT+1** in der Windows-Registrierung überschreiben.
Zum Konfigurieren einer neuen Registrierungseinstellung legen Sie die folgenden Registrierungswerte fest:

- **Schlüssel**:`HKEY_CURRENT_USER\SOFTWARE\Citrix\Graphics`
- **Name**:`HKLM_HotKey`
- **Typ**: `String`

Das Format für die Konfiguration einer Tastenkombination ist `C=0|1, A=0|1, S=0|1, W=0|1, K=val`. Schlüssel müssen durch ein Komma “,”ohne Leerzeichen getrennt werden. Die Reihenfolge der Tasten ist egal.

A, C, S, W und K sind Tasten, wobei C=Control, A=ALT, S=UMSCHALTTASTE, W=Win und K=eine gültige Taste sind und die zulässigen Werte für K 0—9, a—z und jeder virtuelle Tastencode sind.

Beispiel:

- Für **F10** setzen Sie K=0x79
- Für **Strg + F10** setzen Sie C=1,K=0x79
- Für **Alt + A** setzen Sie A=1,K=a oder A=1,K=A oder K=A,A=1
- Für **Strg + Alt + 5** setzen Sie C=1,A=1,K=5 oder A=1,K=5,C=1
- Für **Strg + Umschalt + F5** setzen Sie A=1,S=1,K=0x74

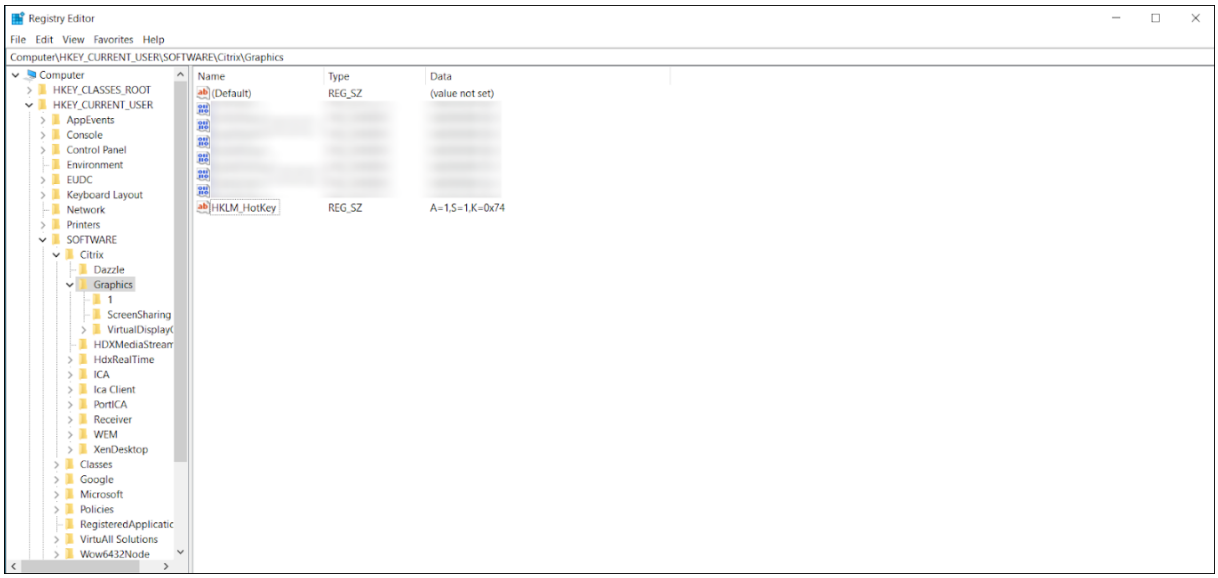
Die folgende Tabelle zeigt eine Beispielliste virtueller Tastencodes:

| Schlüssel | Wert |
|---|---|
| F1 | 0x70 |
| F2 | 0x71 |
| F3 | 0x72 |
| F4 | 0x73 |
| F5 | 0x74 |
| F6 | 0x75 |
| F7 | 0x76 |
| F8 | 0x77 |
| F9 | 0x78 |
| F10 | 0x79 |
| F11 | 0x7A |
| F12 | 0x7B |
| BILD-AUF-Taste | 0x21 |
| BILD-AB-Taste | 0x22 |
| ENDE-Taste | 0x23 |
| Pos1-Taste | 0x24 |
| Nach-Links-Taste | 0x25 |
| Nach-Oben-Taste | 0x26 |
| Nach-Rechts-Taste | 0x27 |
| Nach-Unten-Taste | 0x28 |

Vergewissern Sie sich, dass zwischen den Tastenkombinationen kein Leerzeichen steht. Beispiel:

Richtig:
C=1,K=0x74
Falsch:
C=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. Erstellen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

# Thinwire

June 28, 2024

## Einführung

Thinwire ist ein Teil der Citrix HDX-Technologie und die in Citrix Virtual Apps and Desktops verwendete Standardtechnologie 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 liefert eine hochgradig interaktive Benutzererfahrung –ähnlich wie bei einem lokalen Computer. Bei Thinwire wird dies mit komplexen und effizienten Bildanalyse- und Komprimierungsmethoden erzielt. Thinwire maximiert die Serverskalierbarkeit und verbraucht weniger Bandbreite als 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.

### HDX 3D Pro

In der Standardkonfiguration kann Thinwire 3D- oder hoch interaktive Grafik liefern und, falls vorhanden, eine Grafikprozesseinheit (GPU) verwenden. Citrix empfiehlt jedoch die Aktivierung des HDX 3D Pro-Modus über die Richtlinien **Optimierung für 3D-Grafikworkload** oder **Bildqualität > Zu verlustfrei verbessern** für Szenarien, in denen GPUs vorhanden sind. Diese Richtlinien konfigurieren Thinwire für die Verwendung eines Videocodecs (H.264, H.265 oder AV1) zur Codierung des gesamten Bildschirms mithilfe der Hardwarebeschleunigung, wenn eine GPU vorhanden ist. Dies bietet eine flüssigere Anzeige professioneller 3D-Grafiken. Weitere Informationen finden Sie unter H.264 –Zu verlustfrei verbessern, HDX 3D Pro und GPU-Beschleunigung für Windows-Einzelsitzungs-OS.

### Anforderungen

Thinwire ist optimiert für moderne Betriebssysteme, einschließlich Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows 10 und Windows 7. Für Windows Server 2008 R2 wird der Legacy-Grafikmodus empfohlen. Verwenden Sie die integrierten Citrix Richtlinienvorlagen "Hohe Serverskalierbarkeit –Legacy-OS"und "Für WAN optimiert –Legacy-OS"zum Bereitstellen der von Citrix für solche Anwendungsfälle empfohlenen Kombinationen von Richtlinieneinstellungen.

- Die Richtlinieneinstellung, die das Verhalten von Thinwire steuert (**Videocodec zur Komprimierung verwenden**), ist in VDA-Versionen in 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 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 evtl. die Anzeigequalität gemindert, insbesondere bei einer 8-Bit-Farbtiefe.

### Codierungsmethoden

Thinwire kann je nach Richtlinie und Clientkapazität in zwei Codierungsmodi ausgeführt werden:

- Thinwire mit Adaptive JPEG
  **Videocodec zur Komprimierung verwenden** Richtlinieneinstellung: **Videocodec nicht verwenden**
- Thinwire mit selektivem H.264, H.265 oder AV1
  **Videocodec für Komprimierung verwenden** Richtlinieneinstellung: **Videocodec verwenden, wenn bevorzugt** oder **Für aktive Änderungsbereiche**
- Thinwire mit Vollbild-H.264, -H.265 oder -AV1
  **Videocodec für Komprimierung verwenden** Richtlinieneinstellung: **Für den gesamten Bildschirm**

### H.265

High Efficiency Video Coding (HEVC), auch bekannt als H.265, ist der Nachfolger von H.264. Hardwarecodierung mit dem H.265-Videocodec wird auf den folgenden GPUs unterstützt:

- NVIDIA Maxwell-basierte GPUs und höher
- Intel-GPUs der 6. Generation und höher
- AMD Raven-basierte GPUs und höher

### AV1

Citrix hat Unterstützung für den AV1-Videocodec hinzugefügt. Der Vorteil von AV1 besteht darin, dass es im Vergleich zu H.264 und H.265 eine überlegene Bildkomprimierung, eine bessere Bildqualität und eine geringere Bandbreitennutzung bietet.

Die folgenden Anforderungen für AV1 müssen erfüllt sein:

- VDA 2305 oder höher für NVIDIA-GPUS oder
- VDA 2308 oder höher für Intel-GPUs

Die folgenden GPUs sind für die Codierung kompatibel:

- NVIDIA Ada Lovelace-basierte GPU
- GPUs der Flex-Serie von Intel ARC oder Intel Data Center GPU

Weitere Informationen zu den Ada Lovelace-GPUS von NVIDIA finden Sie unter ADA-Architektur.

Weitere Informationen zu den ARC-GPUs der Flex-Serie für Workstations und Datencenter von Intel finden Sie unter Flex-Serie und Überblick.

### Automatische Videocodecauswahl

Sie können automatisch den am besten geeigneten Videocodec ermitteln, wenn entweder die Richtlinie **Videocodec zur Komprimierung verwenden** oder "Optimierung für 3D-Grafikworkload" auf dem VDA aktiviert ist. Während der Installation der Citrix Workspace-App für Windows werden die Decodierungsfunktionen des Endpunkts evaluiert. Basierend auf diesen Informationen handelt die Citrix Workspace-App für Windows den besten Codec aus, der bei der Verbindung mit dem VDA verwendet werden soll. Die folgende Liste zeigt die Reihenfolge, in der die Videocodecs ausgewertet werden:

- AV1
- H.265
- H.264

Die automatische Auswahl gilt nur für 4:2:0 -Varianten dieser Codecs. Wenn die Einstellung **Bildqualität** auf "Zu verlustfrei verbessern"oder "Immer verlustfrei"gesetzt ist und "Visuell verlustfreie Komprimierung zulassen"auf "aktiviert"gesetzt ist, ist die automatische Auswahl des Videocodecs deaktiviert.

Beim Herstellen einer Verbindung zu einer Ressource testet die Citrix Workspace-App die Fähigkeit des Endpunkts, H.265 und AV1 zu dekodieren und die Funktionen in der Registrierung zu speichern. Die Citrix Workspace-App wählt dann automatisch den besten zu verwendenden Videocodec aus und handelt diesen mit dem VDA aus. Wenn sowohl der VDA als auch der Client H.265 und AV1 verwenden können, wird AV1 als Videocodec ausgewählt. Wenn AV1 weder auf dem VDA noch auf dem Client verfügbar ist, wird H.265 ausgehandelt. Wenn H.265 auch auf keinem von beiden verfügbar ist, verwendet die Sitzung H.264 als Videocodec.

> **Hinweis:**
>
> Dieses Feature ist standardmäßig aktiviert. Dieses Verhalten kann geändert werden, indem die neue clientseitige Registrierungseinstellung `DisableDecoderCaps` festgelegt wird.

Um die automatische Auswahl des Videocodecs zu deaktivieren, setzen Sie 'DisableDecoderCaps'auf `HKLM\Software\WOW6432Node\Policies\Citrix\ICA Client\Graphics Engine`

`DWORD DisableDecoderCaps = 1` oder `HKCU\Software\Policies\Citrix\ICA Client\Graphics Engine DWORD DisableDecoderCaps = 1`.

Wenn einer dieser Werte auf 1 gesetzt ist, wird die automatische Auswahl des Videocodecs nicht verwendet.
Die Grafikstatusanzeige und der HDX-Monitor können den Videocodec überwachen.

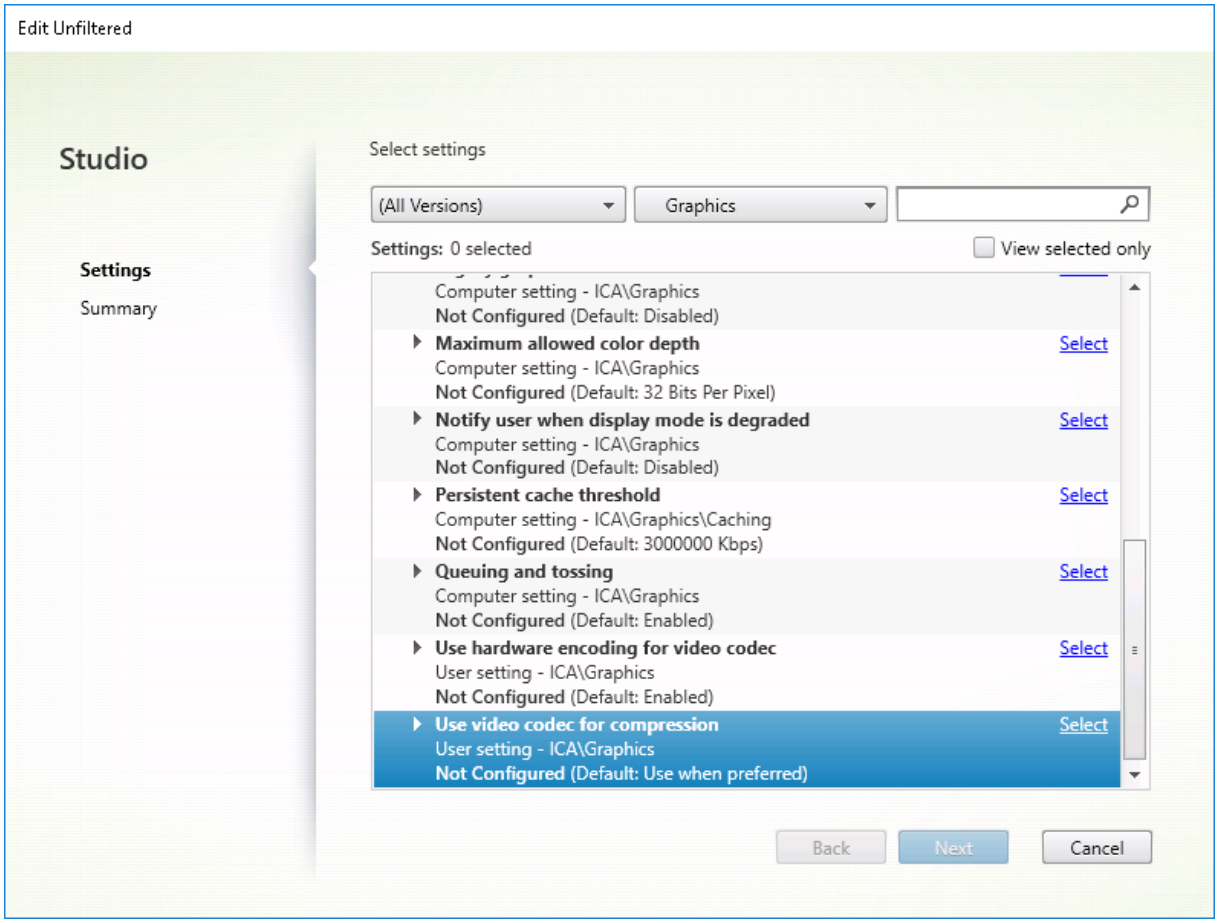
### Konfiguration

Thinwire ist die Standardtechnologie für das Anzeigeremoting.

Die folgende Grafikrichtlinieneinstellung dient zum Festlegen der Standardeinstellung und zur Bereitstellung von Alternativen für verschiedene Anwendungsfälle:

- Videocodec zur Komprimierung verwenden
  - **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. Dies ist funktional gleichwertig mit **Für aktive Änderungsbereiche**.
- Von anderen Optionen in dieser Richtlinieneinstellung wird Thinwire auch verwendet und zwar mit anderen Technologien für verschiedene Anwendungsfälle. Beispiel:
  - **Für aktive Änderungsbereiche**. Die Technologie für die adaptive Anzeige von Thinwire identifiziert bewegliche Bilder (Video, 3D In Motion) und verwendet H.264, H.265 oder AV1 nur in dem Bildschirmbereich, in dem das Bild sich bewegt.
  - **Für den gesamten Bildschirm**. Thinwire wird mit Vollbild-H.264, -H.265 oder -AV1 zur Optimierung der Benutzererfahrung und Bandbreite bei intensiver 3D-Grafiknutzung verwendet. Bei H.264 4:2:0 (Richtlinie **Visuell verlustfrei** deaktiviert) ist das endgültige Bild nicht pixelgenau (verlustfrei) und für bestimmte Szenarien möglicherweise nicht geeignet. In solchen Fällen müssem Sie stattdessen H.264 "Zu verlustfrei verbessern"oder H.265 "Zu verlustfrei verbessern"verwenden.




Diverse weitere Richtlinieneinstellungen, einschließlich der nachfolgend aufgeführten Einstellungen der Richtlinie "Visuelle Anzeige", können zur Optimierung der Anzeigeremoting-Leistung verwendet werden: Thinwire unterstützt sie alle.

- 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 Thinwire mit der optimalen Kombination von Richtlinieneinstellungen für die Prioritäten Ihres Unternehmens und den Erwartungen Ihrer Benutzer.

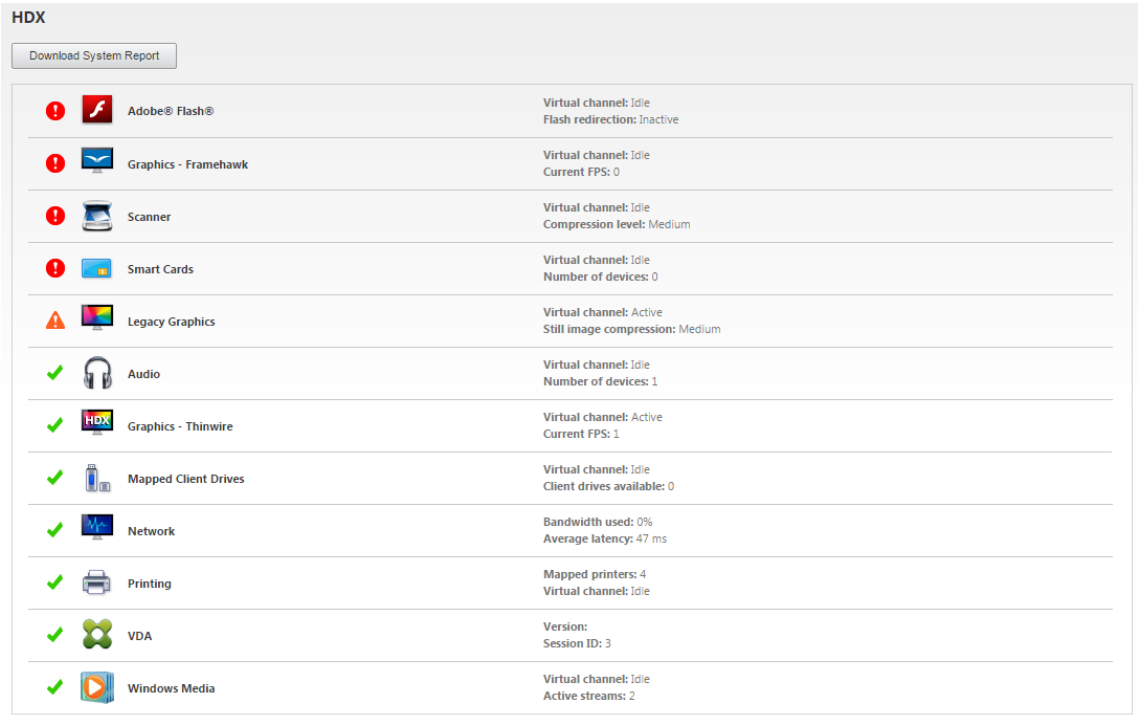
### Überwachen von Thinwire

Sie können die Verwendung und Leistung von Thinwire über Citrix Director überwachen. Die Detailansicht für den virtuellen HDX-Kanal enthält nützliche Informationen zur Überwachung und Problembe-

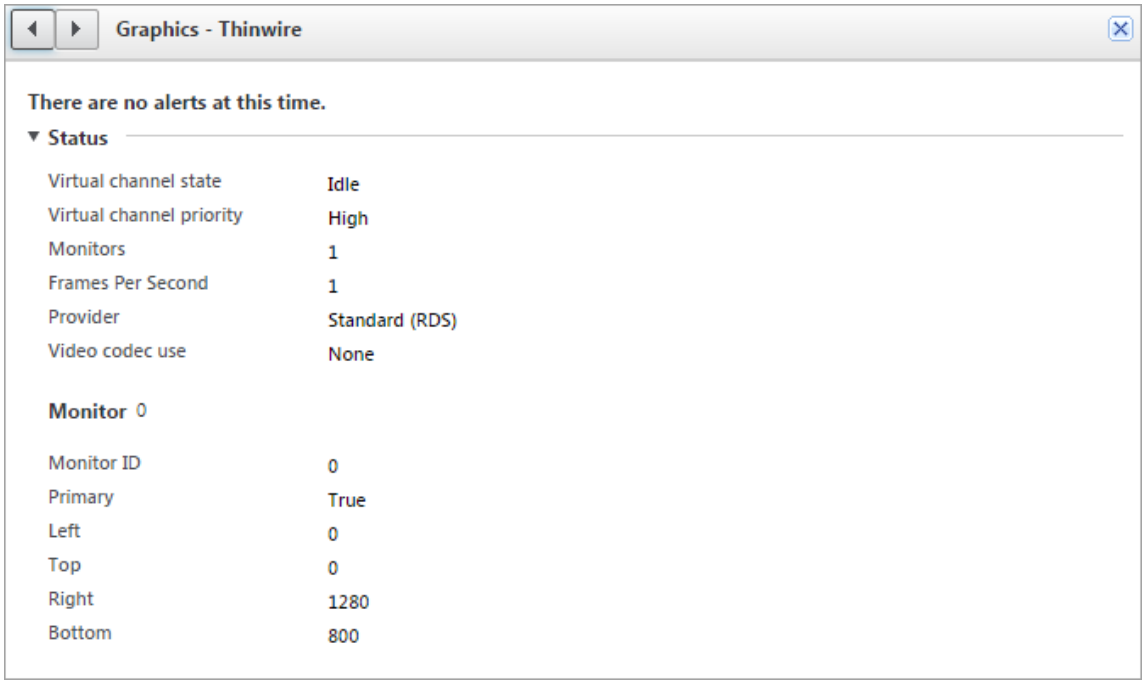
handlung von Thinwire in jeder Sitzung. Gehen Sie zum Anzeigen für Thinwire relevanter Kennzahlen folgendermaßen vor:

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**.




### Verlustfreier Komprimierungscodec (MDRLE)

In einer normalen Desktopsitzung sind die meisten Bilder einfache Grafiken oder Textbereiche. Thinwire sucht diese Regionen und wählt sie 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.

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. Der neue Codec hat keine Auswirkungen auf die Serverskalierbarkeit.

Weniger Bandbreite resultiert in der Regel in einer besseren Sitzungsinteraktivität (insbesondere bei gemeinsam genutzten oder eingeschränkten Verbindungen) und geringeren Kosten.

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

In Citrix Virtual Apps and Desktops 1808 wurde der progressive Modus eingeführt. Er ist standardmäßig aktiviert. Unter eingeschränkten Netzwerkbedingungen (Standard: Bandbreite < 2 Mbps oder Latenz > 200 ms) wurde von Thinwire zur Verbesserung der Interaktivität bei Bildschirmaktivitäten die Komprimierung von Text und statischen Bildern erhöht. Stark komprimierter Text und Bilder werden dann schrittweise in zufälligen Blöcken geschärft, wenn die Bildschirmaktivität beendet wurde. Dieses Verfahren des Komprimierens und Schärfens verbessert zwar die Interaktivität, es reduziert jedoch die Cache-Effizienz und erhöht die Bandbreitennutzung.

Ab Citrix Virtual Apps and Desktops 1906 wurde der progressive Modus standardmäßig deaktiviert. Es kommt nun ein anderes Verfahren zum Einsatz. Die Qualität von Standbildern verbleibt dynamisch basierend auf den Netzwerkbedingungen zwischen einem vordefinierten Mindest- und Maximalwert für jede Einstellung der **visuellen Qualität**. Da es keinen Schärfungsschritt gibt, optimiert Thinwire die Bildbereitstellung unter Beibehaltung der Cache-Effizienz und bietet zugleich nahezu alle Vorteile des progressiven Modus.

#### Ändern des Verhaltens des progressiven Modus

Sie können den Zustand des progressiven Modus über den Registrierungsschlüssel ändern. Weitere Informationen finden Sie unter Progressiver Modus in der Liste der über die Registrierung verwalteten Features.

### Zu verlustfrei verbessern

**Zu verlustfrei verbessern** ist eine spezielle Thinwire-Konfiguration, die die Grafikbereitstellung für Interaktivität und endgültige Bildqualität optimiert. Sie können diese Einstellung aktivieren, indem Sie die Richtlinie **Visuelle Qualität** auf **Zu verlustfrei verbessern** festlegen.

“Zu verlustfrei verbessern”komprimiert die Anzeige mit H.264, H.265 oder AV1 bei Bildschirmaktivität und schärft auf pixelgenau (verlustfrei), wenn die Aktivität beendet wird. Die verlustbehaftete Bildqualität wird zur Erhaltung der bestmöglichen Framerate den verfügbaren Ressourcen angepasst. Das Schärfen wird schrittweise durchgeführt. Ein Beispiel wäre die Auswahl eines Modells und dessen Drehen.

**Zu verlustfrei verbessern**bietet alle Vorteile der Verwendung eines Videocodecs für den gesamten Bildschirm, einschließlich Hardwarebeschleunigung, aber mit dem zusätzlichen Vorteil eines endgültigen, garantiert verlustfreien Bildschirms. Dies ist extrem wichtig für 3D-Arbeiten, die ein pixelgenaues Endbild erfordern. Beispiel wäre die Arbeit mit medizinischen Bildern. Außerdem verbraucht H.264 **Zu verlustfrei verbessern** weniger Ressourcen als Vollbild-H.264 mit 4:4:4. **Zu**

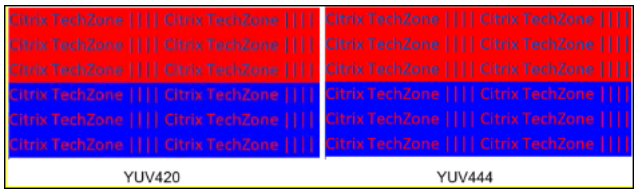
**verlustfrei verbessern** erzielt in der Regel eine höhere Framerate als visuell verlustfreies H.264 mit 4:4:4.

> **Hinweis:**
>
> Sie können bei "Zu verlustfrei verbessern"das Verwenden eines Videocodecs deaktivieren. Stellen Sie einfach die Richtlinie **Videocodec verwenden** auf `Do not use video codec`. Dies führt dazu, dass bewegte Bilder stattdessen mit adaptivem JPEG kodiert werden.

### Visuell verlustfreie Codierung

Bei der visuell verlustfreien Codierung wird der YUV 4:4:4-Farbraum anstelle des Chroma-Subsampling-Farbraums YUV 4:2:0 für die Videocodeckomprimierung verwendet. Dadurch wird sichergestellt, dass bei der Farbraumkonvertierung keine Farbinformationen verloren gehen und nach der Decodierung vom ursprünglichen RGB-Bild visuell nicht wahrnehmbar sind.

Betrachten Sie das folgende Beispiel. Wenn Sie einen Videocodec verwenden, um den gesamten Bildschirm zu komprimieren, kann die 4:2:0 -Farbkomprimierung kontrastreiche Details wie Text verschlechtern, wodurch sie unscharf und schwerer lesbar werden. Im Gegensatz dazu bewahrt 4:4:4 fast die gesamte Farbinformation und zeigt keine visuell wahrnehmbare Verschlechterung.




Workloads, die eine pixelgenaue Qualität oder eine genaue Farbdarstellung erfordern, können von der visuell verlustfreien Codierung profitieren.

Visuell verlustfreie Codierung ist sowohl mit H.264 als auch mit H.265 verfügbar. Die H.264 4:4:4-Codierung ist eine rein softwarebasierte Lösung. Daher kann es erhebliche Auswirkungen auf die CPU-Auslastung sowohl auf dem VDA als auch auf dem Client geben. Dies kann sich auch auf die Framerate auswirken.

H.265 4:4:4-Unterstützung wurde mit der Veröffentlichung der Citrix Workspace-App 2305 hinzugefügt, sodass Thinwire sowohl eine GPU auf dem VDA als auch einen Client für die H.265 4:4:4-Codierung verwenden kann, was die Leistung erheblich verbessert.

Um die visuell verlustfreie 4:4:4-Codierung zu ermöglichen, müssen zwei Richtlinien aktiviert werden:

- **Bildqualität**: Auf `Build to Lossless` oder `Always Lossless` gesetzt
- **Visuell verlustfreie Komprimierung zulassen**: Auf `Enabled` gesetzt

> **Hinweis:**
>
> Wenn **Visuell verlustfreie Komprimierung zulassen** nicht aktiviert ist, wechseln Sie zu Ihrem Thinwire-Codierer in `Build to lossless` oder `Always Lossless`.

H.265 4:4:4 visuell verlustfrei hat folgende zusätzlichen Anforderungen:

- NVIDIA-GPUs benötigen VDA-Version 2209 oder höher
- Intel-GPUs benötigen VDA-Version 2308 oder höher

Die folgenden GPUs werden für H.265 4:4:4 unterstützt:

- NVIDIA-GPUs der Pascal-Generation und höher
- Intel-GPUs der 10. Generation und höher

Für den Client ist die Version 2305 der Citrix Workspace-App für Windows erforderlich (Version 2309.1 wird empfohlen).

Die Hardwaredecodierung von H.265 4:4:4 ist mit den folgenden Clientgeräte-GPUs möglich:

- NVIDIA-GPUs der Turing-Generation und höher
- Intel-GPUS der 10. Generation und höher

## Textbasierte Sitzungswasserzeichen

June 27, 2024

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**.
- Das Sitzungswasserzeichen unterstützt nur den Thinwire-Grafikmodus.
- 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.

## Bildschirmfreigabe

June 27, 2024

Mit der Bildschirmfreigabe können Benutzer eine Citrix Virtual Desktop-Sitzung (einschließlich Bildschirminhalt, Tastatur- und Maussteuerung) mit anderen Personen teilen.

### Systemanforderungen

- Windows: VDA mit Einzel- oder Multisitzungs-OS
- Linux: Weitere Informationen zur Freigabe von Linux-Sitzungen finden Sie in der Linux VDA-Dokumentation.
- Es können nur Desktopsitzungen freigegeben werden.
- Zwischen dem VDA, der als Sitzungshost agiert, und den Maschinen, die eine Verbindung zur freigegebenen Sitzung herstellen, muss Netzwerkkonnektivität bestehen. Die Anforderungen an den Netzwerkport basieren auf den verwendeten ICA-Ports (TCP/UDP 1494 oder 2598) und der Konfiguration der Richtlinie für die Bildschirmfreigabe (standardmäßig TCP 52525 bis 52625).

### Konfiguration

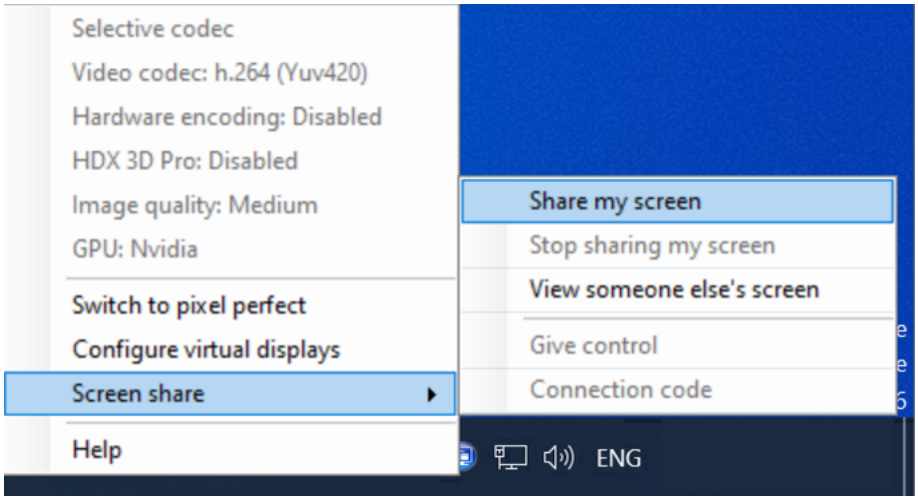
Die Bildschirmfreigabe muss mit Citrix Richtlinien aktiviert werden. Die Bildschirmfreigabe ist standardmäßig deaktiviert. Konfigurieren Sie die Richtlinie für die Bildschirmfreigabe, um das Feature zu aktivieren oder zu deaktivieren und den Bereich verwendbarer Netzwerkports zuzuweisen.

Aktivieren Sie die Richtlinie für die Grafikstatusanzeige, um die Benutzeroberfläche anzuzeigen, die Steuerelemente für die Freigabe und Verbindung mit Sitzungen enthält.

### Freigeben einer Sitzung

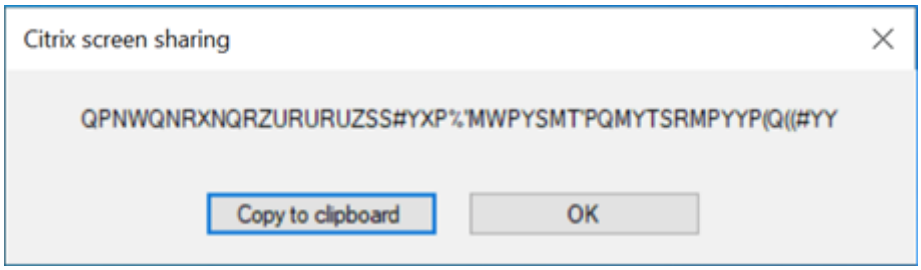
Zur Freigabe einer Sitzung suchen Sie im Windows-Infobereich das Symbol für die HDX-Grafikstatusanzeige. Klicken Sie mit der rechten Maustaste darauf und wählen Sie im angezeigten Menü **Bildschirmfreigabe > Meinen Bildschirm freigeben**.




Klicken Sie auf **In Zwischenablage kopieren** oder markieren und kopieren Sie die gesamte Zeichenfolge im Dialogfeld manuell. Die Zeichenfolge kann dann in die Anwendung Ihrer Wahl (z. B. einen E-Mail- oder IM-Client) eingefügt und an andere Benutzer verteilt werden.

Klicken Sie auf **OK** oder auf das **x**, um das Dialogfeld zu schließen. Während die Sitzung freigegeben ist, kann der Verbindungscode jederzeit über die Menüoption **Bildschirmfreigabe > Verbindungscode** abgerufen werden.

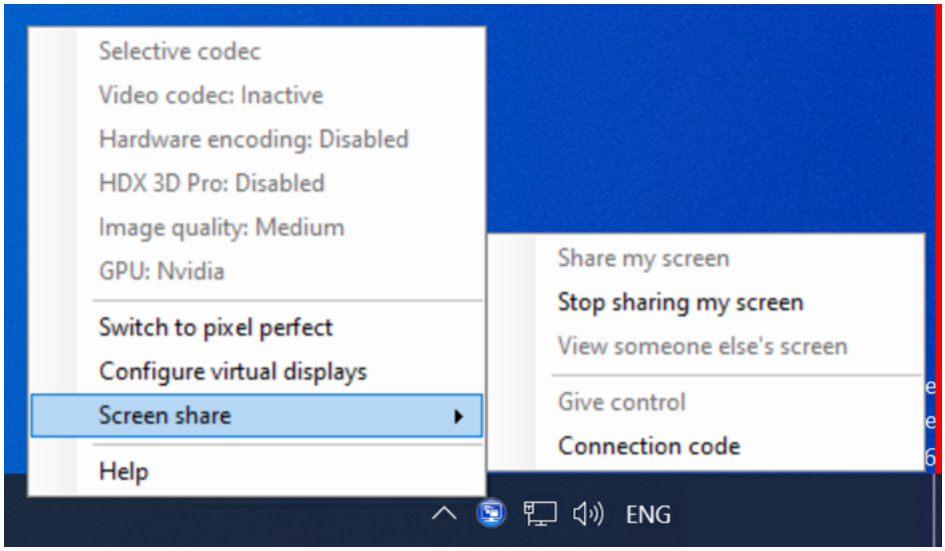



Der Bildschirm wird rot eingerahmt, um anzuzeigen, dass die Sitzung jetzt freigegeben und für andere sichtbar ist.

Tastatur- und Maussteuerung können über **Bildschirmfreigabe > Steuerung übergeben** mit anderen Benutzern geteilt werden.

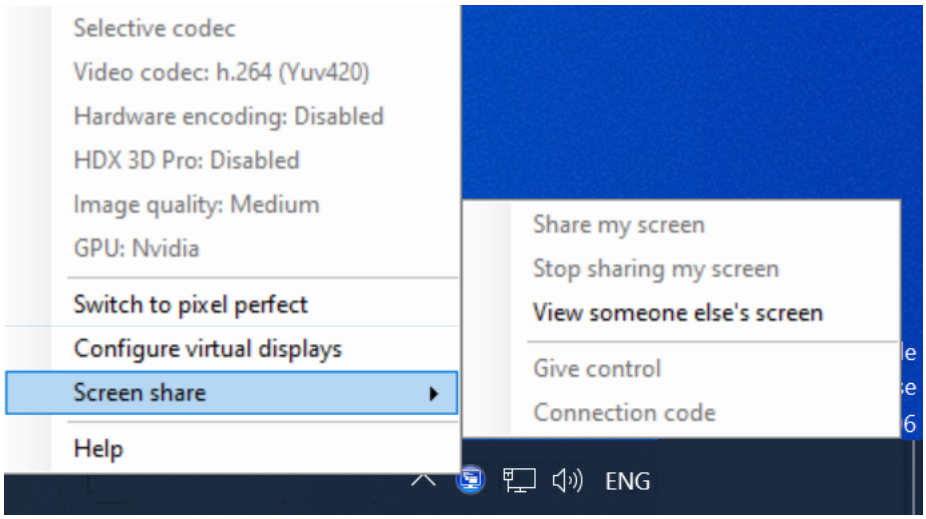
Verwenden Sie die Menüoption **Bildschirmfreigabe > Bildschirmfreigabe stoppen**, um die Sitzungsfreigabe zu beenden und alle Benutzer zu trennen.



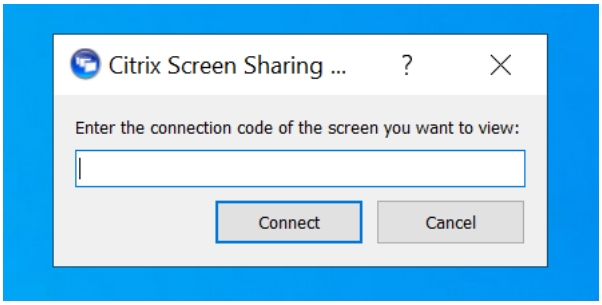

### Verbinden mit einer freigegebenen Sitzung

Um sich mit der Sitzung eines anderen Benutzers zu verbinden, suchen Sie im Windows-Infobereich nach dem Symbol für die HDX-Grafikstatusanzeige. Klicken Sie mit der rechten Maustaste darauf und wählen Sie im angezeigten Menü **Bildschirmfreigabe > Bildschirm einer anderen Person anzeigen**.



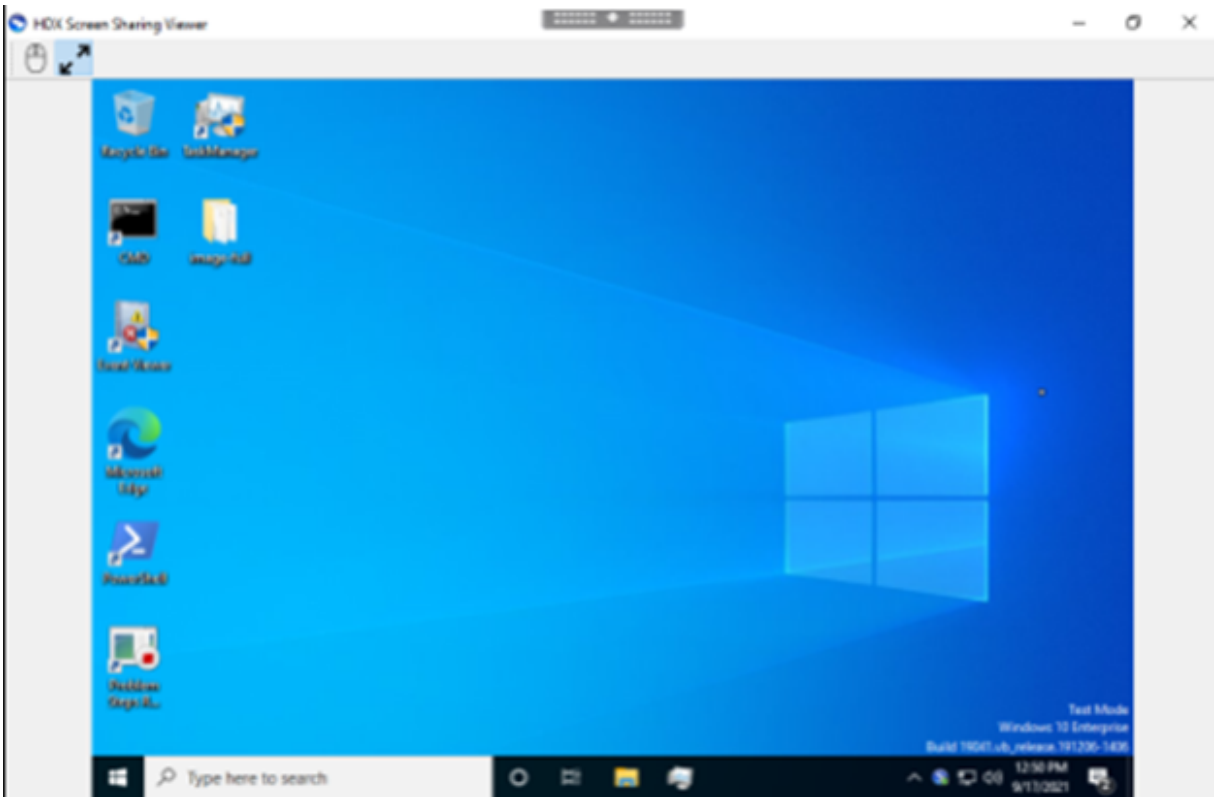

Geben Sie in das Textfeld die Verbindungszeichenfolge ein, die Sie vom Benutzer erhalten haben, der die Sitzung freigibt. Sie können die Zeichenfolge manuell eintippen oder per Kopieren und Einfügen eingeben. Klicken Sie auf **Verbinden**, um eine Verbindung herzustellen.




Sie können die Tastatur- und Maussteuerung anfordern, indem Sie auf das Maussymbol in der linken oberen Ecke des Fensters **HDX Screen Sharing Viewer** klicken.

Schließen Sie jederzeit das Fenster **HDX Screen sharing Viewer**, um die Verbindung zur freigegebenen Sitzung zu trennen.




### Andere Überlegungen

- Der Bildschirmfreigabe-Viewer ist im VDA in *C:\Programme\Citrix\HDX\bin\TwPlayer.exe* enthalten und kann als veröffentlichte Anwendung mit einem Virtual Apps-Server bereitgestellt werden. Dieses alternative Bereitstellungsmodell ermöglicht die Zusammenarbeit mit Benutzern, die keinen Zugriff auf einen virtuellen Desktop haben.
- Die Anzahl der Benutzer, die sich mit einer freigegebenen Sitzung verbinden dürfen, kann mithilfe des Netzwerkportbereichs in der Richtlinie für die Bildschirmfreigabe begrenzt werden. Pro

Benutzer ist ein Port erforderlich. Der Standardbereich erlaubt maximal 100 Benutzer.
- Alle mit der Sitzung verbundenen Bildschirme werden freigegeben. Sie können keine einzelnen Bildschirme auswählen.
- Der H.265-Videocodec wird nicht unterstützt.

## Virtuelles Anzeigelayout

June 27, 2024

Mit der Benutzeroberfläche für die Konfiguration der virtuellen Anzeige können Sie ein virtuelles Anzeigelayout pro Sitzungsbildschirm auf dem VDA innerhalb einer Livesitzung festlegen. Mit diesem Feature können Sie jeden Sitzungsbildschirm unabhängig in mehrere virtuelle Bildschirme aufteilen. Sie können einen Bildschirm in insgesamt 8 virtuelle Bildschirme auf dem Remotedesktop aufteilen. Sie können auch den primären Monitor der Sitzung und die DPI-Einstellungen für die Anzeigen aktualisieren.

Das virtuelle Anzeigenlayout wird pro Benutzer und Clientgerät gespeichert. Diese Konfiguration gilt für alle nachfolgenden Verbindungen von einem spezifischen Client für einen spezifischen Benutzer. Sie besteht fort beim Ändern der Sitzungsbildschirmgröße, beim Trennen oder Wiederverbinden der Sitzung und bei der Sitzungsanmeldung oder -abmeldung. Das Zurücksetzen des konfigurierten virtuellen Anzeigelayouts erfolgt bei einer Änderung der Sitzungsgröße und Änderung der Anzahl der Sitzungsbildschirme.

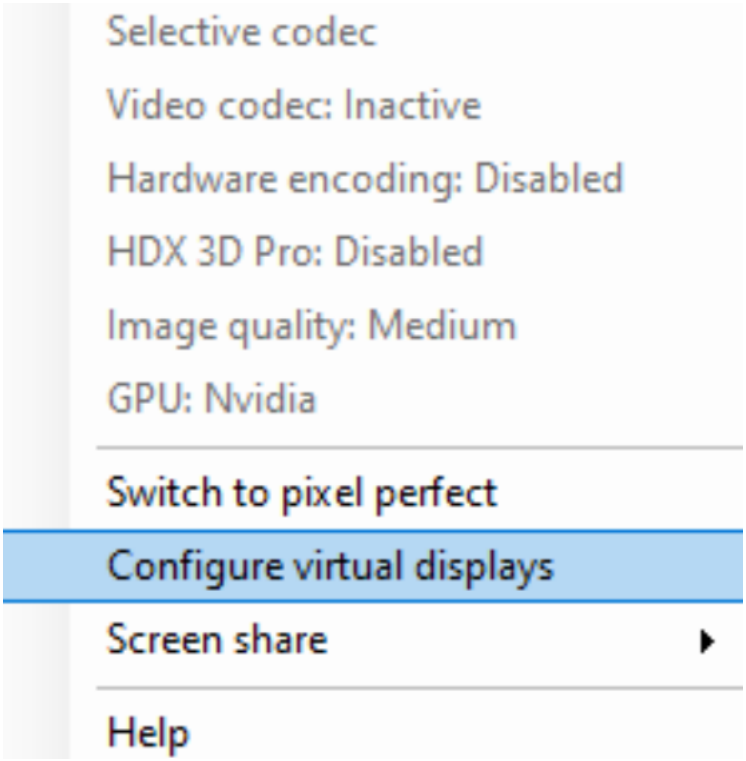
### Systemanforderungen

- Windows: VDA mit Einzel- oder Multisitzungs-OS
- Richtlinie Grafikstatusanzeige muss aktiviert sein
- Es können nur Desktopsitzungen konfiguriert werden.

### Konfiguration

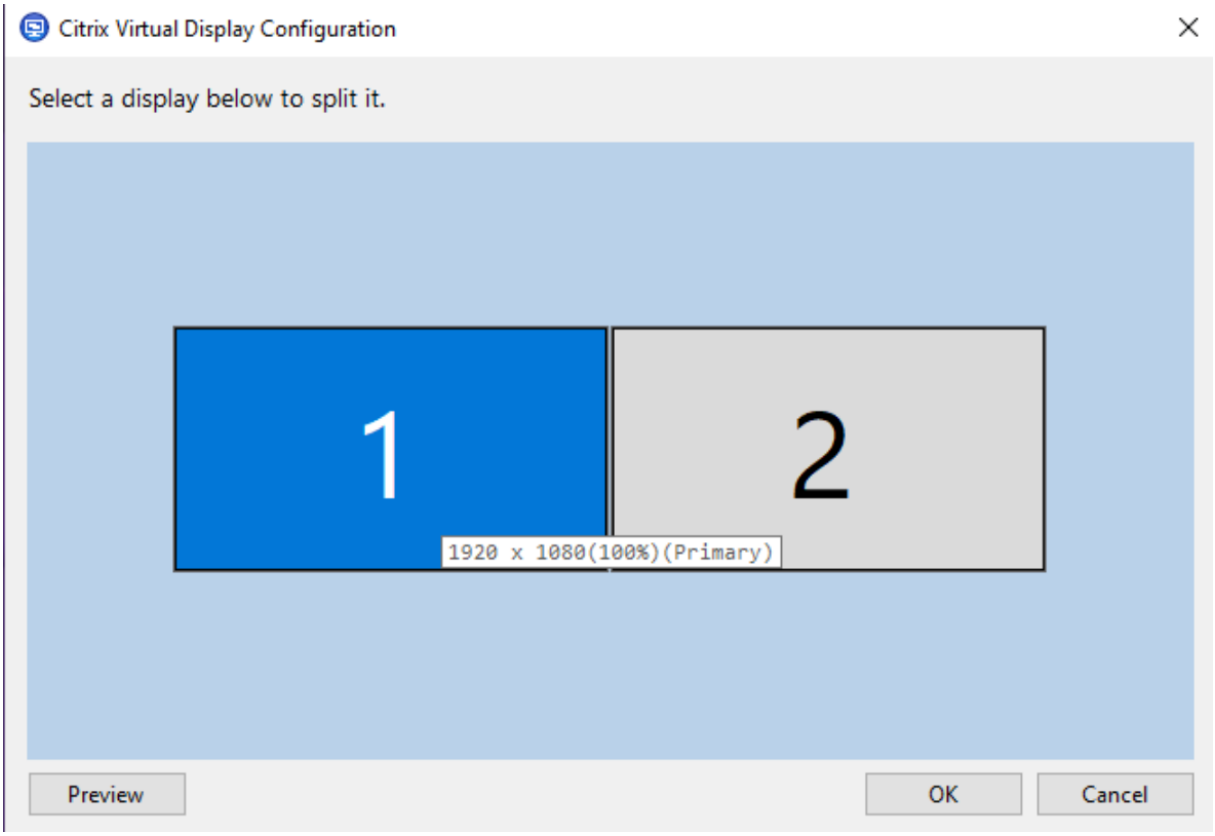
Klicken Sie zum Konfigurieren des virtuellen Anzeigelayouts mit der rechten Maustaste auf das Symbol für die Grafikstatusanzeige und wählen Sie die Option zum Konfigurieren der virtuellen Anzeigen aus. Die Benutzeroberfläche für die Konfiguration der virtuellen Anzeige wird gestartet.

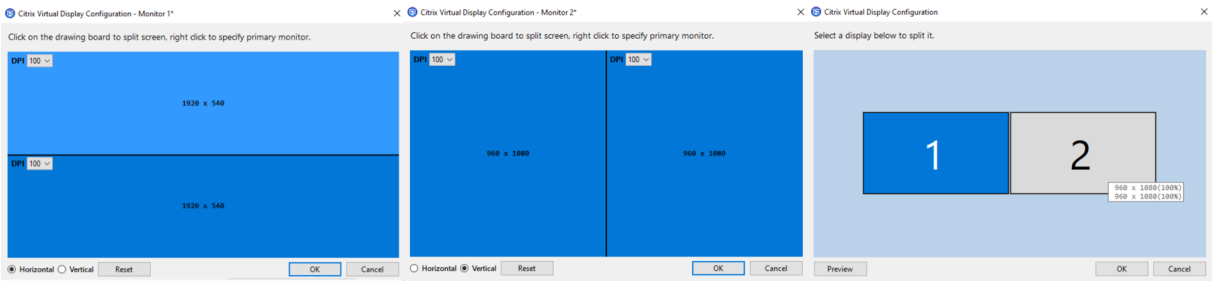



Die Benutzeroberfläche zeigt das Anzeigelayout der aktuellen Sitzung an, wobei der primäre Bildschirm der Sitzung blau gekennzeichnet ist. Sie können die QuickInfo für die Anzeigeeinstellungen sehen, wenn Sie mit der Maus auf eine Anzeige zeigen. Die QuickInfo enthält Informationen über das aktuelle virtuelle Anzeigelayout, das auf einem bestimmten Sitzungsbildschirm definiert ist.

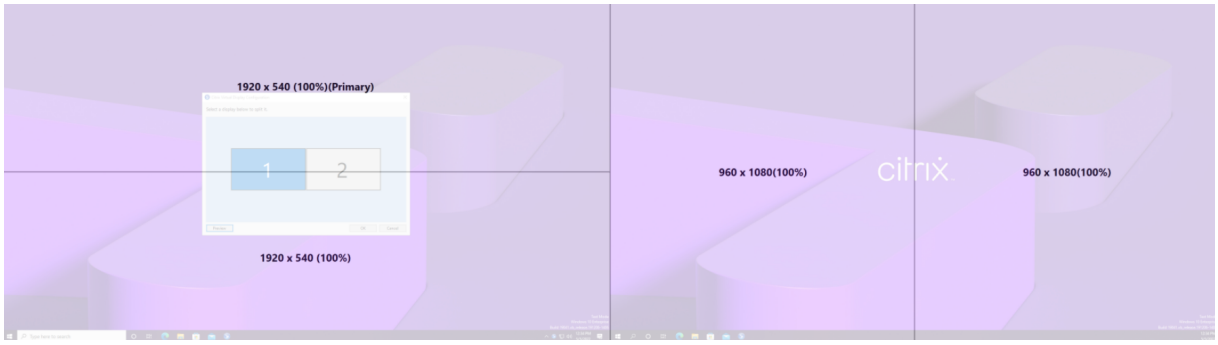



Wählen Sie eine Anzeige für den Übergang zu einer interaktiven Benutzeroberfläche aus, mit der Sie virtuelle Anzeigen für den ausgewählten Sitzungsbildschirm konfigurieren können. Sie können horizontale oder vertikale Linien ziehen, um den Bildschirm in virtuelle Bildschirme zu unterteilen. Der Bildschirm wird entsprechend den angegebenen Prozentsätzen der Auflösung des Sitzungsbildschirms aufgeteilt. Klicken Sie mit der rechten Maustaste auf eine virtuelle Anzeige, um sie als primären Bildschirm zu markieren, und legen Sie mithilfe der DPI-Dropdownliste einen bevorzugten Skalierungsfaktor für die virtuelle Anzeige fest. Klicken Sie nach Einrichtung eines virtuellen Anzeigelayouts auf **OK**, um das Layout vorübergehend zu speichern, oder klicken Sie auf **Abbrechen**, um die Änderungen zu verwerfen. Mit **Zurücksetzen** können Sie die Konfiguration rückgängig machen und das ursprüngliche Layout für den Sitzungsbildschirm wiederherstellen.

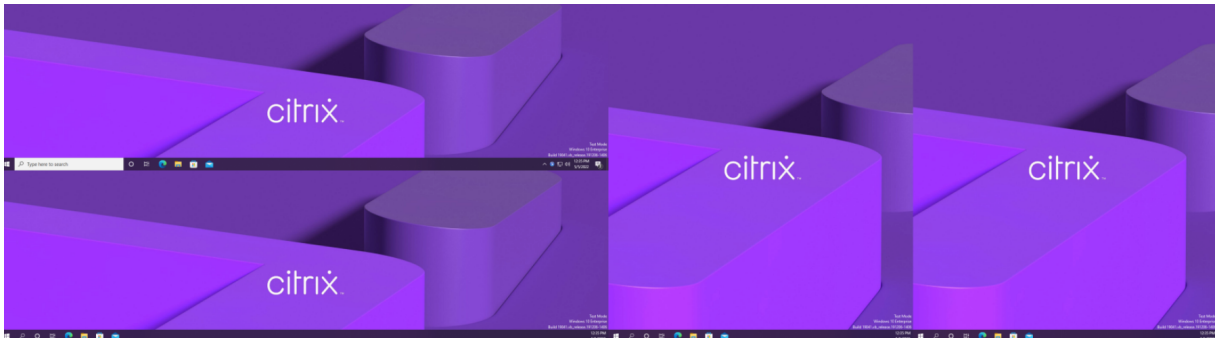


Um eine Vorschau des aktuell konfigurierten virtuellen Anzeigelayouts anzuzeigen, klicken Sie auf die Schaltfläche **Vorschau**. In einem Fenster werden die erwartete Position und Auflösung der virtuellen Anzeigen in der Sitzung hervorgehoben.




Klicken Sie auf **OK**, um das virtuelle Anzeigelayout sofort anzuwenden und zu speichern. Klicken Sie auf **Abbrechen**, um die Benutzeroberfläche zu schließen und alle Änderungen zu verwerfen.



### Andere Überlegungen

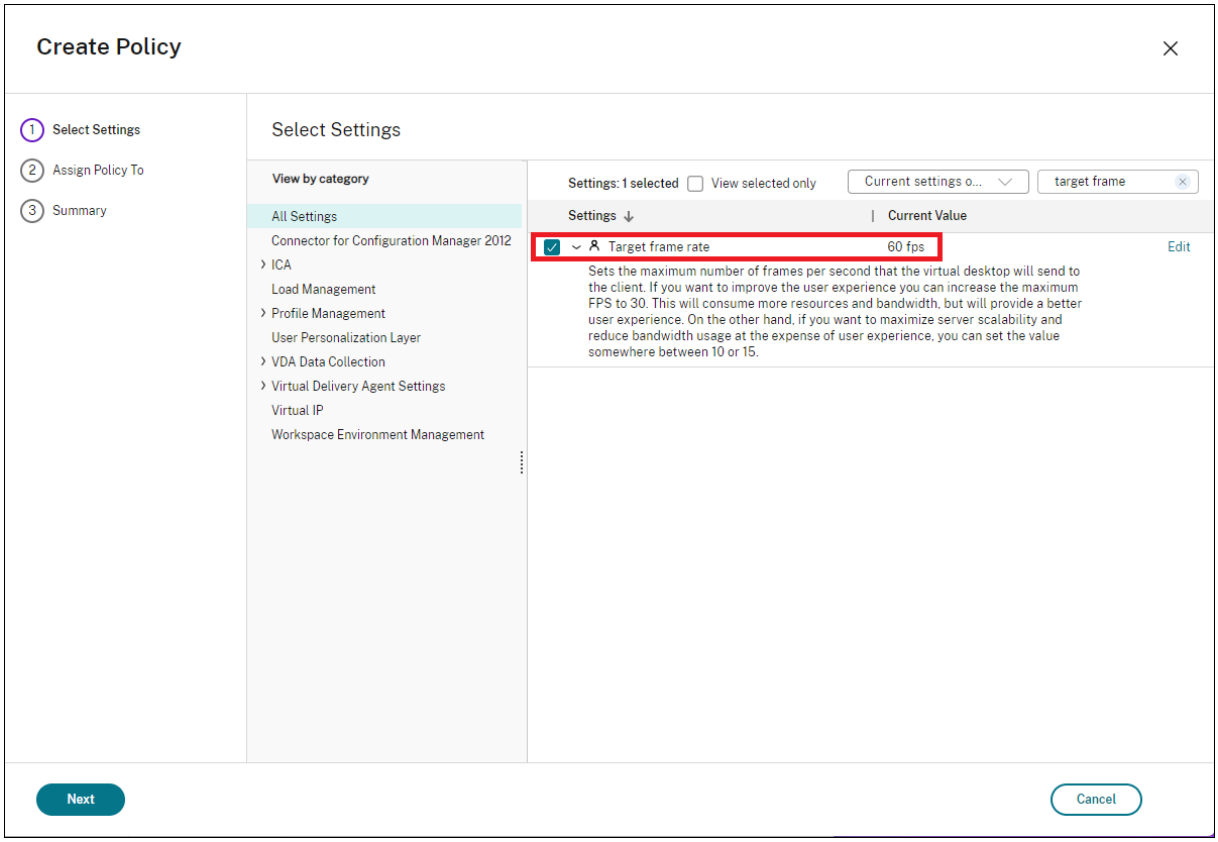
- Die erforderliche Mindestauflösung der virtuellen Anzeigen beträgt 640 x 480.
- Die über die Benutzeroberfläche definierte DPI-Einstellung der virtuellen Anzeige hängt von der Skalierungsunterstützung des Betriebssystems für die angegebene Anzeigeauflösung ab.
- Verwenden Sie dieses Feature nicht zusammen mit dem Feature “virtuelle Anzeige”der Citrix Workspace-App.
- Die Vorschaufunktion wird auf Server 2016 nicht unterstützt.

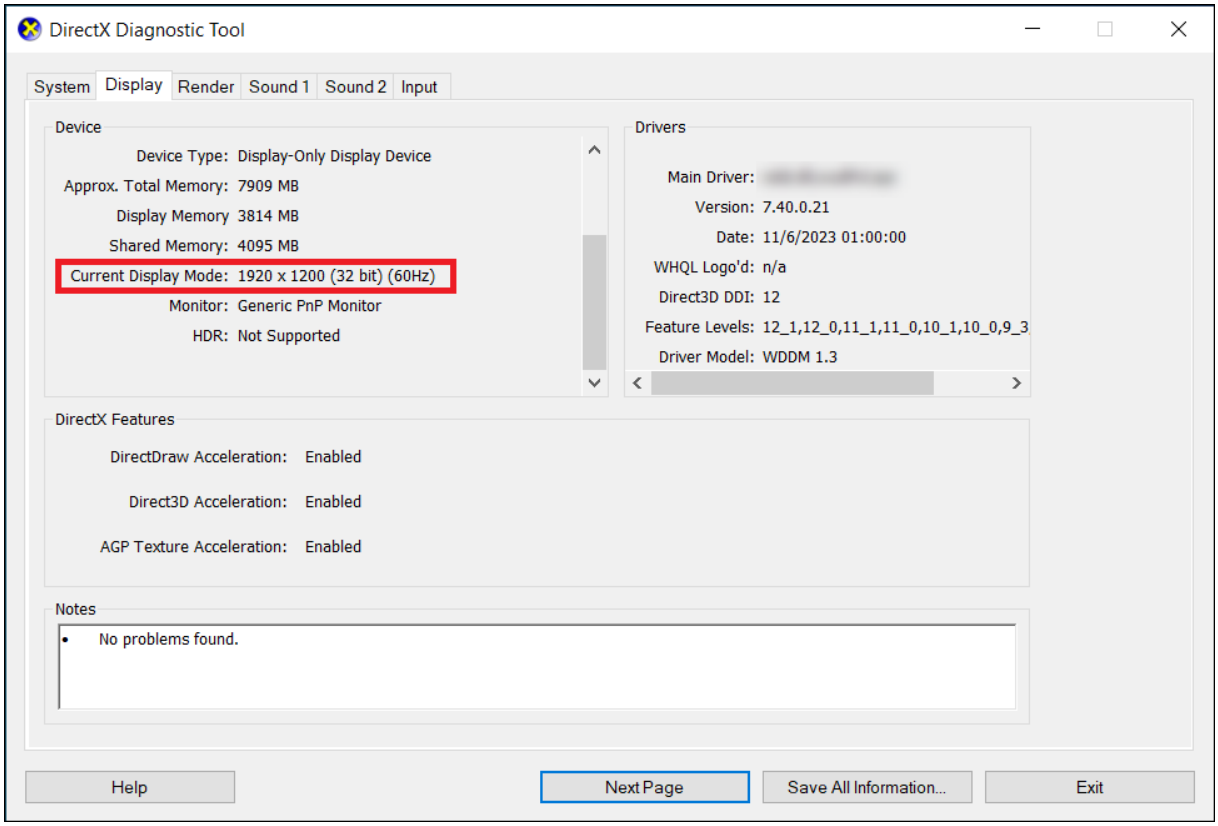
## Angepasste Aktualisierungsrate

June 27, 2024

Mit den neuen Skalierbarkeitsverbesserungen passt HDX die Aktualisierungsrate virtueller Monitore an die festgelegte FPS-Zielrichtlinie an. Adaptive Refresh Rate (ARR) ist sowohl für Einzel- als auch für Multisession-VDAs verfügbar und funktioniert sowohl für GPU-beschleunigte als auch für Nicht-GPU-Szenarien.



> **Hinweis**
>
> Die angepasste Aktualisierungsrate ist nur verfügbar, wenn Citrix Indirect Display oder IDD verwendet wird (gemäß der Standardeinstellung von Citrix Virtual Apps and Desktops) und nicht verfügbar, wenn vom Hersteller bereitgestellte Displayadapter verwendet werden.

## Verlusttoleranzmodus für Grafiken

June 27, 2024

Der Verlusttoleranzmodus für Grafiken wurde gründlich überarbeitet, um sicherzustellen, dass die Sitzung interaktiv bleibt, wenn ein Paketverlust erkannt wird. Wenn sich die Netzwerkbedingungen über die vordefinierten Schwellenwerte für Bandbreite, Latenz und Paketverlust hinaus verschlechtern, wechselt der Citrix Grafikencoder automatisch in einen aggressiveren Modus der Paketzustellung, um die Auswirkungen des Paketverlusts zu überwinden. Infolgedessen steigt die Bandbreitennutzung um einen Betrag, der proportional zum Umfang des Paketverlusts ist. Wenn sich die Bedingungen später verbessern, wechselt der Citrix Grafikencoder nahtlos zurück. Die Schwellenwerte können per Richtlinie konfiguriert werden. Die Standardwerte sind 300 ms Latenz und 5 % Paketverlust.

Citrix Workspace-App für Windows 2311 wird derzeit unterstützt. Unterstützung für andere Plattformen wird in späteren Versionen der Citrix Workspace-App hinzugefügt. Wie bei früheren Versionen dieser Funktion muss HDX Adaptive Transport (EDT) aktiviert sein, damit dieses Feature funktioniert. Wenn Sie eine Verbindung über den Citrix Gateway Service herstellen, muss außerdem der Verlusttoleranzmodus für Grafiken auf dem Gateway aktiviert sein.

## Multimedia

June 27, 2024

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.

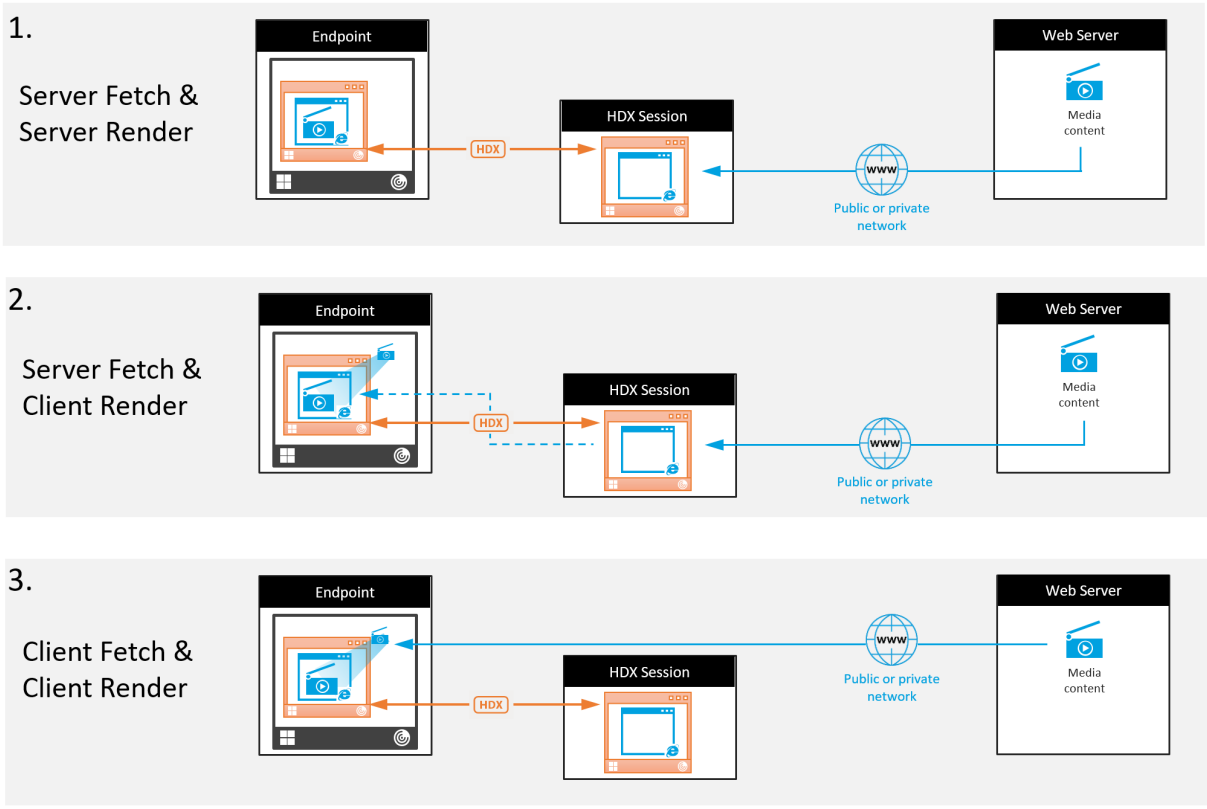
Da die meisten Server keine Hardwarebeschleunigung für die Videokomprimierung bieten, beeinträchtigt eine Abwicklung der gesamten Videoverarbeitung auf der Server-CPU die Serverskalierbarkeit. Zur Wahrung einer hohen Serverskalierbarkeit können viele Multimediaformate zur lokalen Wiedergabe an die Benutzergeräte 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 |
| Quicktime | Mac OS X |

## Double-Hop-Unterstützung mit Medienumleitungstechnologien

| | | |
|---|---|---|
| | Audioumleitung | Nein |
| | Browserinhaltsumleitung | Nein |
| | HDX-Webcamumleitung | Ja |
| | HTML5-Videoumleitung | Ja |
| | Windows Media-Umleitung | Ja |

# Audiofeatures

June 27, 2024

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".

## Adaptives Audio

Bei adaptivem Audio müssen Sie die Audioqualitätsrichtlinien auf dem VDA nicht manuell konfigurieren. Adaptives Audio optimiert die Einstellungen für Ihre Umgebung und ersetzt veraltete Audiokomprimierungsformate für eine hervorragende Benutzererfahrung.

Adaptives Audio ist standardmäßig aktiviert. Informationen zum Deaktivieren von adaptivem Audio finden Sie unter Einstellungen der Richtlinie "Audio".

> **Wichtig:**
>
> Von Citrix wird empfohlen, Audio per User Datagram Protocol (UDP) anstelle von TCP zu senden, wenn Echtzeit-Audioanwendungen erforderlich sind. Die folgenden Audiotransportoptionen sind über UDP verfügbar:
>
> - Audio über UDP
> - Adaptiver HDX-Transport (Enlightened Data Transport)
>
> 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.
>
> Weitere Informationen zu adaptivem Audio und UDP-Audio finden Sie unter Audio über UDP - Real-time Transport und Audio-UDP-Portbereich.

## Unterstützung für Audio über Verlusttoleranzmodus

Der Verlusttoleranzmodus unterstützt Audio. Das Feature verbessert das Echtzeit-Streaming und die Audioqualität gegenüber EDT, wenn die Verbindung über ein Netzwerk mit hoher Latenz und Paketverlust hergestellt wird. Diese Funktion ist standardmäßig deaktiviert und der **Verlusttoleranzmodus für Audiorichtlinien** sollte aktiviert
sein.

#### Systemanforderungen

Achten Sie darauf, dass die folgenden Produkte in der für den Verlusttoleranzmodus erforderlichen Mindestversion vorliegen:

- Citrix Virtual Delivery Agent (VDA) 2308
- Citrix Workspace-App für Windows 2309

Darüber hinaus müssen die folgenden Features aktiviert sein:

- Richtlinie "Adaptiver HDX-Transport".
- Optional: Für Remoteverbindungen ist Citrix Gateway Service erforderlich.

> **Hinweis:**
>
> Wenn die oben genannten Bedingungen nicht erfüllt sind, wird Audio über EDT Reliable gesendet.

#### Weitere Informationen

Der Verlusttoleranzmodus ist ein verlusttolerantes Transportprotokoll, das Paketverluste bei der Übertragung ohne erneutes Senden von Multimediainhalten toleriert und so für ein eher echtzeitähnliches Erlebnis sorgt.

Enlightened Data Transport (EDT) ist ein von Citrix entwickeltes Transportprotokoll, das eine überlegene Benutzererfahrung bei schwierigen Langstreckenverbindungen, ohne Abstriche bei der Serverskalierbarkeit liefert . Der Verlusttoleranzmodus ist ein Citrix Gateway Service-Feature, das unter Einsatz des Transportprotokolls den Verlusttoleranzmodus auch in stark belasteten Netzwerken eine stabile Verbindung aufrechterhält. Er gewährleistet eine gleichförmige und stabile Erfahrung für Remotebenutzer. Unter normalen Bedingungen liefern EDT und der Verlusttoleranzmodus ähnliche Ergebnisse. In Netzwerken mit Paketverlust bietet der Verlusttoleranzmodus jedoch im Vergleich zu EDT ein besseres Audioerlebnis. Dies macht es unverzichtbar für Remotebenutzer, die bei ihrer Arbeit auf Echtzeit-Multimedia angewiesen sind.

### Audioqualität

Im Allgemeinen erfordert eine höhere Audioqualität mehr Bandbreite und führt zu einer höheren CPU-Auslastung, da mehr Audiodaten an die Benutzergeräte gesendet werden. Mit der Audiokomprimierung können Sie die Audioqualität und die Sitzungsleistung aufeinander abstimmen; verwenden Sie Citrix Richtlinieneinstellungen, um den Komprimierungsgrad für Audiodateien zu konfigurieren.

Standardmäßig ist die **Richtlinieneinstellung für Audioqualität** bei Verwendung von TCP auf "Hoch - High Definition-Audio"eingestellt. Bei Verwendung von UDP (empfohlen) wird die Richtlinie auf "Mit-

tel - 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:

- Adaptives Audio (Standard)
  - Bitrate: variabel adaptiv
  - Anzahl der Kanäle: 2 (Stereo) für Wiedergabe, 1 (Mono) für Mikrofonaufnahme
  - Frequenz: 48000 Hz
  - Bit-Tiefe: 16 Bit
- Hohe Qualität
  - 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.

> **Hinweis:**
>
> Wenn Audio über UDP-Real-Time Transport für adaptives Audio nicht erforderlich ist, empfiehlt Citrix, die Richtlinieneinstellung auf "Deaktiviert"zu konfigurieren. Auf diese Weise wird verhindert, dass Citrix Workspace-Apps offene UDP-Verbindungen anfordern oder unerwünschte Citrix Workspace-App-Firewallkonfigurationsfenster aufrufen.

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
```

Wenn Sie UDP-Audio über die Datei default.ica aktiviert, ist UDP-Audio für alle Benutzer des Stores aktiviert.

### Echo in Multimediakonferenzen vermeiden

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. Weitere Informationen finden Sie unter Vermeiden von Echo in Multimediakonferenzen in der Liste der über die Registrierung verwalteten Features.

### 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:
  - HDX-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.

### Befehlszeilentool für die Audiodiagnose

Das Audiodiagnose-Befehlszeilentool auf dem VDA kann verwendet werden, um Sitzungsdaten im Zusammenhang mit Audiorichtlinien, Konfiguration und Datentransport abzufragen.

#### Verwendung

Öffnen Sie eine Befehlszeile und führen Sie `CtxAudio.exe` im Ordner `C:\Program Files\Citrix\HDX\bin` aus.

- Wenn Sie das Tool als Administrator ausführen, werden die Audioinformationen aller aktiven ICA-Sitzungen angezeigt.
- Wenn Sie das Tool ohne Administratorrechte ausführen, werden die Audioinformationen der ICA-Sitzung des aktuellen Benutzers angezeigt.

#### Ausgabe

Das Tool gibt verschiedene Konfigurationseinstellungen aus, die bei der Diagnose von Audioproblemen in einer Sitzung helfen können.

| Abschnitt | Beschreibung |
|---|---|
| Richtlinieninformationen | Die Audiorichtlinien gelten für die aktuelle(n) Sitzung(en). |
| Informationen zu den Einstellungen | Audiobezogene Konfigurationseinstellungen, die in der Registrierung gespeichert werden. |
| Zustandsinformationen | Audiozustand, Version, Codecs und Transport für die aktuelle(n) Sitzung(en). |
| Geräteinformationen | In der Sitzung verwendete Gerätenamen, ihre Rollen und ihr Status. |

> **Hinweis:**
>
> Die Ausgabe hängt davon ab, ob Sie das Tool auf einem Multisitzungs-VDA oder einem Einzelsitzungs-VDA ausführen.

### Einschränkung

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 den Registrierungsschlüssel auf der RDS-Maschine hinzu und starten Sie diese anschließend neu. Weitere Informationen finden Sie unter Audio-Einschränkung in der Liste der über die Registrierung verwalteten Features.

# Browserinhaltsumleitung

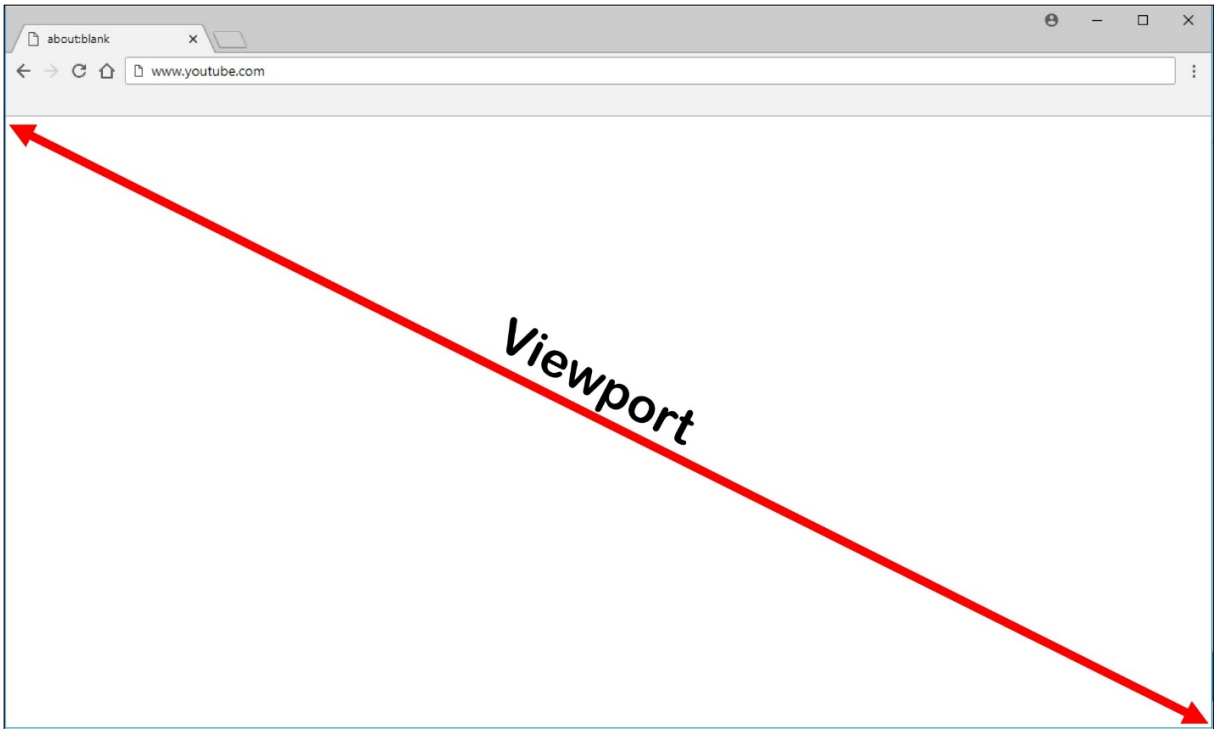
June 27, 2024

Die Umleitung des Browserinhalts verhindert die VDA-seitige Wiedergabe von Webseiten auf einer Positivliste. Dabei wird von der Citrix Workspace-App für Windows oder Linux 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 Browser auf dem VDA führt den Abgleich der von den Benutzern angesteuerten URLs gegen die Positiv- oder Sperrliste mit einer

Browsererweiterung durch. Die Browsererweiterung für Chrome steht im Chrome Web Store zur Verfügung und kann über Gruppenrichtlinien und ADMX-Dateien bereitgestellt werden. Chrome-Erweiterungen werden pro Benutzer installiert. Das Update eines Gold-Masterimages zum Hinzufügen oder Entfernen einer Erweiterung ist nicht erforderlich. Für Microsoft Edge ist die Erweiterung nicht direkt verfügbar. Sie müssen Erweiterungen aus dem Chrome Store erlauben, sie zu finden und zu installieren.

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.

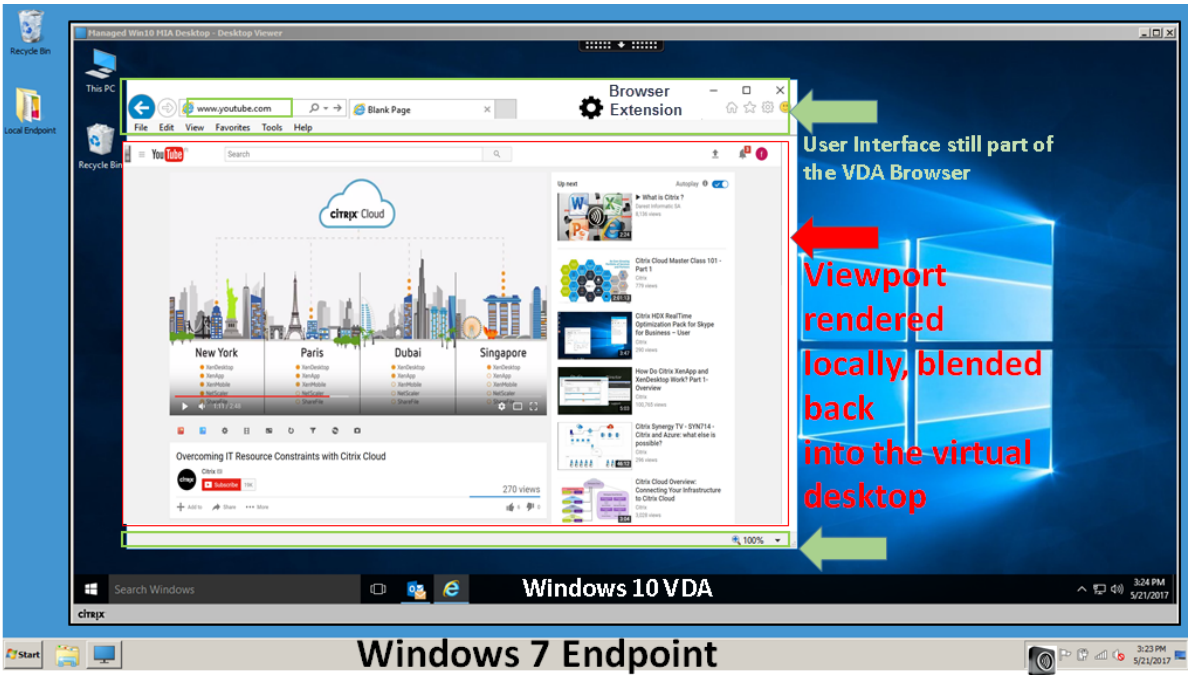
> **Hinweis:**
>
> Weitere Informationen zu neuen Features und Fixes der Erweiterung für die Browserinhaltsumleitung finden Sie zusammen mit der Erweiterung im Chrome Web Store (Suchbegriff "`citrix bcr`").

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.




Szenarien für den Inhaltsabruf durch die Citrix Workspace-App:

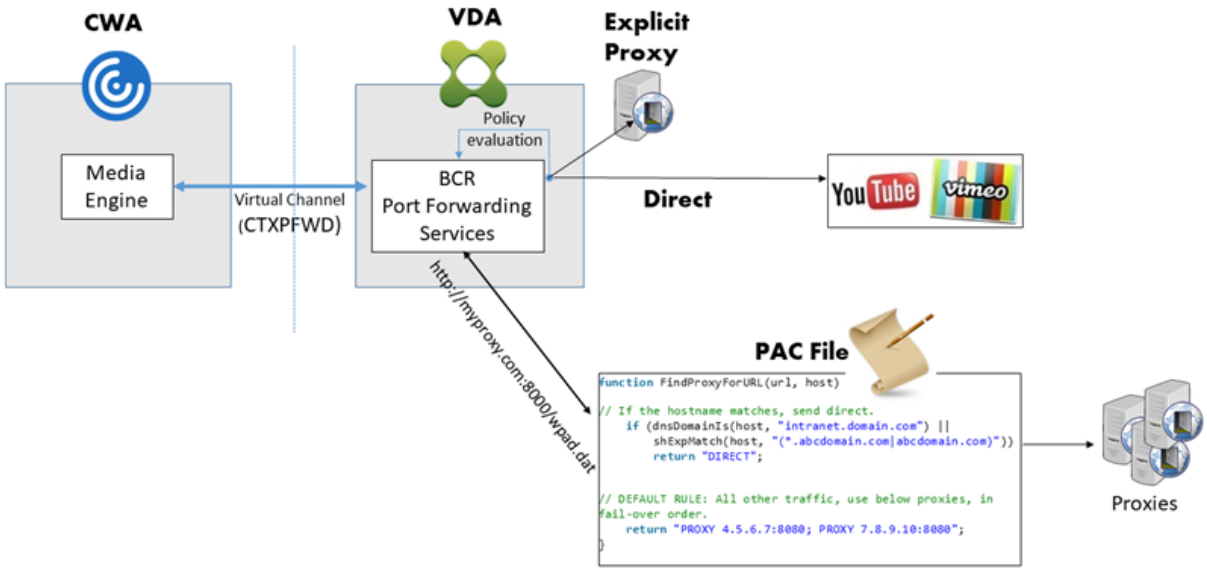
- **Abruf und Wiedergabe auf dem Server**: Es findet keine Umleitung statt, weil die Site nicht auf der Positivliste steht oder ein Fehler aufgetreten ist. Die Wiedergabe findet dann auf dem VDA statt und das Grafikremoting mit Thinwire. Verwenden Sie Richtlinien, um dieses Fallbackverhalten zu steuern. 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 Internetzugriff 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 auf ein Proxygerät, auf das der VDA zugreift, um Internetzugriff zu erhalten.

  Geeignete Richtlinienoption:

  - **Expliziter Proxy**: Wenn Sie einen einzelnen expliziten Proxy im Datencenter haben.
  - **Direkt oder transparent**: Wenn Sie keine Proxys haben oder transparente Proxys verwenden.
  - **PAC- Dateien**: Wenn Sie PAC-Dateien verwenden, sodass Browser auf dem VDA automatisch den geeigneten Proxyserver zum Abrufen einer angegebenen URL auswählen können.

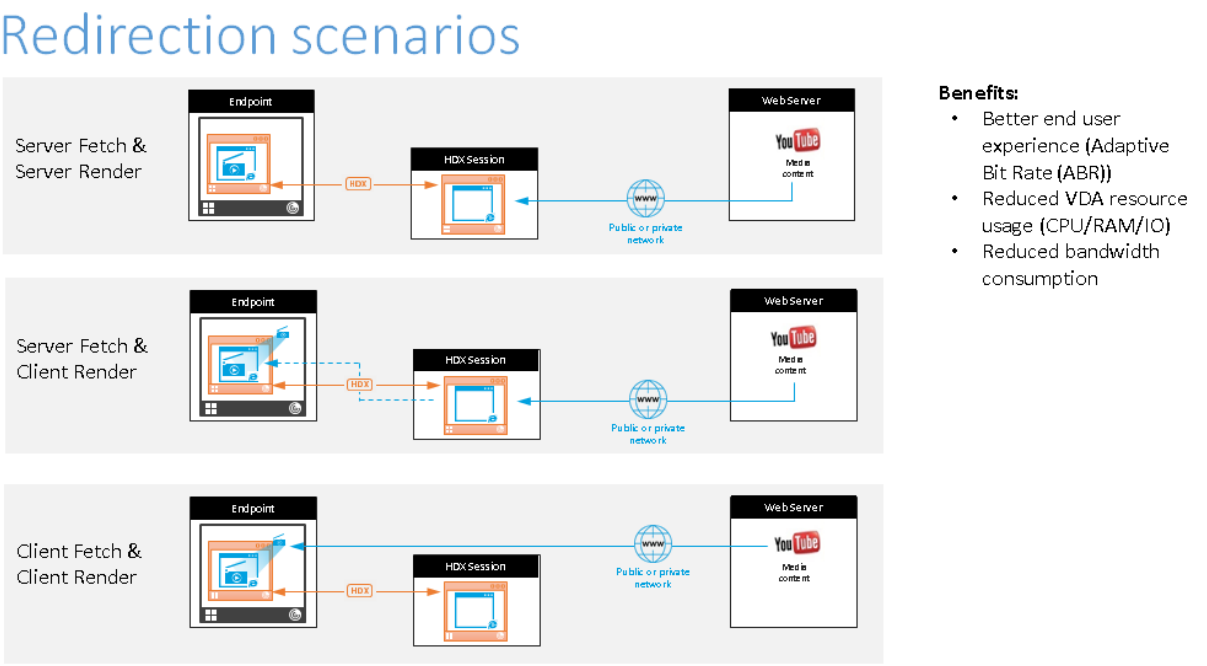



- **Abruf und Wiedergabe auf dem Client**: Da die Citrix Workspace-App direkt auf den Webserver zugreift, ist Internetzugriff erforderlich. In diesem Szenario wird die gesamte Netzwerk-, CPU- und RAM-Last von der XenApp- und XenDesktop-Site abgeladen.

  Vorteile:

  - Bessere Endbenutzererfahrung (adaptive Bitrate (ABR))
  - Reduzierte VDA-Ressourcennutzung (CPU/RAM/IO)
  - Reduzierter Bandbreitenverbrauch




**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 ein serverseitiges Rendering 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 Teil der Sperrlistenrichtlinie sein.

## Systemanforderungen

### Citrix Virtual Apps and Desktops

- Citrix Virtual Apps and Desktops 7 1808 oder höher
- XenApp und XenDesktop 7.15 CU5 oder höher
- VDA-Betriebssystem: Windows 10 und 11, Windows Server 2016/2019/2022
- Browser auf dem VDA:
  - Aktuelle Version von Google Chrome
  - Aktuelle Version von Microsoft Edge

- Die BCR-Erweiterung aus dem Chrome Web Store installiert im Browser auf dem VDA

#### Windows-Endpunkte

- Windows 10 und 11
- Citrix Workspace-App 1809 für Windows oder höher

> **Hinweis:**
>
> Die Browserinhaltsumleitung wird in den LTSR-Versionen -1912 und 2203.1 der Citrix Workspace-App nicht unterstützt.

#### Linux-Endpunkte

- Citrix Workspace-App 1808 für Linux oder später
- Thin Client-Terminals müssen WebKitGTK+ enthalten.

#### Mac-Endgeräte (Preview)

- macOS 11 Big Sur
- macOS 12 Monterey
- macOS 13 Ventura
- macOS 14 Sonoma (bis zu 14.2.1) mit der Mindestversion der Citrix Workspace-App als 2311

### Problembehandlung

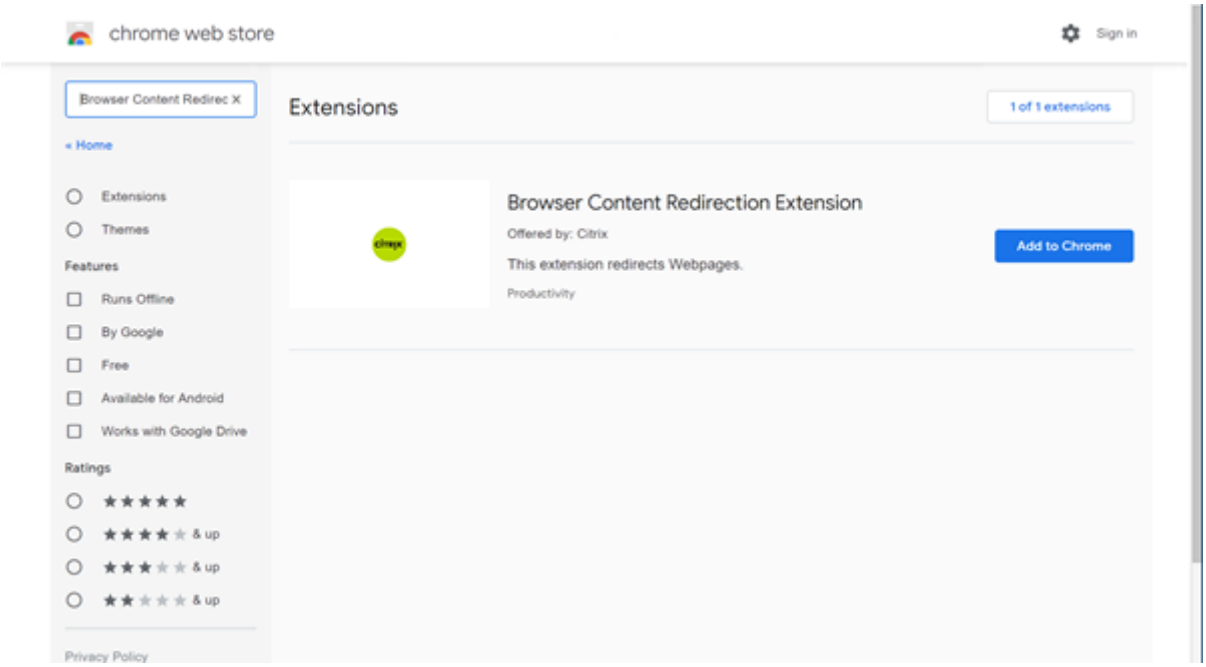
Informationen zur Problembehandlung finden Sie im Knowledge Center-Artikel Problembehandlung bei der Browserinhaltsumleitung.

### 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.

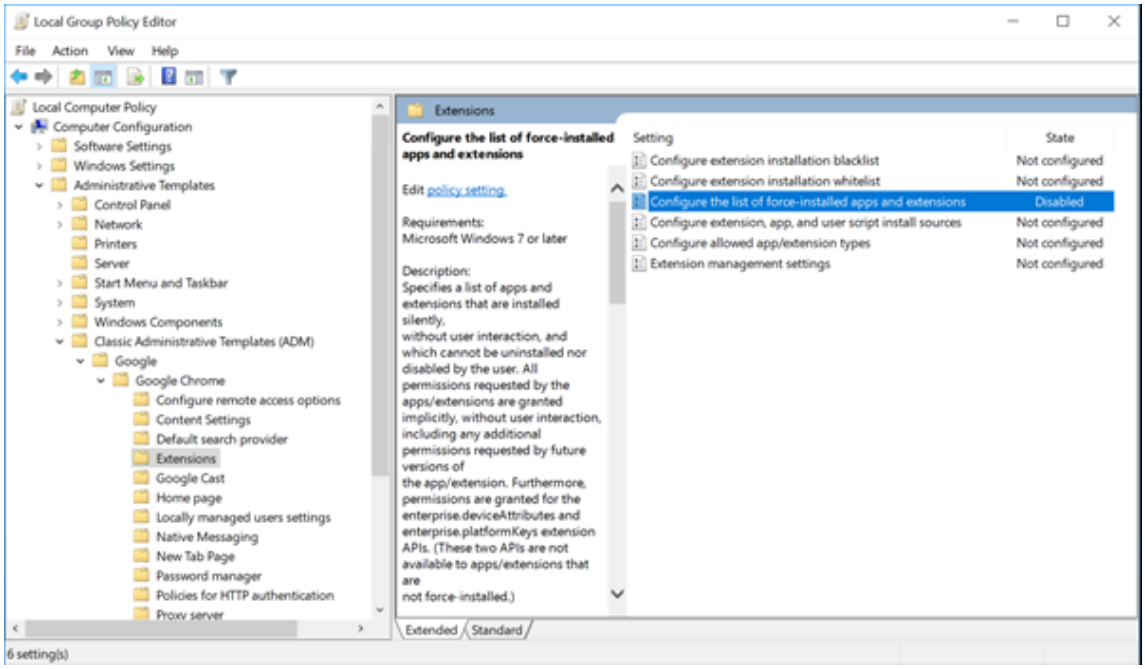



Diese Methode funktioniert für einzelne Benutzer. Um die Erweiterung für eine große Benutzergruppe bereitzustellen, verwenden Sie die Gruppenrichtlinie.

**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 Set Chrome Browser policies on managed PCs.
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**.

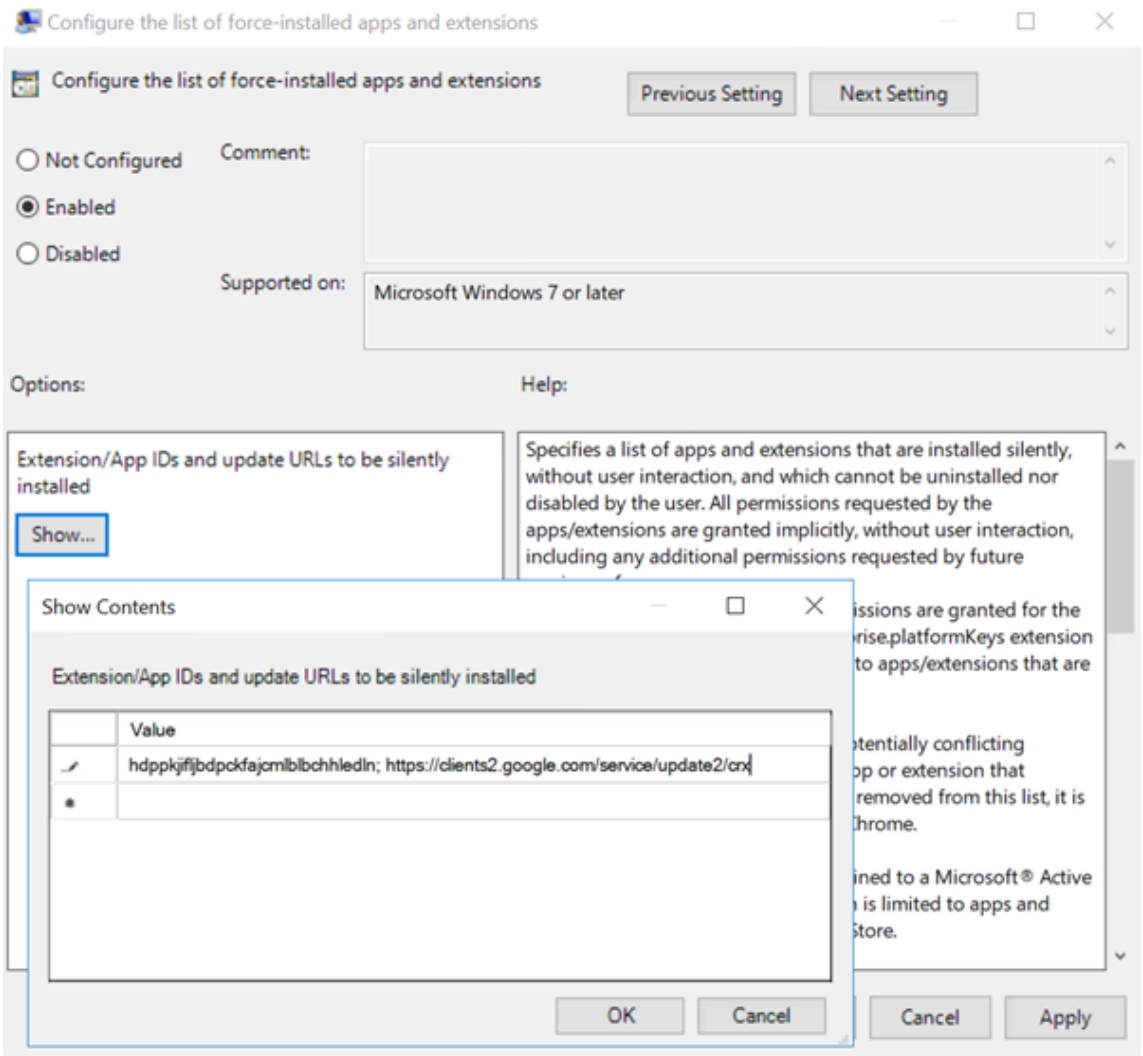
 




3. Klicken Sie auf **Show** und geben Sie die folgende Zeichenfolge ein (= Erweiterungs-ID). Aktualisieren Sie die URL für die Browserinhaltsumleitungserweiterung.

   ```
   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

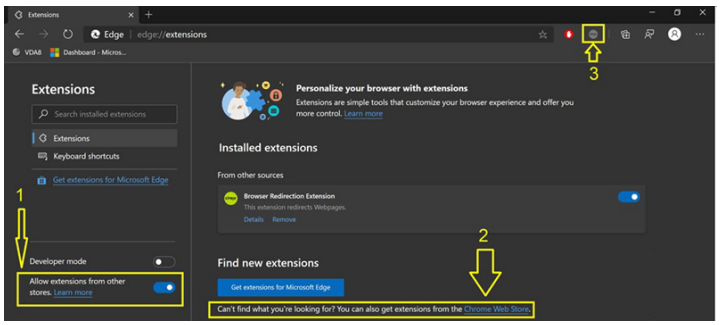
Um die Erweiterung zur Browserinhaltsumleitung in Edge zu installieren, müssen Sie Version **83.0.478.37** oder höher des Edge-Browsers verwenden.

1. Klicken Sie auf die Option **Erweiterungen**. Wählen Sie **Erweiterung verwalten**. Aktivieren Sie

**Erweiterungen aus anderen Stores zulassen**.

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

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. Alternativ können Sie die GPU-Beschleunigung der Browserinhaltsumleitung für Chrome deaktivieren, indem Sie den Registrierungsschlüssel auf der Maschine des Benutzers erstellen. Weitere Informationen finden Sie unter Umleitung des Browserinhalts und DPI in der Liste der über die Registrierung verwalteten Features.

## Single Sign-On mit integrierter Windows-Authentifizierung

Die Browserinhaltsumleitung verbessert das Overlay-Netz und verwendet das **Aushandlungsschema** zur Authentifizierung bei Webservern, die mit der integrierten Windows-Authentifizierung (IWA) in derselben Domäne wie der VDA konfiguriert sind.

In der Regel verwendet die Browserinhaltsumleitung ein Standardauthentifizierungsschema, bei dem Benutzer sich bei jedem Zugriff auf den Webserver mit ihren VDA-Anmeldeinformationen authentifizieren müssen. Für einen Single Sign-On können Sie entweder die Richtlinieneinstellung **Unterstützung der integrierten Windows-Authentifizierung für die Browserinhaltsumleitung** aktivieren oder einen Registrierungsschlüssel auf dem VDA erstellen.

Führen Sie vor dem Aktivieren von Single Sign-On folgende Schritte aus:

- Konfigurieren Sie in der Kerberos-Infrastruktur die Ausgabe von Tickets für Dienstprinzipalnamen, die aus dem Hostnamen erstellt wurden. Beispiel: `HTTP/serverhostname.com`.
- Für serverseitigen Abruf: Wenn Sie die Browserinhaltsumleitung im Modus mit serverseitigem Abruf verwenden, muss das DNS ordnungsgemäß auf dem VDA konfiguriert sein.

- Für den clientseitigen Abruf: Wenn Sie die Browserinhaltsumleitung im Modus mit clientseitigem Abruf verwenden, muss das DNS ordnungsgemäß auf dem Clientgerät konfiguriert sein, und Sie müssen TCP-Verbindungen vom Overlay-Netz zur IP-Adresse des Webservers zulassen.

Informationen zum Konfigurieren von Single Sign-On mit der Richtlinie zur Browserinhaltsumleitung finden Sie in der Einstellung Integrierte Windows-Authentifizierungsunterstützung für die Browserinhaltsumleitung.

Alternativ können Sie Single Sign-On bei einem Webserver aktivieren, indem Sie einen Registrierungsschlüssel auf dem VDA hinzufügen. Informationen finden Sie unter Single Sign-On mit integrierter Windows-Authentifizierung für die Browserinhaltsumleitung in der Liste der Features, die über die Registrierung verwaltet werden.

### User-Agent-Anforderungsheader

Der User-Agent-Header hilft bei der Identifizierung von HTTP-Anforderungen, die von der Browserinhaltsumleitung gesendet werden. Diese Einstellung kann beim Konfigurieren von Proxy- und Firewallregeln nützlich sein. Wenn der Server beispielsweise von der Browserinhaltsumleitung gesendete Anforderungen blockiert, können Sie eine Regel mit dem User-Agent-Header zum Umgehen bestimmter Anforderungen erstellen.

Nur Windows-Geräte unterstützen den User-Agent-Anforderungsheader.

Standardmäßig ist die Zeichenfolge des User-Agent-Anforderungsheaders deaktiviert. Zum Aktivieren des User-Agent-Headers für vom Client gerenderte Inhalte verwenden Sie den Registrierungs-Editor. Weitere Informationen finden Sie unter User-Agent-Anforderungsheader in der Liste der über die Registrierung verwalteten Features.

### Kompatibilität von Clients mit der Browserinhaltsumleitung

Sie können per WMI prüfen, ob Ihr Client mit der Browserinhaltsumleitung kompatibel ist. Verwenden Sie eine beliebige Methode für den Zugriff auf WMI. Das folgende Beispiel gilt für die Verwendung von PowerShell.

1. Öffnen Sie PowerShell.
2. Führen Sie `Get-WmiObject -Class CTXBCRStatus` aus.
3. Prüfen Sie den Parameter `BCR_Capable`.
    - `True` bedeutet, dass der Client mit der Browserinhaltsumleitung kompatibel ist.
    - `False` bedeutet, dass der Client mit der Browserinhaltsumleitung nicht kompatibel ist.

**Weitere Informationen**

- Wenn `CtxBrowserSvc` nicht verfügbar ist, werden beim Ausführen des Befehls keine Ergebnisse angezeigt.
- Wenn `CtxBrowserSvc` noch nie ausgeführt wurde, wird eine ungültige Klasse gemeldet.

### Einschränkungen bei der Umleitung von Browserinhalten

Die Umleitung von Browserinhalten unterstützt die folgenden Anwendungsfälle nicht:

- Webanwendungen, die Popupfenster benötigen, werden nicht unterstützt.
- Webanwendungen, die die Persistenz von Sitzungscookies erfordern, werden ebenfalls nicht unterstützt.
  Anwendungen, die vom Google-Authentifizierungsdienst abhängig sind (z. B. Google Meet), können möglicherweise blockiert werden.
- Das Erweiterungs-Plug-In ist nicht offiziell im Microsoft Edge Store veröffentlicht. Sie können jedoch den Chrome Store verwenden, um die Erweiterungen zu installieren.
- Die HTML5-Videoumleitungsrichtlinie muss deaktiviert sein, wenn die Browserinhaltsumleitung verwendet wird.
- Die Umleitung von Browserinhalten wird im ARMhf -Framework (ARM Hard Float) nicht unterstützt.
- Benutzer können gelegentlich von Sitzungen aufgrund von unzuverlässigen Netzwerken, stark variierender Netzwerklatenz oder Bereichseinschränkungen von drahtlosen Geräten getrennt werden. Derzeit verfügt BCR nicht über ausreichende Ausweichmechanismen oder Berichtsmechanismen für solche Szenarien.
- Sie können im BCR-Overlay-Browser keine Dateien herunterladen oder drucken.

## HDX-Videokonferenzen und Webcam-Videokomprimierung

June 27, 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. Erstellen 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. Die generische HDX-USB-Umleitung wird nur empfohlen, wenn Probleme mit der Anwendungskompatibilität bei der HDX-Videokomprimierung auftreten oder wenn Sie erweiterte native Funktionen der Webcam nutzen müssen. Für eine bessere Leistung empfiehlt Citrix, den Virtual Delivery Agent mit mindestens zwei virtuellen CPUs zu konfigurieren.

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

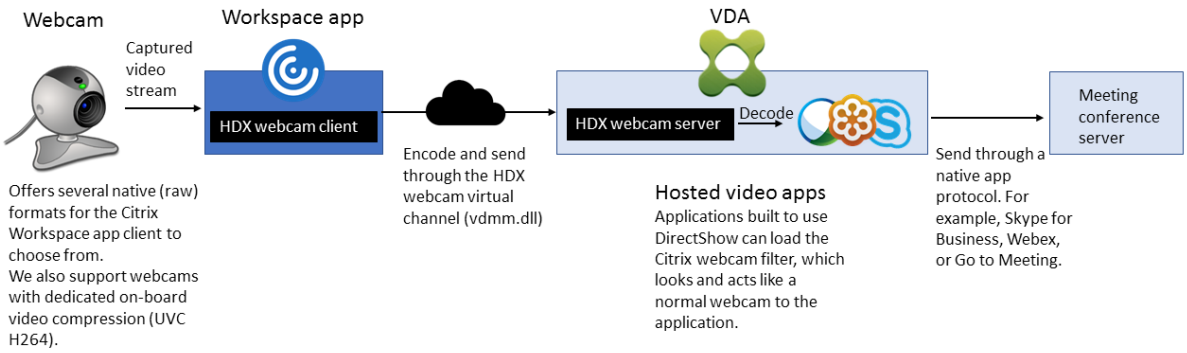
Die HDX-Webcamvideokomprimierung wird auch als **optimierter** Webcammodus bezeichnet. Bei dieser Art der Webcamvideokomprimierung wird das H.264-Video direkt an die Videokonferenzanwendung gesendet, die in der virtuellen Sitzung ausgeführt wird. Zum Optimieren von VDA-Ressourcen wird das Webcamvideo von der HDX-Webcamkomprimierung nicht codiert, transcodiert und decodiert. Dieses Feature ist standardmäßig aktiviert.

Um das direkte Videostreaming vom Server zur Videokonferenz-App zu deaktivieren, legen Sie den Registrierungsschlüssel im VDA auf "0"fest. Weitere Informationen finden Sie unter Webcamvideokomprimierung in der Liste der Features, die über die Registrierung verwaltet werden.

Wenn Sie die Standardfunktion zum Streaming von Videoressourcen deaktivieren, verwendet die HDX-Webcamvideokomprimierung die Multimediaframework-Technologie des Clientbetriebssystems, um Video von Aufnahmegeräten zu erfassen, zu transcodieren und zu komprimieren. Hersteller von Aufnahmegeräten liefern die Treiber, die sich in die Betriebssystem-Kernelstreaming-Architektur einfügen.

Der Client übernimmt die Kommunikation mit der Webcam. Der Client sendet Videos nur an Server, die es ordnungsgemäß anzeigen können. Der Server ist nicht direkt mit der Webcam verbunden, seine Integration sorgt jedoch dafür, dass die gleiche Erfahrung auf dem Desktop geliefert wird. Die Workspace-App komprimiert Videos zum Einsparen von Bandbreite und zur Gewährleistung einer besseren Ausfallsicherheit in WANs.




Die Richtlinie für **Multimediakonferenzen** muss für HDX-Webcamvideokomprimierung aktiviert sein. Diese Richtlinie ist standardmäßig aktiviert.

Bei Hardware-verschlüsselungsfähigen Webcams verwendet HDX-Videokomprimierung die Hardware-Codierung standardmäßig. Die Hardwarecodierung kann mehr Bandbreite verbrauchen als die Softwarecodierung. Zum Erzwingen der Softwarekomprimierung bearbeiten Sie den Registrierungsschlüssel auf dem Client. Weitere Informationen finden Sie unter Webcamsoftwarekomprimierung in der Liste der Features, die über die Registrierung verwaltet werden.

### Anforderungen für die HDX RealTime-Webcamvideokomprimierung

Die HDX-Webcam-Videokomprimierung unterstützt die folgenden Versionen der Citrix Workspace-App:

| Plattform | Prozessor |
|---|---|
| Citrix Workspace-App für Windows | Die Citrix Workspace-App für Windows unterstützt die Webcam-Videokomprimierung für 32-Bit- und 64-Bit-Apps unter XenApp und XenDesktop 7.17 und höher. Unter früheren Versionen unterstützt die Citrix Workspace-App für Windows nur 32-Bit-Apps. |
| Citrix Workspace-App für Mac | Die Citrix Workspace-App für Mac 2006 und später unterstützt die Webcam-Videokomprimierung für 64-Bit-Apps unter XenApp und XenDesktop 7.17 und höher. Unter früheren Versionen unterstützt die Citrix Workspace-App für Mac nur 32-Bit-Apps. |
| Citrix Workspace-App für Linux | Die Citrix Workspace-App für Linux unterstützt 32-Bit- und 64-Bit-Apps auf dem virtuellen Desktop. |

| Plattform | Prozessor |
| --- | --- |
| Citrix Workspace-App für Chrome | Da manche ARM-Chromebooks die H.264-Codierung nicht unterstützen, können nur 32-Bit-Apps die optimierte HDX-Webcam-Videokomprimierung verwenden. |

Media Foundation-basierte Videoanwendungen unterstützen die HDX-Webcam-Videokomprimierung unter Windows 8.x oder höher und Windows Server 2012 R2 und höher. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX132764.

Andere Anforderungen an Benutzergeräte:

- Geeignete Hardware für die Audiowiedergabe
- DirectShow-kompatible Webcam (Webcam-Standardeinstellungen verwenden). Hardware-codierungsfähige Webcams senken die clientseitige CPU-Auslastung.
- Installieren Sie für die HDX-Webcamvideokomprimierung möglichst die Webcamtreiber des Herstellers auf dem Client. Die Installation der Gerätetreiber ist auf dem Server nicht erforderlich.

Die Bildfrequenz sowie Helligkeits- und Kontraststufen sind bei den einzelnen Webcams unterschiedlich. Die Anpassung des Webcamkontrasts kann den Upstreamverkehr erheblich reduzieren. Citrix verwendet die folgenden Webcams für die Feature-Erstvalidierung:

- Microsoft LifeCam VX (2000, 3000, 5000, 7000)
- Creative Live! Cam Optia Pro
- Logitech QuickCam Messenger
- Logitech C600, C920
- HP Deluxe Webcam

Um die Bildfrequenz anzupassen, bearbeiten Sie den Registrierungsschlüssel auf dem Client. Weitere Informationen finden Sie in der Liste der Features, die über die Registrierung verwaltet werden, unter Bildfrequenz der Webcamvideokomprimierung.

### 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 Videokonferenzanwendung die Wiedergabe in HD unterstützen, wird HD in der Anwendung verwendet. Wir unterstützen alle Webcam-Auflösungen.

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 aktivieren und deaktivieren. Weitere Informationen finden Sie unter HD-Webcamstreaming in der Liste der Features, die über die Registrierung verwaltet werden.

Wenn die Medientypaushandlung fehlschlägt, verwendet HDX die VGA-Standardauflösung (640 x 480 Pixel). Anhand der Registrierungsschlüssel auf dem Client können Sie die Standardauflösung konfigurieren. Stellen Sie sicher, dass die Webcam die angegebene Auflösung unterstützt. Weitere Informationen finden Sie unter HD-Webcamauflösung in der Liste der Features, die über die Registrierung verwaltet werden.

Die HDX-Webcam-Videokomprimierung benötigt im Vergleich zur generischen Plug & Play-USB-Weiterleitung deutlich weniger Bandbreite und funktioniert gut über WAN-Verbindungen. Um die Bandbreite anzupassen, legen Sie den Registrierungsschlüssel auf dem Client fest. Weitere Informationen finden Sie unter HD-Webcambandbreite in der Liste der Features, die über die Registrierung verwaltet werden.

Geben Sie einen Wert in Bits pro Sekunde ein. Wenn Sie die Bandbreite nicht angeben, wird für Videokonferenzanwendungen standardmäßig 350000 Bit/s verwendet.

### Generische HDX-USB-Umleitung für Plug & Play

Die generische HDX-USB-Umleitung für Plug & Play wird auch als **generischer** Webcammodus bezeichnet. Der Vorteil der generischen HDX-USB-Umleitung für Plug & Play 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 auf dem Server 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 and XenDesktop Engineering; CN = Citrix XenApp and 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 and XenDesktop Engineering; CN = Citrix XenApp and 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

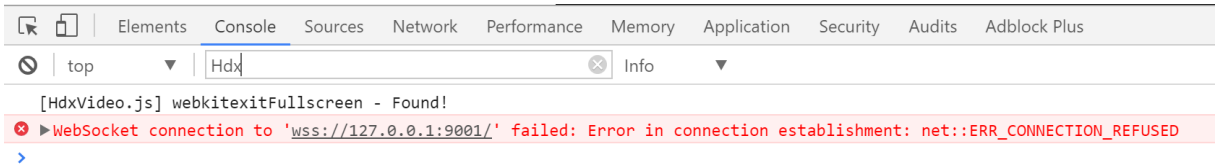
In diesem Release ist dieses Feature nur für Webseiten verfügbar, die unter Ihrer Kontrolle stehen. Die Aktivierung erfordert das Hinzufügen der JavaScript-Datei HdxVideo.js (auf dem Citrix Virtual Apps and Desktops-Installationsmedium enthalten) zu Webseiten mit HTML5-Multimediainhalt. Beispiel: Videos 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

June 27, 2024

> **Hinweis:**
>
> Das neue Microsoft Teams 2.1 ist jetzt allgemein für VDA verfügbar. Diese Microsoft Teams-Version ist mit Citrix Microsoft Teams Optimization unter Verwendung von WebRTC (VDI 1.0) kompatibel.
>
> Ab Citrix Virtual Apps and Desktops 2402 müssen Sie den Registrierungseintrag `msedgewebview2.exe` nicht mehr manuell konfigurieren, da er standardmäßig auf der Positivliste steht.
>
> Veröffentlichte Apps werden jetzt von Microsoft Teams unterstützt.

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 umfasst VDA-seitige HDX-Dienste und eine 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 Multimediainhalte lokal und stellt sie lokal bereit, wobei das Fenster der Citrix Workspace-App in die gehostete Microsoft Teams-App zurückverschoben wird.

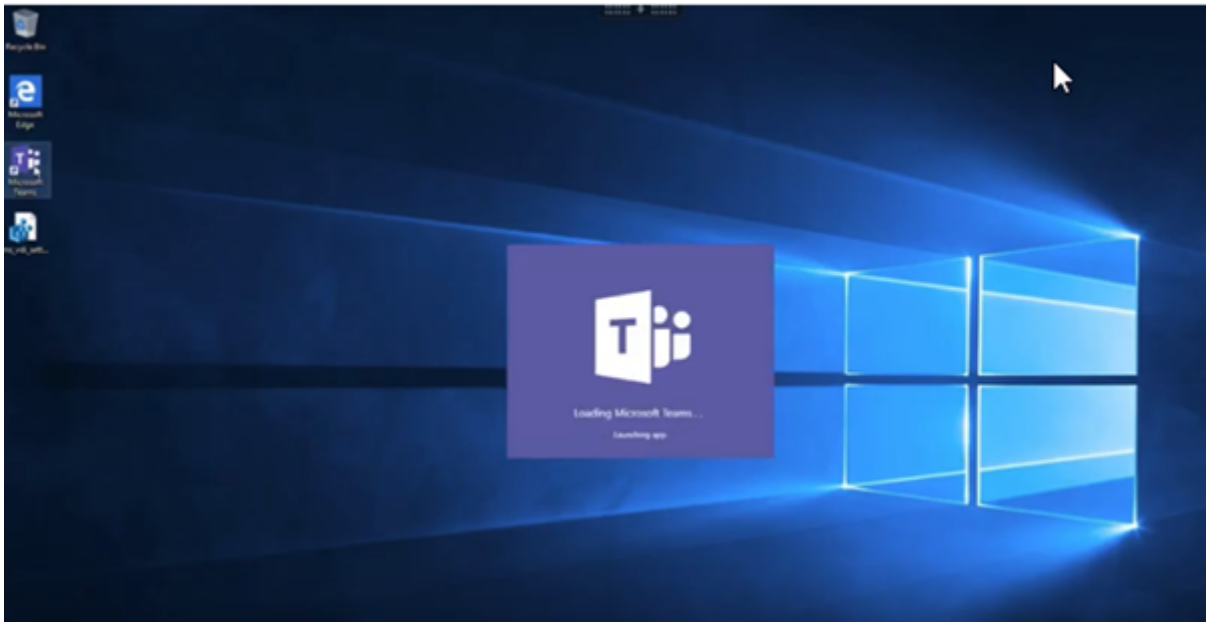
Authentifizierung und Signalisierung erfolgen nativ in der von Microsoft Teams gehosteten App, genau wie die anderen Microsoft Teams-Dienste (zum Beispiel Chat oder Teamarbeit). Die Audio-/Videoumleitung hat auf sie keine Auswirkungen.

`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

Citrix und Microsoft empfehlen, die neueste verfügbare Version von Microsoft Teams zu verwenden und sie auf dem neuesten Stand zu halten.
Versionen der Microsoft Teams Desktop-App mit einem Veröffentlichungsdatum, das mehr als 90 Tage älter als das Veröffentlichungsdatum der aktuellen Version sind, werden nicht unterstützt.
Nicht unterstützte Versionen der Microsoft Teams Desktop-App zeigen Benutzern eine blockierende Seite und fordern zum Update der App auf.

Informationen zu den neuesten verfügbaren Versionen finden Sie unter Updateverlauf für Microsoft Teams App (Desktop und Mac).

Wir empfehlen, den Richtlinien zur maschinenweiten Installation von Microsoft Teams zu folgen. Vermeiden Sie die Verwendung des EXE-Installationsprogramms, mit dem Microsoft 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 Microsoft Teams für alle Benutzer des Computers in der Systemsteuerung unter **Programme und Funktionen** und in der Windows-**Systemsteuerung** angezeigt. Außerdem in **Apps und Features** in den Windows-Einstellungen für alle Benutzer des Computers. Alle Benutzer können Microsoft 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 Microsoft Teams-Anwendung nicht automatisch aktualisiert, sobald eine neue Version vorhanden ist. Wir empfehlen diesen Modus für nicht persistente Umgebungen, z. B. 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).

Angenommen, Sie verfügen über eine dedizierte persistente VDI-Umgebung mit Windows 10. Wenn Sie die Microsoft Teams-Anwendung automatisch aktualisieren und pro Benutzer unter `Appdata/Local` installieren möchten, verwenden Sie das Microsoft Teams-Installationsprogramm oder die MSI. Verwenden Sie in diesem Fall das `.exe`-Installationsprogramm oder die MSI ohne `ALLUSER=1`.

> **Hinweis:**
>
> Citrix empfiehlt, den VDA zu installieren, bevor Microsoft Teams im goldenen Image installiert wird. Diese Installationsreihenfolge ist notwendig, damit das Flag `ALLUSER=1` wirksam wird. Wenn Sie Microsoft Teams vor dem VDA auf der virtuellen Maschine installiert haben, deinstallieren Sie Microsoft Teams und installieren Sie es neu.

### Remote-PC-Zugriff

Citrix empfiehlt die Installation von Microsoft Teams Version 1.4.00.22472 oder höher, nachdem Sie den VDA installiert haben. Andernfalls müssen Sie sich abmelden und erneut anmelden, damit Microsoft Teams den VDA wie erwartet erkennen kann. Version 1.4.00.22472 und später enthält erweiterte Logik, die zur Startzeit von Microsoft Teams und zur Anmeldezeit für die VDA-Erkennung ausgeführt wird. Diese Versionen enthalten auch eine Identifizierung des aktiven Sitzungstyps (HDX, RDP oder lokal mit dem Clientcomputer verbunden). Wenn Sie lokal verbunden sind, können frühere Versionen von Microsoft Teams bestimmte Features oder UI-Elemente möglicherweise nicht erkennen und deaktivieren. Beispiele: separate Räume, Pop-Out-Fenster für Besprechungen und Chats oder Reaktionen in Besprechungen.

> **Wichtig:**
>
> Wenn Sie von einer lokalen Sitzung zu einer HDX-Sitzung wechseln und Microsoft Teams geöffnet bleibt und im Hintergrund ausgeführt wird, müssen Sie Microsoft Teams beenden und neu starten, um die Optimierung mit HDX korrekt zu ermöglichen.
> Wenn Sie dagegen Microsoft Teams remote über eine optimierte HDX-Sitzung verwenden,

> trennen Sie die HDX-Sitzung und stellen Sie die Verbindung lokal auf dem Gerät zu derselben Windows-Sitzung wieder her. Wenn Sie im Büro arbeiten, müssen Sie Microsoft Teams neu starten, damit es den Remote-PC-Zugriff-Zustand (HDX oder lokal) korrekt erkennen kann. Microsoft Teams kann den VDI-Modus nur zum Zeitpunkt des App-Starts bewerten und nicht, während es bereits im Hintergrund ausgeführt wird. Ohne einen Neustart kann Microsoft Teams möglicherweise Funktionen wie Pop-Out-Fenster, Gruppenräume oder Besprechungsreaktionen nicht laden.

### App Layering

Wenn Sie Citrix App Layering zum Verwalten von VDA- und Microsoft Teams-Installationen auf verschiedenen Layern verwenden, müssen Sie einen Registrierungsschlüssel auf Windows-VDAs erstellen, bevor Sie Microsoft Teams mit dem Flag `ALLUSER=1` über die Befehlszeile installieren. Weitere Informationen finden Sie im Abschnitt *Optimierung für Microsoft Teams mit Citrix App Layering* unter Multimedia.

### 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 Microsoft 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.

> **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 für die maschinenweite Installation

Im Folgenden finden Sie ein Beispiel für Ordner, Desktopverknüpfungen und Registrierungen, die bei der Installation von Microsoft Teams mit dem Installationsprogramm für die maschinenweite Installa-

tion 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`
- Name:`Teams`
- Typ: `REG_SZ`
- Wert: `C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe`

> **Hinweis:**
>
> Das Registrierungsverzeichnis variiert je nach den zugrunde liegenden Betriebssystemen und der Bitanzahl.

#### Empfehlungen

- Es wird empfohlen, den automatischen Start durch Löschen der Microsoft Teams-Registrierungsschlüssel zu deaktivieren. Dadurch wird verhindert, dass viele gleichzeitige Anmeldungen (z. B. zu Beginn des Arbeitstags) die CPU der VM überlasten.
- Wenn der virtuelle Desktop keinen GPU/vGPU hat, wird empfohlen, die Einstellung **GPU-Hardwarebeschleunigung deaktivieren** in den **Einstellungen** von Microsoft Teams festzulegen, um die Leistung zu verbessern. Diese Einstellung (`"disableGpu":true`) wird in `%Appdata%\Microsoft\Teams` in `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 Microsoft Teams zu verwalten.

#### Installationsprogramm pro Benutzer

Bei Verwendung des `.exe`-Installationsprogramms verläuft die Installation anders. Alle Dateien werden unter AppData abgelegt.

*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 Microsoft Teams mit flüchtigem Setup erfordert einen Profilcaching-Manager für die effiziente Synchronisierung der Microsoft Teams-Laufzeitdaten. Mit einem Profilcaching-Manager werden die richtigen benutzerspezifischen Informationen während der Benutzersitzung zwischengespeichert. Zu den benutzerspezifischen Informationen gehören beispielsweise Benutzerdaten, Profil und Einstellungen. Synchronisieren Sie die Daten in den folgenden beiden Ordnern:

- C:\Users\<username>\AppData\Local\Microsoft\IdentityCache
- C:\Users\<username>\AppData\Roaming\Microsoft\Teams

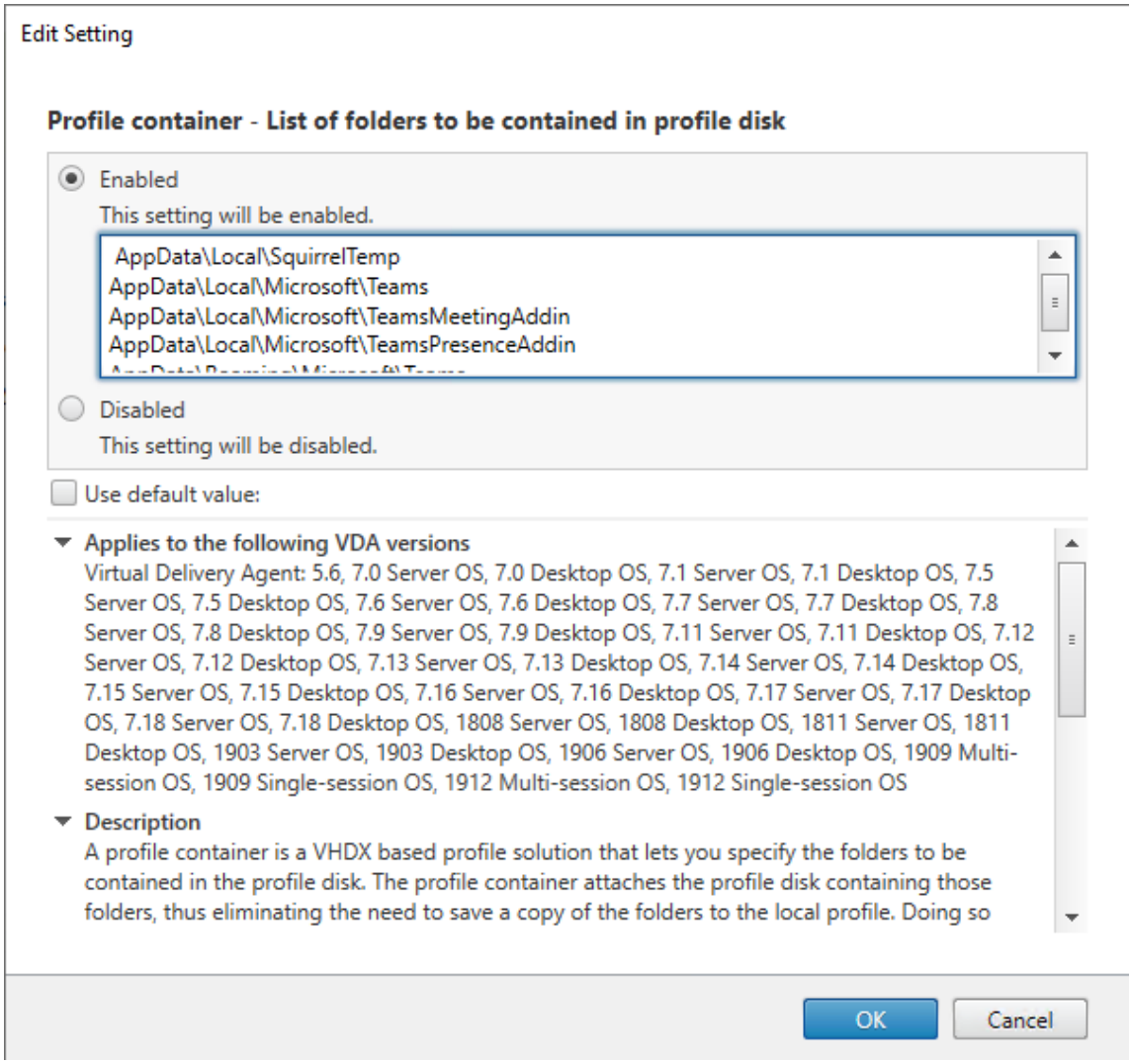
**Ausschlussliste für zwischengespeicherte Microsoft Teams-Inhalte bei beständigem Setup**
Schließen Sie die Dateien und Verzeichnisse aus dem Caching-Ordner von Microsoft Teams aus, wie in der Microsoft-Dokumentation beschrieben. Dadurch wird die Größe des Benutzercaches reduziert und das flüchtige Setup weiter optimiert.

**Anwendungsfall: Einzelsitzung** In diesem Szenario verwendet der Endbenutzer Microsoft Teams an einem Ort. Microsoft Teams muss nicht in zwei Windows-Sitzungen gleichzeitig ausgeführt werden. Gewöhnlich wird jedem Benutzer ein virtueller Desktop zugewiesen und Microsoft Teams im virtuellen Desktop als Anwendung bereitgestellt.
Wir empfehlen, Citrix Profilcontainer zu aktivieren und die unter Installationsprogramm pro Benutzer aufgeführten 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 Benutzerverzeichnisse enthalten. Sie können 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 (DDCs) 1906.2

Wenn Sie eine frühere Version verwenden, lesen Sie den Artikel Aktivieren der Optimierung für Microsoft Teams:

Unterstützte Betriebssysteme:

- Windows Server 2022, Windows Server 2019, 2016, 2012R2 Standard und Datacenter Edition und mit der Server Core-Option

### Mindestversion –Virtual Delivery Agents (VDAs) 1906.2

Unterstützte Betriebssysteme:

- Windows 11
- Windows 10 64-Bit, ab Version 1607. VM-gehostete Apps werden von der Citrix Workspace-App für Windows ab Version 2109.1 unterstützt
- Windows Server 2022, 2019, 2016 und 2012 R2 (Standard und Data Center 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 für Windows, neuestes Release und Mindestversion –Citrix Workspace-App 1907 für Windows

- Windows 11.
- Windows 10 (32-Bit- und 64-Bit-Editionen, einschließlich Embedded-Editionen) (Unterstützung für Windows 7 wurde ab Version 2006 eingestellt) (Unterstützung für Windows 8.1 wurde ab Version 2204.1 eingestellt).
- Windows 10 IoT Enterprise 2016 LTSB (v1607) und 2019 LTSC (v1809).
- Unterstützte Prozessorarchitekturen: x86 und x64 (ARM wird nicht unterstützt).
- Endpunktanforderung: 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 und AIO.

- 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.
- Die Mindestanforderung für Microsoft .NET Framework ist Version 4.8. Die Citrix Workspace-App lädt das .NET Framework automatisch herunter und installiert es, wenn es nicht vorhanden ist.

Administratoren können den Start von Microsoft Teams im optimiertem Modus über die Richtlinie zur Microsoft Teams-Optimierung aktivieren und deaktivieren. Beim Start in der Citrix Workspace-App im optimierten Modus kann Microsoft Teams nicht deaktiviert werden.

**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
- `libnsl`
- Ubuntu 20.04 oder höher

Verbesserung der Authentifizierung:

- Libsecret-Bibliothek
- libunwind-12 library. Weitere Informationen finden Sie unter Hinzufügen der Abhängigkeit "libunwind-12 library"für llvm-12.

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

Eine vollständige Liste aller geprüften Endpunkte finden Sie unter Thin Clients.

Weitere Informationen finden Sie unter Voraussetzungen für die Installation der Citrix Workspace-App.

Sie können die Microsoft Teams-Optimierung deaktivieren, indem Sie den Wert des Felds **VDWEBRTC** in der Datei `/opt/Citrix/ICAClient/config/module.ini` auf "Off"festlegen. Der

Standardwert ist VDWEBRTC=On. Nachdem das Update abgeschlossen ist, starten Sie die Sitzung neu. (Rootberechtigungen erforderlich)

#### Mindestversion –Citrix Workspace-App 2012 für Mac

Unterstützte Betriebssysteme:

- macOS Catalina (10.15).
- macOS Big Sur 11.0.1 und später.
- macOS Monterey.

Unterstützte Features:

- Audio
- Video
- Optimierung der Bildschirmfreigabe (eingehend und ausgehend)

> **Hinweis:**
>
> Die Citrix Viewer-App benötigt Zugriff auf die Einstellungen für macOS-Sicherheit und Datenschutz, damit die Bildschirmfreigabe funktioniert. Die Benutzer konfigurieren diese Einstellung unter **Apple-Menü > Systemeinstellungen > Sicherheit & Datenschutz > Bildschirmaufzeichnung** und wählen **Citrix Viewer**.

Die Optimierung für Microsoft Teams ist bei Verwendung der Citrix Workspace-App 2012 oder später und von macOS 10.15 standardmäßig aktiviert.

Um die Optimierung für Microsoft Teams zu deaktivieren, führen Sie diesen Befehl in einem Terminal aus und starten die Citrix Workspace-App neu:

```
defaults write com.citrix.receiver.nomas mtopEnabled -bool NO
```

#### Mindestversion: Neueste Version der Citrix Workspace-App für ChromeOS wird auf der neuesten Version von ChromeOS ausgeführt

Hardware:

- Prozessoren mit gleichwertiger oder besserer Leistung als Intel i3, Quad Core 2,4 GHz.

Unterstützte Features:

- Audio
- Video
- Optimierung der Bildschirmfreigabe (ein- und ausgehend) - standardmäßig deaktiviert. In diesen Einstellungen finden Sie Anweisungen zum Aktivieren.

## Skalierbarkeit einzelner Server

Dieser Abschnitt enthält Empfehlungen und Orientierung zur Schätzung der Zahl der Benutzer bzw. virtuellen Maschinen (VMs), die auf einem einzelnen physischen Host unterstützt werden können. Dies wird in der Regel als SSS (Citrix Virtual Apps and Desktops Single Server Scalability) bezeichnet. Im Zusammenhang mit Citrix Virtual Apps (CVA) oder der Sitzungsvirtualisierung wird es allgemein auch als Benutzerdichte bezeichnet. Es geht darum herauszufinden, wie viele Benutzer oder VMs auf einer Hardware mit einem größeren Hypervisor ausgeführt werden können.

> **Hinweis:**
>
> Dieser Abschnitt enthält Orientierung zur Schätzung der SSS. Es geht darum um allgemeine Empfehlungen, die sich nicht unbedingt komplett auf Ihre spezifische Situation bzw. Umgebung anwenden lassen. Citrix Virtual Apps and Desktops-SSS kann nur mit einem Tool für Skalierbarkeitstests oder Lasttests wie Login VSI genau ermittelt werden. Citrix empfiehlt die Verwendung der vorliegenden Empfehlungen nur für schnelle SSS-Schätzungen. Citrix empfiehlt aber, die Ergebnisse insbesondere vor dem Kauf von Hardware oder dem Treffen finanzieller Entscheidungen mit Login VSI oder einem Lasttest-Tool Ihrer Wahl zu validieren.

### Hardware (Testsystem)

- Dell PowerEdge R740
- Intel Xeon (Gold) 6126 mit 2,60 GHz (max. Turbo 3,70 GHz), 12 Kerne pro Sockel, Dual-Sockel mit aktiviertem Hyperthreading
- 382 GB RAM
- Lokaler SSD RAID 0-Speicher (11 Datenträger) 6 TB

### Software

Eine virtuelle Maschine (40 logische Prozessoren) mit Windows 2019 (TSVDA) und Citrix Virtual Apps and Desktops 2106
VMware ESXi 6.7

### Terminologie

- Wissensarbeiter-Workload: Umfasst Acrobat Reader, Freemind-/Java-, Fotoviewer-, Edge- und MS Office-Apps (z. B. Excel, Outlook, PowerPoint und Word).
- Baseline: Serverskalierbarkeitstests mit Wissensarbeiter-Workload (ohne Microsoft Teams).
- Microsoft Teams-Workload: Typische Wissensarbeiter-Workload + Microsoft Teams.

**Belastungstestmethode für Microsoft Teams**

- Microsoft Teams ist HDX-optimiert. Daher wird die gesamte Multimedia-Verarbeitung auf den Endpunkt oder Client abgeladen und ist nicht Teil der Messung.
- Alle Microsoft Teams-Prozesse werden gestoppt oder beendet, bevor die Workload startet.
- Öffnen Sie Microsoft Teams (Kaltstart).
- Messen Sie die Zeit, die zum Laden benötigt wird, und aktivieren Sie den Fokus des Microsoft Teams-Hauptfensters.
- Wechseln Sie per Tastenkombination zum Chatfenster.
- Wechseln Sie per Tastenkombination zum Kalenderfenster.
- Senden Sie eine Chat-Nachricht per Tastenkombinationen an einen Benutzer.
- Wechseln Sie per Tastenkombination zum Microsoft Teams-Fenster.

**Ergebnisse**

- 40 % Skalierbarkeitsauswirkung bei Microsoft Teams-Workload (81 Benutzer) im Vergleich zur Baseline (137 Benutzer).
- Durch eine Erhöhung der Serverkapazität (CPU) um ca. 40 % wird die Benutzeranzahl der Baseline-Workload wieder erreicht.
- 20 % zusätzlicher Arbeitsspeicher bei Microsoft Teams-Workload im Vergleich zur Baseline erforderlich.
- Erhöhen Sie die Speichergröße pro Benutzer um 512 bis 1024 MB.
- Ca. 50 % mehr IOPS-Schreibvorgänge, ca. 100 % mehr IOPS-Lesevorgänge. Microsoft Teams kann in einer Umgebung mit langsamerem Speicher erhebliche Auswirkungen haben.

## Featurematrix und Versionsunterstützung

| Feature | Microsoft Teams (Mindestversion) | VDA (Mindestversion) | Citrix Workspace-App für Windows (Mindestversion) | Citrix Workspace-App für Mac (Mindestversion) | Citrix Workspace-App für Linux (Mindestversion) | Citrix Workspace-App für ChromeOS (Mindestversion) |
|---|---|---|---|---|---|---|
| Audio/Video (P2P und Konferenz) | Aktuelle Version minus 90 Tage | 1906 | 1907 | 2009 | 2004 | 2105.5 |

| Feature | Microsoft Teams (Mindestversion) | VDA (Mindestversion) | Citrix Workspace-App für Windows (Mindestversion) | Citrix Workspace-App für Mac (Mindestversion) | Citrix Workspace-App für Linux (Mindestversion) | Citrix Workspace-App für ChromeOS (Mindestversion) |
|---|---|---|---|---|---|---|
| Bildschirmfreigabe | Aktuelle Version minus 90 Tage | 1906 | 1907 | 2012 | 2006 | 2105.5 |
| i. Roter Rahmen für Bildschirmanzeige | Aktuelle Version minus 90 Tage | 1906 | 2002 | 2012 | 2006 | Nein |
| ii. Erfassung auf Desktop Viewer beschränken | Aktuelle Version minus 90 Tage | 1906 | 2009.5 | 2012 | 2006 | Nein |
| iii. Mehrere Monitore | Aktuelle Version minus 90 Tage | 1912 CU6+ | 2106 (1) | 2106 | 2106 | Nein |
| Mehrfrequenzwahlverfahren | Aktuelle Version minus 90 Tage | – | 2102 | 2101 | 2101 | 2111.1 |
| Proxyserverunterstützung | Aktuelle Version minus 90 Tage | – | 2012 (2) | 2104 (3) | 2101 (3) | 2305 |
| App-Freigabe | Aktuelle Version minus 90 Tage | 2109 | 2109.1 | 2203.1 | 2209 | Nein |

| Feature | Microsoft Teams (Mindestversion) | VDA (Mindestversion) | Citrix Workspace-App für Windows (Mindestversion) | Citrix Workspace-App für Mac (Mindestversion) | Citrix Workspace-App für Linux (Mindestversion) | Citrix Workspace-App für ChromeOS (Mindestversion) |
|---|---|---|---|---|---|---|
| Liveuntertitel | Aktuelle Version minus 90 Tage | –(4) | 2109.1 | 2109 | 2109 | 2303 |
| Dynamisches e911 | Aktuelle Version minus 90 Tage | – | 2112.1 | 2112 | 2112 | 2112 |
| Steuerung übergeben | Aktuelle Version minus 90 Tage | – | 2112.1 | 2203.1 | Nein | Nein |
| Steuerung anfordern | Aktuelle Version minus 90 Tage | – | 2112.1 | 2203.1 | 2203 | 2303 |
| Mehrfenstermodus | 1.5.00.11865 | 2112, 1912 CU6 (5) | 2112.1 | 2203.1 | 2203 | 2303 |
| Besprechungstranskription | Aktuelle Version minus 90 Tage | 2112.1, 1912 CU6+ | 2112 | 2203.1 | 2203 | 2303 |
| Hintergrundunschärfe | Aktuelle Version minus 90 Tage | 2112, 1912 CU6+ | 2207 | 2301 | 2212 | 2303 |

1. CD-Viewer nur im Vollbildmodus. UMSCHALT+F2 wird nicht unterstützt.
2. Negotiate/Kerberos, NTLM, Basic und Digest. Pac-Dateien werden ebenfalls unterstützt.
3. Nur anonym.
4. Wenn die VDA-Version 2112 oder höher ist, funktionieren Liveuntertitel nur, wenn die Citrix Workspace-App-Version 2203.1 für MAC und 2203 Linux oder 2112 für Windows ist. Dies liegt

daran, dass sich Liveuntertitel unterschiedlich verhalten, wenn Microsoft Teams im Einzel- oder im Mehrfenstermodus ist.

5. Der Mehrfenstermodus wurde mit VDA 2112 eingeführt, aber auf die Version VDA 1912 LTSR CU6 zurückportiert.

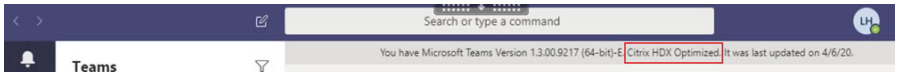
> **Hinweis:**
>
> - Alle unter **Citrix Workspace-App für Windows 1912 CU6 (oder höher)** aufgeführten Features gelten für die Citrix Workspace-App für Windows 2203.1 LTSR CU1.
> - Microsoft hat die Unterstützung für den Einzelfenstermodus in Microsoft Teams eingestellt. Um die Anforderungen zu erfüllen, müssen Sie Ihren VDA auf 1912 CU6+ LTSR und die Citrix Workspace-App auf 2203 CU2+ oder höher aktualisieren. Dies unterstützt den Mehrfenstermodus.

### Aktivieren der Optimierung für Microsoft Teams

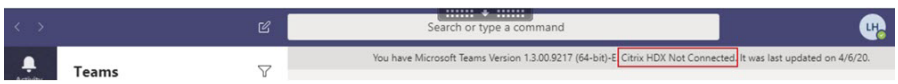
Verwenden Sie die unter Microsoft Teams-Umleitung beschriebene Richtlinie der Verwaltungskonsole, um die Optimierung für Microsoft Teams zu aktivieren. Diese Richtlinie ist standardmäßig auf **EIN** festgelegt. Zusätzlich zu der Aktivierung dieser Richtlinie überprüft HDX, ob die Version der Citrix Workspace-App 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** 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 später mit älteren Controller-Versionen (z. B. Version 7.15) verwenden, für die die Richtlinie in der Verwaltungskonsole (Studio) nicht verfügbar ist, ist die Optimierung des VDA immer noch möglich. Die HDX-Optimierung für Microsoft Teams ist im VDA standardmäßig aktiviert.

Wenn Sie auf **Info > Version** klicken, wird die Legende **Citrix HDX Optimized** angezeigt:

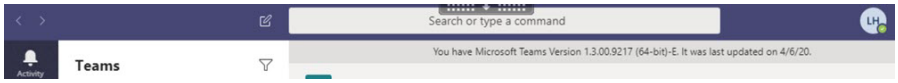



Wenn **Citrix HDX Not Connected** angezeigt wird, wurde die Citrix API in Microsoft Teams geladen. Das Laden der API ist der erste Schritt der Umleitung. In den nachfolgenden Teilen des Stacks ist ein Fehler aufgetreten. Der Fehler trat höchstwahrscheinlich in VDA-Diensten oder der Citrix Workspace-App auf.



Wenn keine Legende angezeigt wird, konnte Microsoft Teams die Citrix API nicht laden. Klicken Sie mit der rechten Maustaste auf das Symbol für den Infobereich, um Microsoft Teams zu beenden und neu starten. Vergewissern Sie sich, dass die Richtlinie der Verwaltungskonsole nicht auf **Nicht zugelassen** festgelegt ist und dass die Citrix Workspace-App-Version unterstützt wird.




**Wichtig: Sitzungswiederverbindung**

- Möglicherweise müssen Sie Microsoft Teams neu starten, um eine Sitzung mit HDX-Optimierung zu erhalten, wenn sich die Konnektivität ändert. Beispiel: beim Roaming von einem nicht unterstützten Endpunkt (Workspace-App für iOS, Android oder alte Versionen von Windows/Linux/Mac) zu einem unterstützten Endpunkt (Workspace-App für Windows/Linux/Mac/ChromeOS/HTML5) oder umgekehrt.
- Ein Neustart von Microsoft Teams ist auch dann erforderlich, wenn Sie die App im VDA mit dem EXE-Installationsprogramm für Microsoft Teams installiert haben. Das EXE-Installationsprogramm wird für persistente VDI-Bereitstellungen empfohlen. In solchen Fällen kann Microsoft Teams automatische Updates durchführen, während sich die HDX-Sitzung im getrennten Zustand befindet. Benutzer, die sich erneut mit einer HDX-Sitzung verbinden, stellen also fest, dass Microsoft Teams nicht optimiert ausgeführt wird.
- Beim Roaming von einer lokalen Sitzung zu einer HDX-Sitzung müssen Sie Microsoft Teams neu starten, um HDX-Optimierung zu erreichen. Diese Aktion ist bei Remote-PC-Zugriff erforderlich.

### Netzwerkanforderungen

Microsoft Teams benötigt Medienprozessor-Server unter Microsoft 365 für Besprechungen oder Anrufe mit mehreren Teilnehmern. Microsoft Teams benötigt außerdem Microsoft 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 Microsoft 365-Cloud ab. Ausführliche Richtlinien zur Netzwerkplanung finden Sie in den Prinzipien von Microsoft 365-Netzwerkverbindungen.

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 Microsoft 365-Netzwerk her.
- Sie müssen ausreichend Bandbreite für die Zweigstelle einplanen und bereitstellen.
- Überprüfen Sie Qualität und Konnektivität des Netzwerks für jede Zweigstelle.
- Wenn Sie folgende Funktionen in der Zweigstelle verwenden, muss der RTP/UDP Teams-Verkehr (von HdxRtcEngine.exe in der Citrix Workspace-App behandelt) ungehindert erfolgen.
  - Proxyserver umgehen
  - Netzwerk-SSL abfangen
  - DPI-Geräte (Deep Packet Inspection)
  - VPN-Hairpins (nach Möglichkeit Split-Tunneling verwenden)

> **Wichtig: VPN-Split-Tunnelkonfiguration**
>
> Der Datenverkehr von HdxRtcEngine.exe muss vom VPN-Tunnel umgeleitet werden und in der Lage sein, über die lokale Internetverbindung des Benutzers eine direkte Verbindung zum Dienst herzustellen. Wie dies erreicht wird, hängt vom verwendeten VPN-Produkt und der verwendeten Maschinenplattform ab; die meisten VPN-Lösungen ermöglichen jedoch eine einfache Konfiguration der Richtlinie, um diese Logik anzuwenden. Weitere Hinweise zum Festlegen der VPN-spezifischen Split-Tunnelkonfiguration finden Sie in diesem Microsoft-Artikel.

Die WebRTC Media Engine in der Workspace-App (HdxRtcEngine.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. Für dieses Feature werden mit DTLS ausgehandelte, symmetrische Schlüssel zum Verschlüsseln von Medien verwendet und Nachrichten unter Verwendung der AES-Verschlüsselung gesteuert.

Folgende Metriken werden für eine positive Benutzererfahrung empfohlen:

| Metrik | Endpunkt zu Microsoft 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.

Für Bandbreitenanforderungen kann die Optimierung für Microsoft Teams eine Vielzahl von Codecs für Audio (OPUS/G.722/PCM G711) und Video (H264) 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 |
| 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 H264 sind die bevorzugten Codecs für Peer-to-Peer-Anrufe und Telefonkonferenzen.

> **Wichtig:**
>
> Codierung nimmt mehr CPU-Leistung in Anspruch als die Decodierung auf dem Clientcomputer. Sie können die maximal mögliche Codierungsauflösung in der Citrix Workspace-App für Linux und Windows fest codieren. Siehe Geschätzte Codierungsleistung und Geschätzte Codierungsleistung für Microsoft Teams.

### 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 `127.0.0.1:9002` umgehen.

  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 Internetzugriff über einen Proxy konfiguriert ist, unterstützen folgende Versionen Proxyserver:

  - Citrix Workspace-App für Windows Version 2012 (Negotiate/Kerberos, NTLM, Basic und Digest. `Pac`-Dateien werden ebenfalls unterstützt.)
  - Citrix Workspace-App für Windows Version 1912 CU5 (Negotiate/Kerberos, NTLM, Basic und Digest. `Pac`-Dateien werden ebenfalls unterstützt.)
  - Citrix Workspace-App für Linux Version 2101 (anonyme Authentifizierung)
  - Citrix Workspace-App für Mac Version 2104 (anonyme Authentifizierung)

Clientgeräte mit früheren Releases der Citrix Workspace-App können keine Proxykonfigurationen lesen. Diese Geräte senden Datenverkehr direkt an Microsoft 365 TURN-Server.

> **Wichtig:**
>
> - Vergewissern Sie sich, dass das Clientgerät für die DNS-Auflösung eine Verbindung zum DNS-Server herstellen kann. Ein Clientgerät muss die folgenden FQDNs des Microsoft Teams Relay-Servers auflösen können:
>
>   ```
>   - worldaz.relay.teams.microsoft.com
>   - inaz.relay.teams.microsoft.com
>   - uaeaz.relay.teams.microsoft.com
>   - euaz.relay.teams.microsoft.com
>   - usaz.relay.teams.microsoft.com
>   - turn.dod.teams.microsoft.us
>   - turn.gov.teams.microsoft.us
>   ```
>
> Wenn DNS-Anfragen nicht erfolgreich sind, schlagen P2P-Anrufe bei externen Benutzern und Telefonkonferenzen mit Medieneinrichtung fehl.
>
> - Der Standort des Konferenzservers wird gemäß dem Standort des virtuellen Desktops des ersten Teilnehmers (und nicht des Clients) ausgewählt.

### Anrufeinrichtung und Medienflusspfad

Wenn möglich, versucht die HDX WebRTC Media Engine in der Citrix Workspace-App (HdxRtcEngine.exe), eine direkte Netzwerkverbindung mit SRTP über UDP in einem Peer-to-Peer-Anruf herzustellen. Wenn die UDP-High-Ports blockiert sind, fällt die Media Engine auf TCP/TLS 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. Der Endpunkt muss daher in der Lage sein, DNS-Auflösungen durchzuführen.

Angenommen, es gibt keinen direkten Pfad zwischen den beiden Peers bzw. zwischen einem Peer und einem Konferenzserver, wenn Sie einem Anruf oder einer Besprechung mit mehreren Teilnehmern beitreten. HdxRtcEngine.exe verwendet einen Microsoft Teams-Transportrelayserver in Microsoft 365, um den anderen Peer bzw. den Medienprozessor zu erreichen, auf dem Besprechungen gehostet werden. Ihr Clientcomputer muss Zugriff auf drei Microsoft 365-Subnetz-IP-Adressbereiche und vier UDP-Ports haben (oder TCP/TLS 443 als Fallback, wenn UDP gesperrt ist). Weitere Informationen finden Sie im Architekturdiagramm im Call Setup und 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, 52.122.0.0/15 | **UDP:** 3478, 3479, 3480, 3481, **TCP:** 443 (Fallback) |

Diese Bereiche enthalten Transport-Relays und Medienprozessoren mit einem Azure Load Balancer-Front-End.
Microsoft Teams Transport-Relays bieten die Funktionen STUN und TURN, sie sind aber keine ICE-Endpunkte. Microsoft Teams Transport-Relays beenden auch keine Medien, TLS und führen keine Transcodierung durch. Relays können als Bridge zwischen TCP (wenn HdxRtcEngine.exe TCP verwendet) und UDP fungieren, wenn sie den Datenverkehr an andere Peers oder Medienprozessoren weiterleiten.

Die WebRTC Media Engine der Workspace-App kontaktiert das nächstgelegene Microsoft Teams Transport-Relay in der Microsoft 365-Cloud. Die Media Engine verwendet Anycast-IP und Port 3478-3481 UDP (verschiedene UDP-Ports pro Workload, wobei Multiplexing möglich ist) oder 443 TCP/TLS 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.

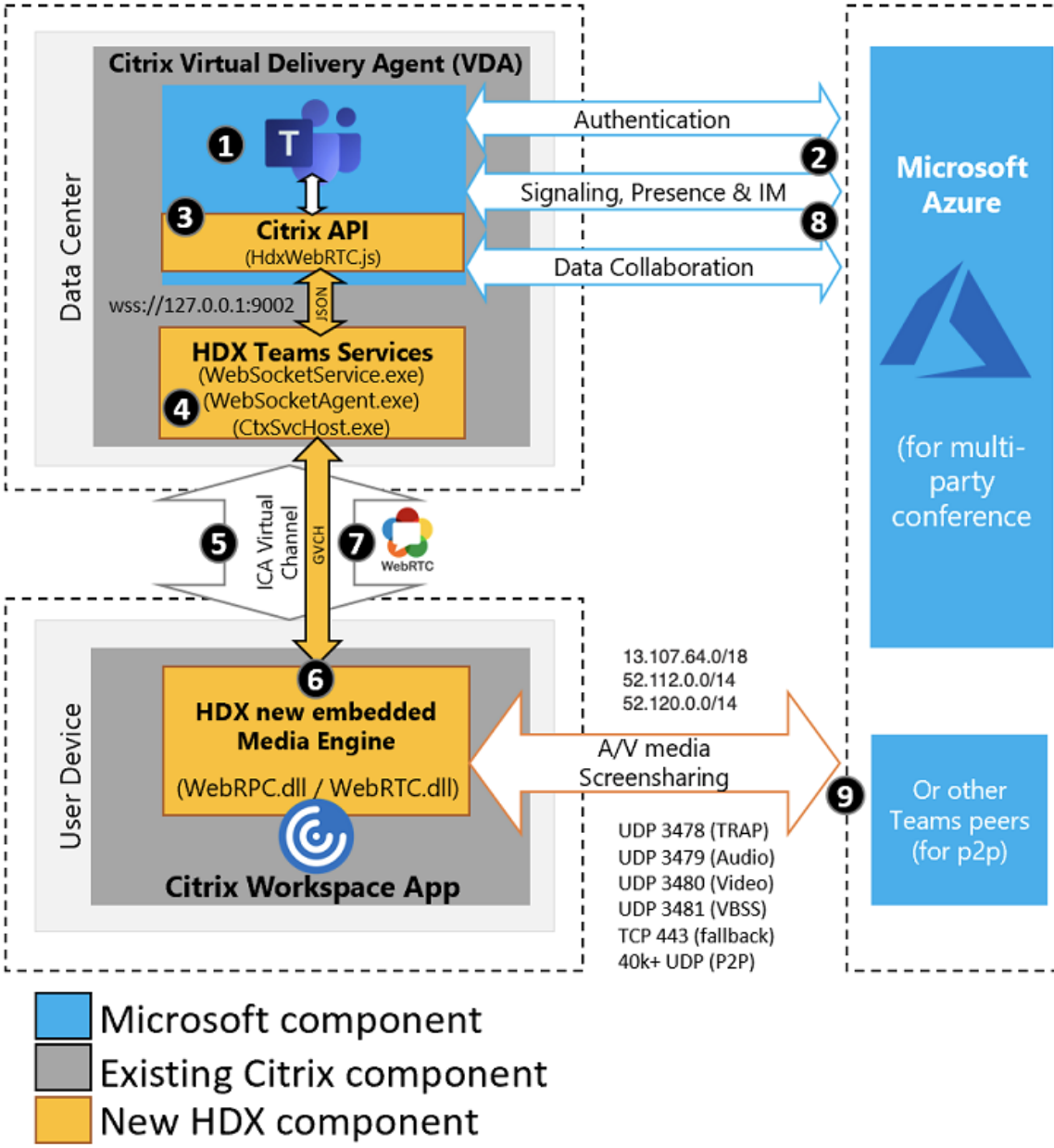
Wurde Microsoft Teams im optimierten Modus geladen und wird HdxRtcEngine.exe auf dem Endpunkt ausgeführt, können ICE-Fehler dazu führen, dass bei der Anrufeinrichtung ein Fehler auftritt oder Audio-/Video-Daten nur in einer Richtung übertragen werden. Wenn ein Anruf nicht zustande kommt oder der Medienfluss keinen vollen Duplexmodus bietet, sollten Sie zuerst die **Wireshark-Trace** auf dem Endpunkt prüfen. Weitere Informationen zum Sammeln von ICE-Kandidaten finden Sie unter “Sammeln von Protokollen”im Abschnitt Support.

> **Hinweis:**
>
> Wenn die Endpunkte keinen Internetzugriff haben, können Benutzer unter Umständen dennoch einen Peer-to-Peer-Anruf tätigen, wenn beide in demselben LAN sind. 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. Sie starten Microsoft Teams.
2. Microsoft Teams authentifiziert sich bei O365. Mandantenrichtlinien werden an den Microsoft Teams-Client übertragen, und relevante TURN- und Signalkanalinformationen werden an die App weitergeleitet.

3. Microsoft Teams erkennt, dass es in einem VDA ausgeführt wird, und sendet API-Aufrufe an die Citrix JavaScript-API.
4. Citrix JavaScript in Microsoft Teams öffnet eine sichere WebSocket-Verbindung zu WebSocketService.exe, das auf dem VDA ausgeführt wird. Dies generiert WebSocketAgent.exe in der Benutzersitzung.
5. WebSocketAgent.exe instanziiert einen generischen virtuellen Kanal, indem es den Citrix HDX-Microsoft Teams-Umleitungsdienst (CtxSvcHost.exe) aufruft.
6. Die HDX-Engine der Citrix Workspace-App (wfica32.exe) erzeugt einen neuen Prozess namens HdxRtcEngine.exe. Dies ist die neue WebRTC-Engine, die für die Optimierung für Microsoft Teams verwendet wird.
7. Die Citrix Media Engine 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 Microsoft Teams-Diensten in Microsoft 365, die einen End-to-End-Signalpfad mit **Peer B** einrichten. Microsoft Teams schickt eine Anfrage an HdxRtcEngine 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 Microsoft Teams-Dienste in Microsoft 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). Anschließend erfolgt der Medienfluss per SRTP (Secure Real-Time Transport Protocol) direkt zwischen HdxRtcEngine.exe und dem anderen Peer (oder Microsoft 365-Konferenzservern im Falle einer Besprechung).

### Microsoft-Telefonsystem

Das Microsoft-Telefonsystem aktiviert die Anrufsteuerung und PBX in der Microsoft 365-Cloud mit Microsoft Teams. Die Optimierung für Microsoft Teams unterstützt Microsoft Phone System mit Microsoft 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.
Anrufwarteschlangen, Übertragen, Weiterleiten, Halten, Stummschalten und Fortsetzen eines Anrufs werden unterstützt.

### Mehrfrequenzwahlverfahren

Das Mehrfrequenzwahlverfahren (DTMF) wird ab den folgenden Versionen der Citrix Workspace-App unterstützt:

- Citrix Workspace-App für Windows Version 2102
- Citrix Workspace-App für Windows LTSR 1912 CU5 (nur Windows 10)
- Citrix Workspace-App für Linux, Version 2101
- Citrix Workspace-App für Mac Version 2101
- Citrix Workspace-App für ChromeOS Version 2111.1

### Unterstützung für dynamischen Notruf

Ab Version 2112 unterstützt die Citrix Workspace-App den dynamischen Notruf. Wenn Sie Microsoft-Anrufpläne, Operator Connect und Direct Routing verwenden, haben Sie folgende Möglichkeiten:

- Konfigurieren und Übermitteln von Notrufen.
- Benachrichtigen von Sicherheitspersonal.

Die Benachrichtigung erfolgt basierend auf dem aktuellen Standort der Citrix Workspace-App auf dem Endpunkt anstelle des Microsoft Teams-Clients, der auf dem VDA ausgeführt wird.

Das US-Gesetz (Ray Baum's Law) schreibt vor, dass der Standort des Notrufanrufers an die entsprechende Einsatzleitstelle (PSAP) übertragen wird. Die Microsoft Teams-Optimierung mit HDX erfüllt die Bestimmungen des Gesetzes Ray Baum's Law bei Nutzung mit folgenden Citrix Workspace-App-Versionen:

- Citrix Workspace-App für Windows Version 2112.1 und später
- Citrix Workspace-App für Linux, Version 2112 und später
- Citrix Workspace-App für Mac Version 2112 und später
- Citrix Workspace-App für ChromeOS Version 2112 und später

Zum Ermöglichen dynamischer Notrufe muss der Administrator im Microsoft Teams Admin Center Folgendes zur Erstellung einer Netzwerk- oder Notfallstandortkarte konfigurieren:

- Netzwerkeinstellungen
- Standortinformationsdienst (LIS)

Weitere Informationen zu dynamischen Notrufen finden Sie in der Dokumentation von Microsoft.

Die Citrix Workspace-App übermittelt folgende Standortinformationen an Microsoft Teams:

- Gehäuse-ID/Port-ID per Link Layer Discovery Protocol (LLDP) für Ethernet-/Switch-Verbindungen. Ethernet/Switch (LLDP) wird unterstützt unter:

  - Windows-Versionen 8.1 und 10
  - macOS (erfordert LLDP-Aktivierungssoftware). Zum Download der LLDP-Aktivierungssoftware suchen Sie unter `www.microsoft.com` nach LLDP-Aktivierungssoftware.
  - Linux (erfordert LLDP-Bibliothek in der OS-Distribution des Thin Clients)

- WLAN BBSID und {IPv4-IPv6; Subnetz; MAC-Adresse} des Endpunkts, auf dem die Citrix Workspace-App installiert ist.

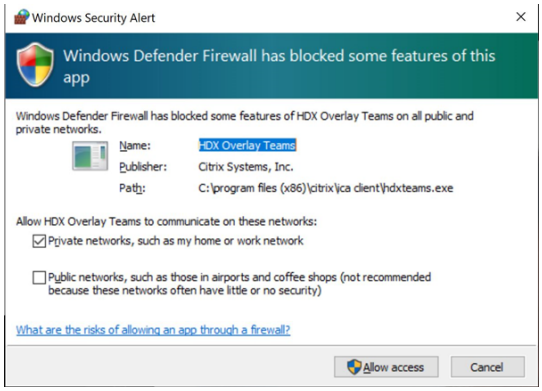
  - Subnetz- und WLAN-basierte Standorte werden von der Workspace-App für Windows, Linux und Mac unterstützt.

- Breitengrad und Längengrad, wenn Benutzerberechtigungen auf Betriebssystemebene erteilt werden, auf der die Citrix Workspace-App installiert ist (Berechtigung ist auf HDX RTC Engine festgelegt)

  - Dies wird auf allen Workspace-App-Plattformen unterstützt. Für Citrix Workspace für Linux müssen Sie die `libgps`-Bibliothek in die OS-Distribution des Thin Clients aufnehmen (>sudo apt-get install libgps23 gpsd lldpd).

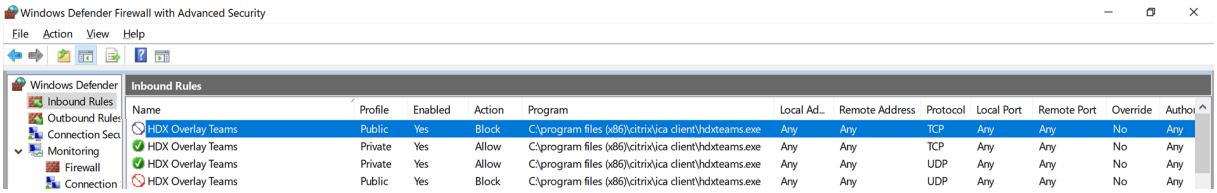
### Überlegungen zu Firewalls

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 oder HdxRtcEngine.exe (HDX Overlay Microsoft Teams) zuzulassen.




Die folgenden vier Einträge werden unter **Eingehende Regeln** in der Konsole **Windows Defender Firewall > Erweiterte Sicherheit** hinzugefügt. Sie können bei Bedarf restriktivere Regeln anwenden.

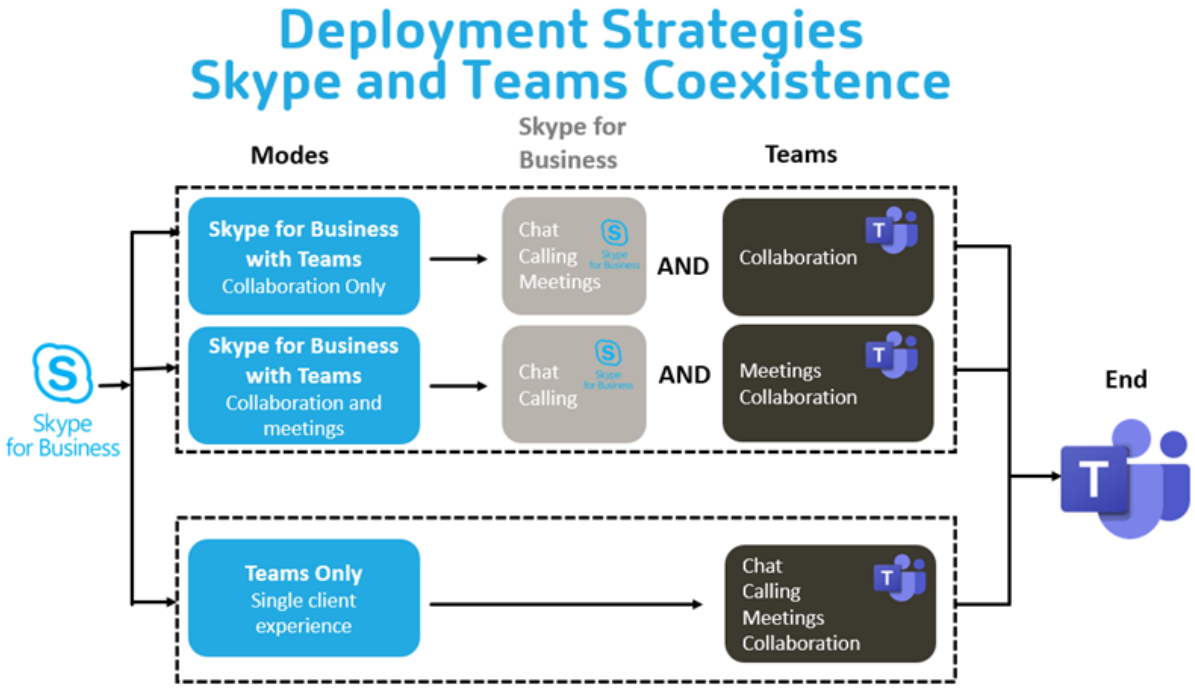



### Koexistenz von Microsoft Teams und Skype for Business

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.

Das Citrix RealTime Optimization Pack und die HDX-Optimierung für Microsoft Teams-Multimedia-Engines befolgen dann die Konfiguration in Ihrer Umgebung. Beispiele sind Island Mode und Zusammenarbeit zwischen Skype for Business und Microsoft Teams. Außerdem Zusammenarbeit zwischen Skype for Business und Microsoft Teams und Besprechungen.

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 Microsoft Teams zur Verfügung.



### Citrix SD-WAN: optimierte Netzwerkkonnektivität für Microsoft Teams

Eine optimale Audio- und Videoqualität erfordert eine Netzwerkverbindung zur Microsoft 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 führen. Es kann auch zu Staus bei WAN-Verbindungen kommen. Citrix SD-WAN optimiert die Konnektivität für Microsoft Teams gemäß den Netzwerkverbindungsprinzipien für Microsoft 365. Citrix SD-WAN verwendet die Microsoft REST-basierte Microsoft 365-IP-Adresse samt Webdienst und naheliegender DNS. Dies dient dazu, den Microsoft Teams-Datenverkehr zu identifizieren, zu kategorisieren und zu steuern.

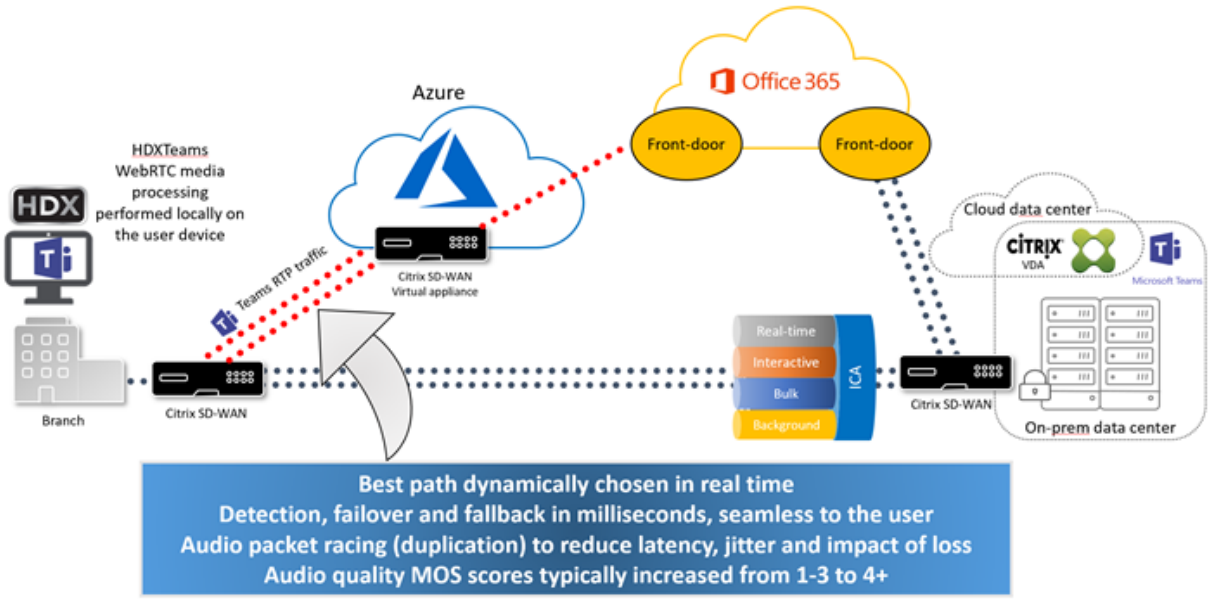
Breitband-Internetverbindungen von Unternehmen verzeichnen immer wieder Paketverluste, exzessiven Jitter und Ausfälle.

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.
- Citrix SD-WAN-Kunden können sich über Citrix Cloud Direct Service mit Microsoft 365 verbinden. Dieser Dienst bietet eine zuverlässige und sichere Bereitstellung für den gesamten Datenverkehr ins Internet.

Wenn die Qualität der Branch-Internetverbindung kein Problem darstellt, reicht es möglicherweise aus, die Latenz zu minimieren. Leiten Sie den Microsoft Teams-Datenverkehr direkt von der Citrix SD-WAN-Zweigstelle zur nächsten Microsoft 365-Haustür, um die Latenz zu minimieren. Weitere Informationen finden Sie unter Citrix SD-WAN Office 365-Optimierung.




### Meetings und Chat mit mehreren Fenstern

Sie können mehrere Meeting- bzw. Chat-Fenster für Microsoft Teams unter Windows verwenden. Einzelheiten zum Pop-Out-Feature finden Sie unter Microsoft Teams Pop-Out Windows for Chats and Meetings auf der Microsoft 365-Website.

> **Hinweis:**
>
> Das Feature wird für die Citrix Workspace-App für Windows 2112.1, Mac 2203, Linux 2203 und ChromeOS 2303 unterstützt. Es erfordert VDA 2112 oder höher und wurde auf 1912 CU6+ LTSR zurückportiert.

### Hintergrundunschärfe und Hintergrundeffekte

Die Citrix Workspace-App für Windows, Mac, Linux und ChromeOS/HTML5 unterstützt Hintergrundunschärfe und Hintergrundeffekte für die Microsoft Teams-Optimierung mit HDX.

Sie können den Hintergrund weichzeichnen oder durch ein Standardbild ersetzen, damit Ablenkungen vermieden und die Konzentration auf die Silhouette (Körper und Gesicht) erleichtert wird. Sie können das Feature für Einzel- und Konferenzgespräche verwenden.

> **Hinweis:**
>
> Dieses Feature ist in die Benutzeroberfläche und die Schaltflächen von Microsoft Teams integriert. Unterstützung für mehrere Fenster ist eine Voraussetzung, die ein VDA-Update auf 2112 oder

> später erfordert. Weitere Informationen finden Sie unter Meetings und Chat mit mehreren Fenstern.

Für Microsoft Teams-Steuerelemente für Hintergrundunschärfe und -effekte sind die folgenden Mindestversionen erforderlich:

- Citrix Workspace-App für Windows 2207
- Citrix Workspace-App für Mac 2301
- Citrix Workspace-App für Linux 2307
- Citrix Workspace-App für ChromeOS 2303

**Einschränkungen:**

- Der Client muss mit dem Internet verbunden sein, während das Hintergrundbild durch ein Microsoft Teams-Standardbild setzt wird.
- Das Ersetzen durch Administrator- und benutzerdefinierte Hintergrundbilder wird in der Microsoft Teams-Benutzeroberfläche nicht unterstützt. Benutzerdefinierte Hintergrundbilder können über Konfigurationseinstellungen auf dem Client konfiguriert werden, wenn das Bild auch auf dem Client gespeichert ist.

#### Festlegen eines benutzerdefinierten Hintergrundbilds

Die folgenden Registrierungsschlüssel sind nur erforderlich, wenn Sie die Microsoft Teams-Benutzeroberfläche nicht zur Steuerung des Features verwenden möchten oder ein Administrator das Standardverhalten außer Kraft setzen möchte. Deaktivieren Sie beispielsweise die Hintergrundunschärfe, weil der Endpunkt nicht leistungsfähig genug ist.

**Unter Windows** Um ein benutzerdefiniertes Hintergrundbild einzurichten, müssen Administratoren oder Endbenutzer den folgenden Registrierungsschlüssel auf dem Client oder Endpunkt konfigurieren:

Ort: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream`

- Name: VideoBackgroundEffect
- Typ: DWORD
- Wert: 0 (deaktiviert), 1 (aktiviert), 2 (Hintergrundbild ersetzen)

Bei einem Wert von 1 wird der Hintergrund unscharf. Der Endbenutzer oder der Administrator kann diesen Wert festlegen.

Bei einem Wert von 2 muss auch der Schlüssel **VideoBackgroundImage** vorhanden sein. Nur der Administrator kann diesen Wert festlegen. Der folgende Schlüssel ist nur erforderlich, wenn Sie das Hintergrundbild ersetzen möchten (für das Weichzeichnen ist er nicht erforderlich):

- Name: VideoBackgroundImage
- Typ: REG_SZ
- Wert: my_image_name.jpeg

Das Videohintergrundbild muss im Verzeichnis `C:\Program Files (x86)\Citrix\ICA Client` sein.

Diese Registrierungskonfiguration kann auch verwendet werden, um die Hintergrundunschärfe oder das Ersetzen von Bildern in der Citrix Workspace-App 2206 ohne Microsoft Teams-UI-Selektor zu aktivieren. Das heißt, wenn Ihre Umgebung oder Ihr VDA den Mehrfenstermodus nicht unterstützt, können Sie dennoch das Workaround in der HKCU-Registrierung mit der Citrix Workspace-App 2206 oder höher anwenden, um ein ähnliches Ergebnis zu erzielen, obwohl der Benutzer die Funktionalität während der HDX-Sitzung oder des Microsoft Teams-Anrufs nicht steuern kann.

Änderungen am Registrierungsschlüssel werden nur wirksam, wenn die HDX-Sitzung eine Verbindung herstellt.

**Unter Mac** Speicherort des vom Benutzer heruntergeladenen Bilds: */Users/username/Downloads/any_image.png*

Führen Sie die folgenden Befehle aus, um das benutzerdefinierte Bild als Standardbild festzulegen:

```
defaults write com.citrix.HdxRtcEngine VideoBackgroundEffect -int 2
```

```
defaults write com.citrix.HdxRtcEngine VideoBackgroundImage -string "
/Users/username/Downloads/any_image.png"
```

**Unter Linux** Speicherort des vom Benutzer heruntergeladenen Bilds: */home/username/Downloads/any_image.jpg*

Erstellen Sie die Datei */var/.config/citrix/hdx_rtc_engine/config.json* und fügen Sie die folgenden Konfigurationsschlüssel im JSON-Format hinzu. Beispiel:

```
1 {
2
3
4 "VideoBackgroundEffect":2,
5
6 "VideoBackgroundImage":"/home/username/Downloads/any_image.jpg"
7
8  }
```

**Unter HTML5**

1. Gehen Sie zur Datei **configuration.js** im Ordner **HTML5Client**.

2. Fügen Sie das Attribut **backgroundEffects** hinzu und legen Sie es auf **true** fest. Beispiel:

```
'features' : {

    'msTeamsOptimization' :
    {

        'backgroundEffects' : true
     }

 }

<!--NeedCopy-->
```

3. Speichern Sie die Änderung.

#### Überlegungen zur Client-CPU-Auslastung

Das Unschärfefeature verwendet die CPU sparsam, sie müssen dennoch mit einem Anstieg des Verbrauchs rechnen. Bei einem Thin Client mit einem Intel® Pentium® Silver-Chip 4 Core und 1,5 GHz und TurboBoost bis zu 2,8 GHz erhöht die Hintergrundunschärfe beispielsweise die CPU-Auslastung um etwa 2%. Die durchschnittliche CPU-Auslastung liegt unter 20%.

### Katalogansicht und aktive Sprecher in Microsoft Teams

Microsoft Teams unterstützt Layouts **Gallery**, **Large gallery** und **Together mode**.

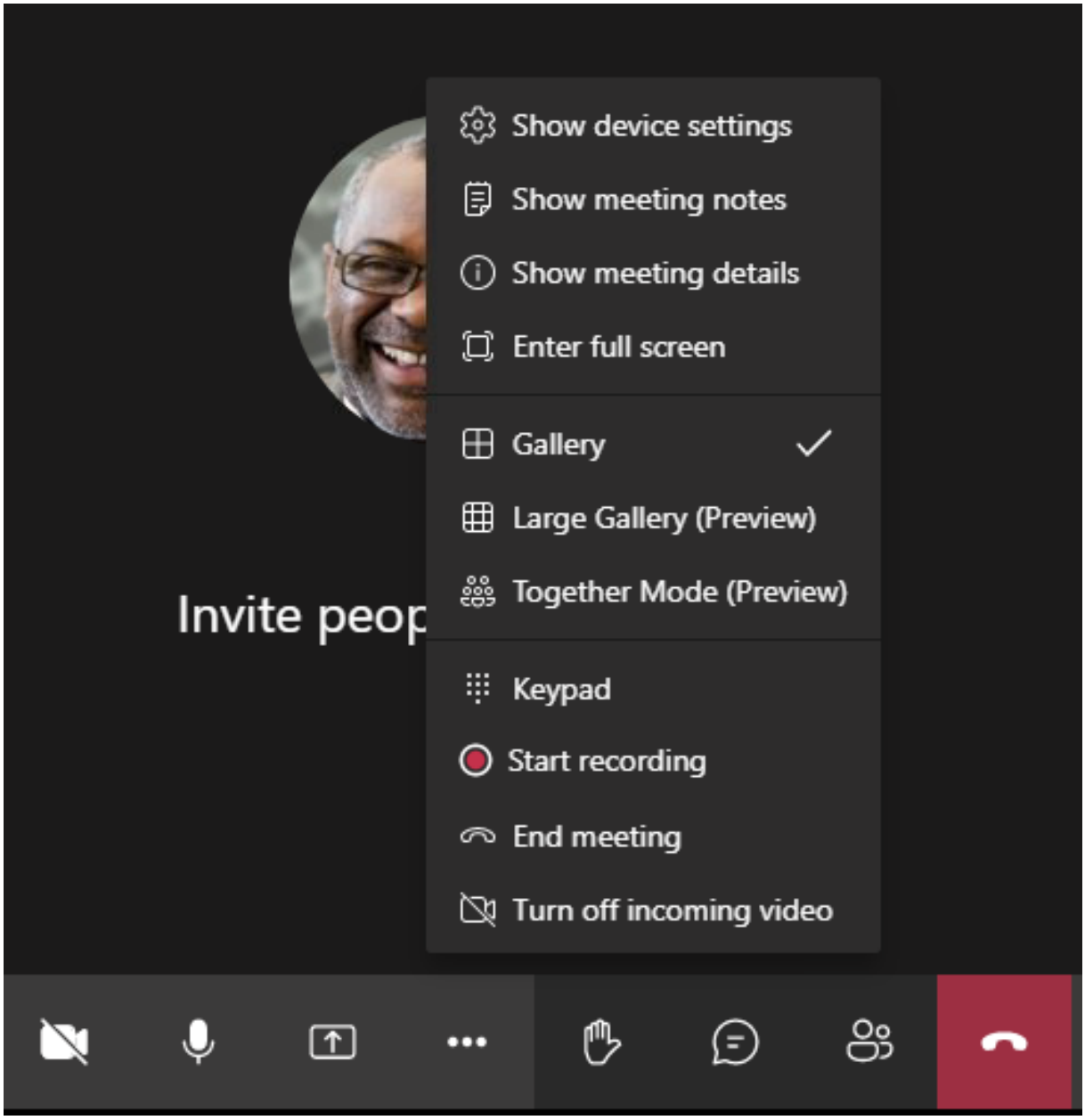
In Microsoft Teams wird ein 2x2-Raster mit Videostreams von vier Teilnehmern angezeigt (= **Gallery**). In diesem Modus sendet Microsoft Teams vier Videostreams zur Decodierung an das Clientgerät. Bei mehr als vier Teilnehmern werden nur die letzten vier aktivsten Sprecher auf dem Bildschirm angezeigt.

Microsoft Teams bietet auch die Ansicht “Large Gallery”mit einem Raster bis zu 7x7. Der Microsoft Teams-Konferenzserver stellt dann einen einzigen Videofeed zusammen und sendet ihn zur Decodierung an das Clientgerät, was zu einem geringeren CPU-Verbrauch führt. Dieser matrixartige Einzelfeed kann auch Eigenvorschauvideos der Benutzer enthalten.

Microsoft Teams unterstützt auch den **Together**-Modus als Teil der neuen Benutzeroberfläche “New Meeting Experience”. Mit KI-Segmentierungstechnologie zur digitalen Platzierung der Teilnehmer auf einen gemeinsamen Hintergrund werden in Microsoft Teams 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.




Einschränkungen bei der Unterstützung des Videoseitenverhältnisses (Citrix Workspace-App für Windows 2102, Citrix Workspace-App für Linux 2106, Citrix Workspace-App für MAC 2106 und später):

- Die Option **Frame ausfüllen** ist in der Ansicht "Galerie"bzw. "Große Galerie"verfügbar. Mit ihr wird die Videogröße so angepasst, dass sie in das Unterfenster passt. Mit der Option **An Frame anpassen** werden schwarze Balken an den Seiten des Videos angezeigt, welches nicht abgeschnitten wird.

Die folgende Tabelle bietet einen Vergleich der Layouts "Galerie"und "Große Galerie":

| | Galerieansicht 2x2 (Standard) | Große Galerieansicht |
|---|---|---|
| Layout/Raster | Zeigt ein 2x2-Raster mit Videostreams von vier Teilnehmern an. Nur die letzten vier aktivsten Sprecher erscheinen auf dem Bildschirm. Andere Teilnehmer werden nicht im Raster angezeigt. | Zeigt ein 7x7-Raster mit Videostreams von 49 Teilnehmern an. |
| Mischtechnik | Ein Medienrouter leitet einzelne Streams von jedem Teilnehmer an jeden Benutzer weiter. | Ein zentraler Konferenzserver mischt und transcodiert alle Audio- oder Videodaten und erstellt für jeden Teilnehmer ein angepasstes zusammengesetztes Layout. Dadurch entsteht etwas zusätzliche Latenz. |
| Aktiver Sprecher | Der neue aktive Sprecher ersetzt den am wenigsten aktiven Lautsprecher im Raster. | Zeigt alle Teilnehmer an, unabhängig davon, ob sie aktiv oder inaktiv sind. |
| Codierung am Endpunkt | Ein oder mehrere Videostreams können am Endpunkt codiert werden, wenn Simulcast aktiviert ist. Weitere Informationen zur Simulcast-Unterstützung finden Sie unter Simulcast. | Ein oder mehrere Videostreams können am Endpunkt codiert werden, wenn Simulcast aktiviert ist. Weitere Informationen zur Simulcast-Unterstützung finden Sie unter Simulcast. |
| Decodierung am Endpunkt | Jeder Teilnehmer erhält bis zu vier einzelne Medienstreams. Dies erhöht den CPU-Verbrauch am Endpunkt um HdxRtcEngine.exe (zum Decodieren/Rendering). | Jeder Teilnehmer erhält nur einen einzigen Stream für Audio und Video. Diese Einstellung senkt den CPU-Verbrauch am Endpunkt. |

| | Galerieansicht 2x2 (Standard) | Große Galerieansicht |
|---|---|---|
| Maximale Auflösung | 720 p. Wenn vier Teilnehmer Videos teilen, beträgt die maximale Auflösung 360p pro Videofeed. Wenn weniger als vier Teilnehmer Videos teilen, ist die Auflösung pro Videofeed möglicherweise höher. | 720p für das zusammengesetzte Layout oder das Mischen. In einem zusammengesetzten Layout ist kein qualitativ hochwertiger Videostream pro Teilnehmer erforderlich. Deshalb reduziert jeder Absender die Auflösung oder die Upload-Bitrate. |
| Problem "Langsamer Benutzer" | Sender ändert Qualität jeder Modalität (Audio/Video/Bildschirmfreigabe) auf die niedrigste gemeinsame Netzwerkqualität unter den Teilnehmern. Dieser Multimediastream wird dann an alle anderen Teilnehmer weitergeleitet. Infolgedessen wirken sich schlechte Netzwerkbedingungen bei einem Teilnehmer auf die Qualität für alle anderen im Gespräch aus. | Weniger anfällig für das Szenario der niedrigsten gemeinsamen Netzwerkqualität. Der Konferenzserver bietet verschiedene Qualitätsstufen in Abhängigkeit von den Netzwerkbedingungen einzelner Teilnehmer. |
| Eigenvorschau | Zeigt eine Miniaturansicht von Ihnen in Echtzeit an. | Zeigt eine Miniaturansicht von Ihnen und gemischt mit den übrigen Videofeeds an. Infolgedessen sehen Sie sich möglicherweise im Hauptvideolayout mit einer zusätzlichen Verzögerung. |

### 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.

Benutzer können in der Citrix Workspace-App ab Version 2109 für Windows, Linux, Mac und Citrix Workspace-App 2303 für ChromeOS ihre Bildschirme und Videokameras gleichzeitig freigeben.

In früheren Versionen wird der Videofeed der ursprünglichen Kamera angehalten, wenn der andere Gesprächsteilnehmer während eines Videoanrufs seinen Desktop freigibt. Stattdessen wird der Videofeed für die Bildschirmfreigabe angezeigt. Der Peer muss die Kamerafreigabe dann manuell fortsetzen.

> **Hinweis für PowerPoint Live**
>
> Diese Einschränkung besteht nicht, wenn Sie Inhalte aus PowerPoint Live freigeben. In diesem Fall können andere Gesprächsteilnehmer weiterhin Ihren Webcamfeed und Ihre Inhalte sehen und zwischen einzelnen Folien wechseln. In diesem Szenario werden die Folien auf dem VDA gerendert. Um auf ein Foliendeck in PowerPoint Live zuzugreifen, klicken Sie auf die Schaltfläche der Freigabeablage (Share tray) und wählen Sie dort eine PowerPoint-Folie aus. Oder klicken Sie auf "Durchsuchen", um die gewünschte PowerPoint-Datei auf Ihrem Computer oder in OneDrive zu lokalisieren.

Die ausgehende Bildschirmfreigabe wird ebenfalls optimiert und in die Citrix Workspace-App ausgelagert. In diesem Fall erfasst und überträgt die Media Engine nur das Fenster des Citrix Desktop Viewer (CDViewer.exe) mit einem roten Rahmen darum. Lokale Anwendungen, die den Desktop Viewer überlappen, werden nicht erfasst.

> **Hinweis**
>
> Legen Sie in der Citrix Workspace-App für Mac spezifische Berechtigungen fest, um die Bildschirmfreigabe zu aktivieren. Weitere Informationen finden Sie unter Systemanforderungen.

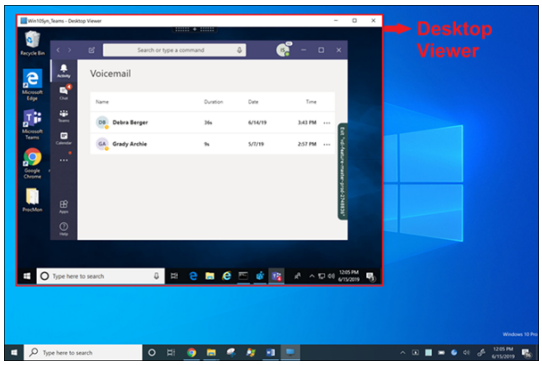
**Bekannte Einschränkung:**

- Wenn Desktop Viewer deaktiviert ist oder Desktop Lock verwendet wird, ist die Multimonitorauswahl in der Microsoft Teams-Bildschirmauswahl nicht verfügbar. Der Desktop Viewer kann durch Bearbeiten der Dateivorlage `.ICA` oder von `StoreFront web.config` deaktiviert werden. Die Tastenkombination UMSCHALT+F2 ist nicht mit der Multimonitorfreigabe kompatibel.
- In Versionen der Workspace-App, die älter als 2106 ist, wird nur der primäre Bildschirm freigegeben. Ziehen Sie die Anwendung im virtuellen Desktop auf den primären Monitor, damit die anderen Gesprächsteilnehmer sie sehen können.
- Die Multimonitorfreigabe funktioniert möglicherweise nicht, wenn Sie die Citrix Workspace-App mit dem Feature für virtuelles Bildschirmlayout (logische Partition eines einzelnen physischen Monitors) konfigurieren. In diesem Fall werden alle virtuellen Monitore als zusammengesetztes Bild freigegeben.
- Ältere Versionen der Citrix Workspace-App für Windows (1907 bis 2008) teilen auch eine lokale Anwendung, die auf der Clientmaschine ausgeführt wird. Diese Freigabe ist nur möglich, wenn

die lokale App über Desktop Viewer überlagert wurde. Dieses Verhalten wurde in 2009.6 oder höher und in 1912 CU5 oder höher entfernt.

- Wenn Sie während der Bildschirmfreigabe vom Fenstermodus in den Vollbildmodus wechseln, wird die Bildschirmfreigabe beendet. Sie müssen die Bildschirmfreigabe anhalten und neu starten, damit sie funktioniert.
- Im optimierten Microsoft Teams ist es nicht möglich, die Steuerelemente für die Freigabe an einen bestimmten Ort anzuheften.
- Beim Freigeben einer minimierten App wird möglicherweise auch die App-Titelleiste freigegeben.




**Bildschirmfreigabe aus Seamlessanwendung:**

Wenn Sie Microsoft Teams als eigenständige Seamlessanwendung veröffentlichen, erfasst die Bildschirmfreigabe den lokalen Desktop Ihres physischen Endpunkts. Dafür ist mindestens Version 1909 der Citrix Workspace-App erforderlich.

### App-Freigabe

Ab der Citrix Workspace-App für Windows 2112 und VDA 2112.1 unterstützt Microsoft Teams die App-Freigabe.

Microsoft Teams unterstützt ab Citrix Workspace-App für Windows 2109, Mac 2203, Linux 2209 und VDA 2109 die Bildschirmfreigabe für bestimmte Apps, die in der virtuellen Sitzung ausgeführt werden. In Microsoft Teams mit Optimierung können Sie auch benutzerdefinierte interne Anwendungen wie Java freigeben. Freigabe einer App:

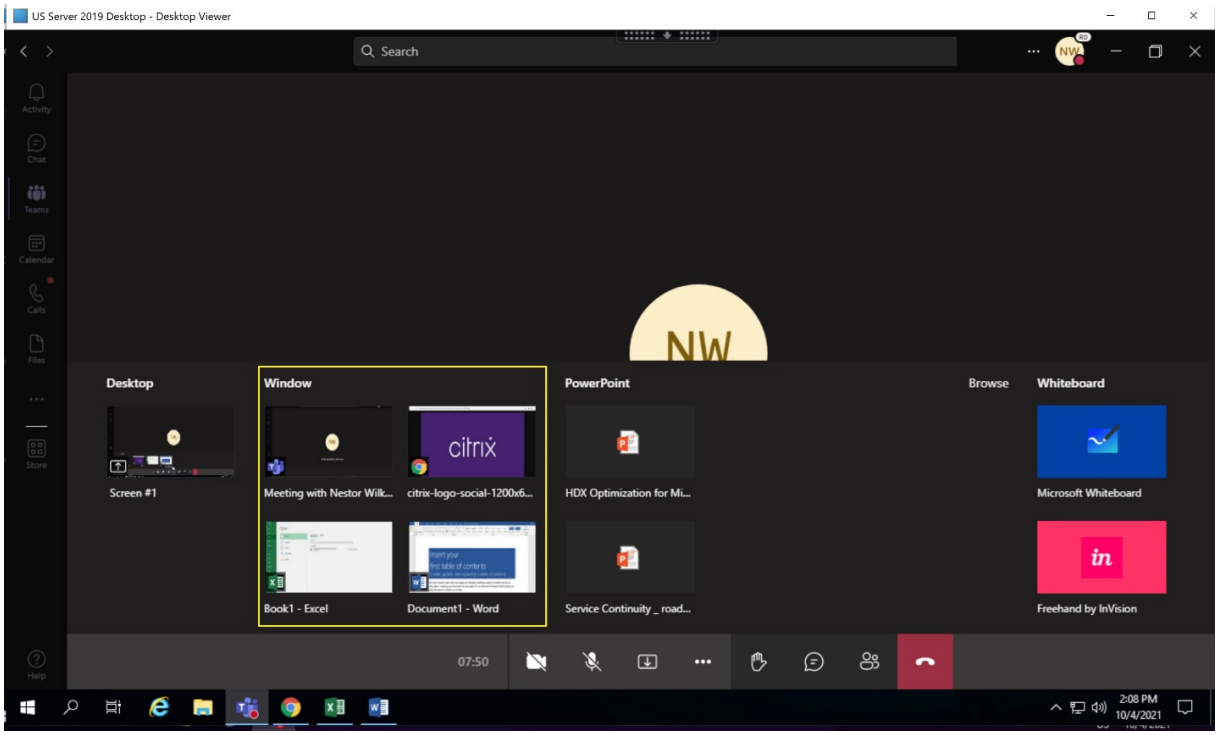
1. Navigieren Sie innerhalb der Remotesitzung zur Microsoft Teams-App.
2. Klicken Sie in der Microsoft Teams-Benutzeroberfläche auf **Inhalt freigeben**.
3. Wählen Sie die App aus, die Sie in der Besprechung freigeben möchten. Die ausgewählte App wird rot umrandet angezeigt, und die übrigen Gesprächsteilnehmer können die freigegebene App sehen.

Um eine andere App freizugeben, klicken Sie erneut auf **Inhalt freigeben** und wählen eine neue App aus.

Wenn Sie die App-Freigabe deaktivieren möchten, erstellen Sie den folgenden Registrierungsschlüssel auf dem VDA unter `HKLM\SOFTWARE\Citrix\Graphics`:
Name: `UseWsProvider`
Typ: `DWORD`
Wert: 0

> **Hinweis:**
>
> - Wenn Sie eine App minimieren, zeigt Microsoft Teams das letzte Bild der freigegebenen App an. Sie können das Fenster maximieren, um die Bildschirmfreigabe fortzusetzen.
> - Die Bildschirmfreigabe hängt von der VDA-seitigen Erfassung des Fensters ab. Der Inhalt wird dann mit einer maximalen Rate (30 Frames pro Sekunde) an die Citrix Workspace-App weitergeleitet. Die Citrix Workspace-App leitet den Inhalt an die Peers oder den Konferenzserver weiter.




**Bekannte Einschränkungen bei der Bildschirmfreigabe einer bestimmten App:**

- Der Mauszeiger ist nicht sichtbar, wenn Sie eine App auf dem Bildschirm freigeben.
- Wenn Sie eine App während der Freigabe minimieren, wird nur das App-Symbol in der Bildschirmauswahl angezeigt. Das Miniaturbild der App ist in der Bildschirmauswahl nicht zu sehen. Sie können den Inhalt nicht teilen und die rote Umrandung wird erst angezeigt, wenn Sie die App maximiert haben.
- Als Apps mit lokalem App-Zugriff werden Apps aufgelistet, die für Desktop-Apps im optimierten Microsoft Teams im VDA freigegeben werden können. Wenn Sie die App jedoch in der Liste

auswählen, wird das Ergebnis möglicherweise nicht wie erwartet angezeigt.

**Kompatibilität mit App-Schutz**
Die Bildschirmfreigabe einer bestimmten App ist mit dem App-Schutzfeature in HDX-optimiertem Microsoft Teams kompatibel. Sie können eine bestimmte App auf dem Bildschirm freigeben, wenn Sie die App oder den Desktop aus einer Bereitstellungsgruppe mit aktiviertem App-Schutz gestartet haben.

Wenn Sie in der Microsoft Teams-Benutzeroberfläche auf **Inhalt freigeben** klicken, entfernt die Bildschirmauswahl die Option **Desktop**. Sie können nur die Option **Fenster** auswählen, um eine geöffnete App zu teilen.

> **Hinweis:**
>
> Mit der Citrix Workspace-App für Windows 2202 oder früher können Sie das eingehende Video bzw. den freigegebenen Bildschirm nicht sehen, wenn Sie Apps oder Desktops aus einer Bereitstellungsgruppe mit aktiviertem App-Schutz starten.

**Übergeben und Anfordern der Steuerung in Microsoft Teams** Dieses Feature wird in den folgenden Versionen der Citrix Workspace-App unterstützt (unabhängig von VDA- oder Betriebssystemversion –Multisitzungs-/Einzelsitzungs-OS):

- Citrix Workspace-App für Windows Version 2112.1 oder später
- Citrix Workspace-App für Mac Version 2203.1 oder später
- Citrix Workspace-App für Linux, Version 2203 oder später
- Citrix Workspace-App für ChromeOS Version 2303 oder später

Sie können bei einem Microsoft Teams-Anruf die Steuerung anfordern, wenn ein Teilnehmer den Bildschirm freigibt. Wenn Sie die Steuerung übernommen haben, können Sie auf dem freigegebenen Bildschirm Tastatur- und Mausaktivitäten wie Auswahl, Änderungen usw. vornehmen.

Zum Übernehmen der Steuerung bei Freigabe eines Bildschirms klicken Sie in Microsoft Teams auf **Steuerung anfordern**. Der Teilnehmer des Meetings, der den Bildschirm freigibt, kann die Anforderung akzeptieren oder ablehnen.

Wenn Sie die Steuerung übernommen haben, können Sie Elemente auf dem freigegebenen Bildschirm auswählen, bearbeiten und andere Änderungen vornehmen. Für diese Aktionen können Sie sowohl eine Tastatur als auch eine Maus verwenden. Wenn Sie fertig sind, klicken Sie auf **Steuerung anfordern**.

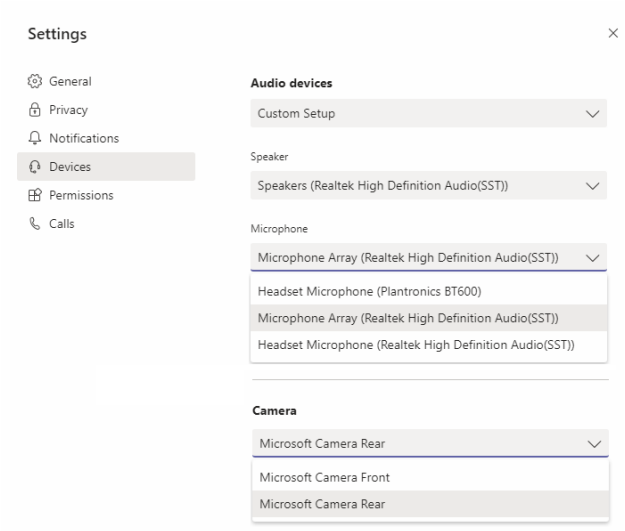
> **Einschränkungen:**
>
> - Übergeben- und Anfordern der Steuerung sind nicht möglich, wenn der Benutzer eine einzelne App teilt (“App-Freigabe”). Der gesamte Desktop oder Bildschirm muss

> freigegeben werden.
> - Das Feature zum Anheften der Steuerleiste an eine bestimmte Position ist nicht verfügbar.

### Peripheriegeräte in Microsoft Teams

Wenn die Optimierung für Microsoft Teams aktiv ist, greift die Citrix Workspace-App auf die Peripheriegeräte (Headsets, Mikrofone, Kameras, Lautsprecher usw.) zu. Anschließend werden die Peripheriegeräte ordnungsgemäß in der Benutzeroberfläche von Microsoft Teams (**Einstellungen > Geräte**) aufgelistet.




Microsoft Teams greift nicht direkt auf die Geräte zu. Stattdessen verwendet es die WebRTC Media Engine der Workspace-App, um die Medien zu erfassen, aufzuzeichnen und zu verarbeiten. Microsoft Teams listet die Geräte auf, die der Benutzer auswählen kann.

Peripheriegeräte, die angeschlossen werden, während Microsoft Teams aktiv ist, sind standardmäßig nicht ausgewählt. Sie müssen die Peripheriegeräte manuell im Bildschirm **Einstellungen** > **Geräte** der Microsoft Teams-Benutzeroberfläche auswählen. Nachdem das Peripheriegerät ausgewählt ist, speichert Microsoft Teams die Informationen der Peripheriegeräte im Cache. Die Peripheriegeräte werden daher automatisch ausgewählt, wenn Sie sich vom selben Endpunkt aus erneut mit der Sitzung verbinden.

**Empfehlungen:**

- Microsoft Teams-zertifizierte Headsets mit integrierter Echounterdrückung. Bei Konfigurationen mit weiteren 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, platzieren Sie diese so weit wie möglich weg vom Mikrofon. Stellen Sie sie außerdem nicht in der Nähe von Oberflächen auf, die den Ton in Richtung Mikrofon lenken

könnten. Weitere Informationen finden Sie durch Suchen nach "Microsoft Teams certified headsets"auf www.microsoft.com.

- Microsoft Teams-zertifizierte Kameras, obwohl für Skype for Business zertifizierte Peripheriegeräte mit Microsoft Teams kompatibel sind. Weitere Informationen finden Sie durch Suchen nach "Microsoft Teams certified cameras and Skype for Business certified peripherals" auf .
- Eine Entlastung des Hauptprozessors durch Onboard-H.264-Codierung der Webcams (UVC 1.1 und 1.5) kann die Media Engine der Citrix Workspace-App nicht nutzen.

> **Hinweis:**
>
> Die Workspace-App 2009.6 für Windows kann jetzt Peripheriegeräte mit Audioformaten mit 24 Bit oder mit Frequenzen über 96 kHz abrufen.
>
> HdxTeams.exe (in der Citrix Workspace-App für Windows 2009 oder früher) 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 Microsoft 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!
> ```
>
> Deaktivieren Sie als Workaround das Gerät oder:
>
> 1. Öffnen Sie das **Audiosteuerungsfeld** (mmsys.cpl).
> 2. Wählen Sie das Wiedergabe- oder Aufnahmegerät aus.
> 3. Gehen Sie zu **Eigenschaften > Erweitert** und ändern Sie die Einstellungen in einen unterstützten Modus.

#### Fallbackmodus

Wenn Microsoft Teams nicht im optimierten VDI-Modus geladen werden kann ("Citrix HDX Not Connected"in Microsoft Teams/Info/Version), greift der VDA auf ältere HDX-Technologien zurück. Zu älteren HDX-Technologien gehören Webcamumleitung und Clientaudio- sowie Mikrofonumleitung. Wenn Ihre Workspace-App- oder Plattform-OS-Version die Microsoft Teams-Optimierung nicht

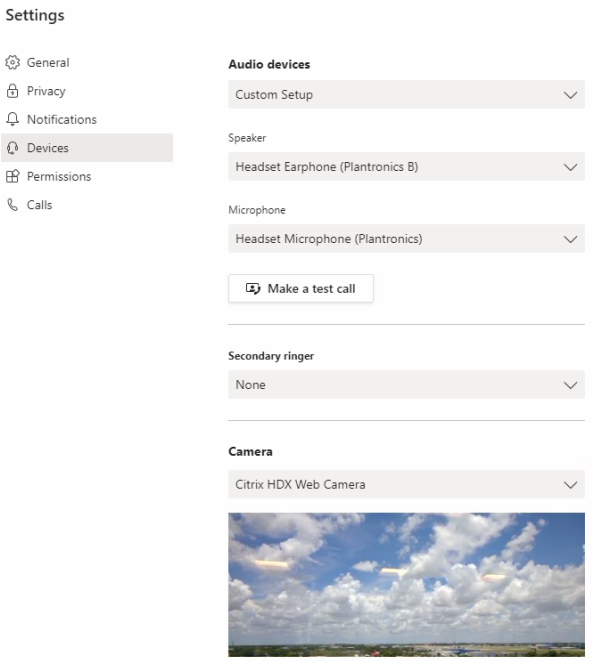
 

unterstützt, werden Fallback-Registrierungsschlüssel nicht angewendet.
Im Fallbackmodus werden die Peripheriegeräte dem VDA zugeordnet. Die Peripheriegeräte werden in der Microsoft Teams-App so angezeigt, als wären sie lokal an den virtuellen Desktop angeschlossen.

Sie können jetzt den Fallbackmechanismus präzise steuern, indem Sie die Registrierungsschlüssel im VDA festlegen. Weitere Informationen finden Sie unter Fallbackmodus für Microsoft Teams in der Liste der über die Registrierung verwalteten Features.

Für dieses Feature ist die Microsoft 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 der Microsoft Teams-App auf der Registerkarte **Einstellungen > Geräte**. Wenn Microsoft Teams im nicht optimierten Modus geladen wird, 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:

- HID-Schaltflächen - "Antworten"und "Anruf beenden"werden nicht unterstützt. Der Lautstärkeregler (lauter/leiser) wird unterstützt.
- QoS-Einstellungen im Microsoft Teams Admin Center gelten nicht für VDI-Benutzer.
- Benutzer können keine Screenshots von Microsoft Teams-Inhalten machen, wenn sie ein Snipping-Tool auf dem VDA verwenden. Wenn clientseitig jedoch ein Snipping-Tool verwendet wird, können die Inhalte aufgenommen werden.

Beschränkung auf dem VDA:

- Wenn Sie die **High DPI-Einstellung der Citrix Workspace-App** auf `Yes` konfigurieren, wird das umgeleitete Videofenster an der falschen Stelle angezeigt. Diese Einschränkung tritt auf, wenn der DPI-Skalierungsfaktor des Monitors auf einen Wert über 100 % festgelegt ist

Einschränkungen bei Citrix Workspace-App und VDA:

- Sie können die Lautstärke bei optimierten Anrufen nur über die Lautstärkeleiste auf dem Client steuern, nicht über die auf dem VDA.

### Simulcast

Die Simulcast-Unterstützung ist für optimierte Microsoft Teams-Videokonferenzen unter Windows und Mac aktiviert. Im Fall von Linux wenden Sie sich an Ihren Thin Client-Anbieter.
Mit Simulcast werden die Qualität und das Erlebnis bei Videokonferenzen an verschiedenen Endpunkten verbessert, indem die bestgeeignete Auflösung für alle Anrufer gewählt wird.

Dank dieser verbesserten Benutzererfahrung kann jeder Benutzer abhängig von der Endpunktfähigkeit, den Netzwerkbedingungen usw. mehrere Videostreams in unterschiedlichen Auflösungen (z. B. 720p, 360p usw.) senden. Der empfangende Endpunkt fordert dann die maximale Auflösung an, die er verarbeiten kann, sodass alle Benutzer das optimale Videoerlebnis erhalten.

> **Hinweis:**
>
> Dieses Feature ist erst nach Veröffentlichung eines Microsoft Teams-Updates verfügbar. Informationen zum voraussichtlichen Releasedatum finden Sie durch Suchen nach "Microsoft 365 roadmap"auf https://www.microsoft.com/. Wenn das Update von Microsoft veröffentlicht wurde, finden Sie in CTX253754 Informationen über das Dokumentationsupdate und die Ankündigung.

#### Microsoft-Einschränkungen

- Eine 3x3-Galerieansicht wird nicht unterstützt. Microsoft 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.
- PSTN-Freizeichen wird nicht unterstützt.
- Medienumgehung für Direct Routing wird nicht unterstützt.
- Die Rollen "producer"und "presenter"für Live-Ereignisse werden nicht unterstützt. Die Teilnehmerrolle wird unterstützt, aber nicht optimiert (das Rendering erfolgt stattdessen auf dem VDA).
- Die Zoomfunktion in Microsoft Teams wird nicht unterstützt.
- Standortbasiertes Routing und Medienumgehung werden nicht unterstützt.
- Das Zusammenführen von Aufrufen wird nicht unterstützt (Option wird nicht in der Benutzeroberfläche angezeigt).

#### Citrix und Microsoft-Einschränkungen

- Bei der Bildschirmfreigabe ist die Option **Systemaudio einschließen** nicht verfügbar.
- Simulcast wird unter ChromeOS 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.

> **Hinweis:**
>
> Citrix weist Sie darauf hin, dass Sie Ihren VDA und die Citrix Workspace-App auf die unterstützten Versionen aktualisieren müssen, um Microsoft Teams weiterhin im optimierten Modus für Videoanrufe und die Bildschirmfreigabe zu verwenden. Wenn Sie Ihre Infrastruktur und Ihre Endgeräte nicht so aufrüsten, dass sie mehrere Fenster unterstützen, werden Ihre Anrufe, Videoanrufe und die Bildschirmübertragung nicht mehr optimiert. Dies kann zu Problemen mit der Anrufqualität, erhöhter Latenz und erhöhter Serverlast führen.

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 (1) | Version für LTSR (2) | Empfohlene Version (3) |
|---|---|---|---|
| Microsoft Teams | 1.5.00.11865 | Nicht zutreffend | Aktuell |
| VDA | 1912 CU6 LTSR, 2109 CR, 2203 LTSR | 1912 CU8+, 2203 LTSR CU2+ (4) | 2308 CR+ |
| Citrix Workspace-App für Windows | 2112.1 CR | 2203 CU2+ (4) | 2309 CR+ |
| Citrix Workspace-App für Mac | 2203 CR | Nicht zutreffend | 2308 CR+ |
| Citrix Workspace-App für Linux | 2202 CR | Nicht zutreffend | 2308 CR+ |
| Citrix Workspace-App für ChromeOS oder HTML5 | 2303 CR | Nicht zutreffend | 2309 CR+ |

**Hinweise:**

1. Mindestversion: Dies ist die Version, in der der Mehrfenstermodus zum ersten Mal eingeführt wurde. Einige der hier aufgeführten Mindestversionen können End-of-Life-Versionen sein.
2. LTSR-unterstützte Version: Dies ist die LTSR-Version, die von Citrix für den Mehrfenstermodus unterstützt wird. Ältere Versionen dieser LTSR-Releases funktionieren möglicherweise, aber die Unterstützung für diese Versionen ist nicht mehr verfügbar, sobald eine neue LTSR CU-Version veröffentlicht wird. Weitere Informationen zu LTSR-Supportrichtlinien finden Sie unter https://support.citrix.com/article/CTX205549/faq-citrix-virtual-apps-and-desktops-and-citrix-hypervisor-long-term-service-release-ltsr.
3. Empfohlene Version: Dies ist die Softwareversion, die Citrix empfiehlt, wenn der Benutzer/Kunde sich für ein Upgrade seiner Software entscheidet. Dies sind alles CR-Versionen.
4. Version 2203 LTSR für VDA- und CWA-Basisversionen beinhaltet die Mehrfensterfunktionalität. Diese Versionen wurden durch die neueste CU ersetzt, die offiziell unterstützte Version. Kunden können diese nicht unterstützten Versionen nach eigenem Ermessen weiterhin verwenden. Citrix empfiehlt Kunden der LTSR-Version, ein Upgrade auf die neueste CU durchzuführen.

## 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 Microsoft 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

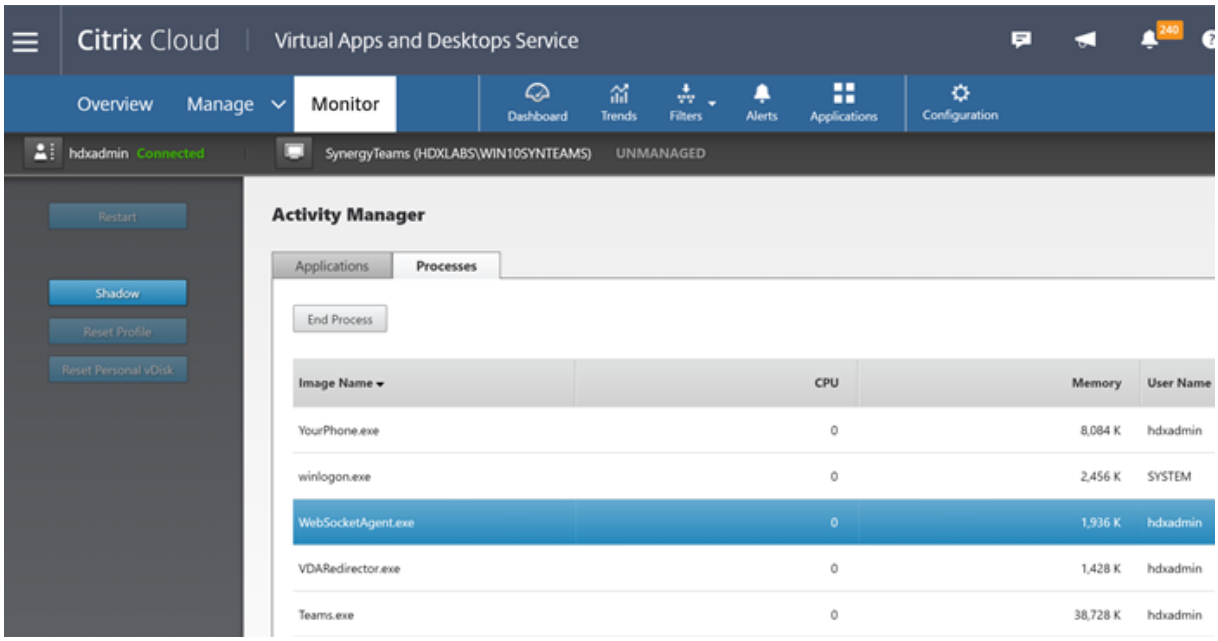
 

# Microsoft Teams überwachen sowie Problembehandlung und Support

June 27, 2024

## Teams überwachen

Dieser Abschnitt enthält Richtlinien zum Überwachen der Microsoft Teams-Optimierung mit HDX. Wenn Sie den optimierten Modus verwenden und auf dem Clientcomputer `HdxRtcEngine.exe` ausgeführt wird, wird in der Sitzung der VDA-Prozess `WebSocketAgent.exe` ausgeführt. Verwenden Sie den **Aktivitätsmanager** in Director, um die Anwendung anzuzeigen.




Der Status der Microsoft Teams-Optimierung kann auf der Seite Director > **Benutzerdetails** > Bereich **Sitzungsdetails** > Feld **MS Teams-Optimierung** eingesehen werden. Die Optimierung von Microsoft Teams ist entscheidend für eine bessere Benutzererfahrung, z. B. für klares Audio und Video. Diese Funktion ist für VDA-Version 2311 und höher verfügbar. Die unterstützten Versionen der Citrix Workspace-App sind unter Optimierung für Microsoft Teams aufgeführt. Director zeigt den Status der Microsoft Teams-Optimierung nur an, wenn Microsoft Teams als veröffentlichte App oder auf einem veröffentlichten Desktop ausgeführt wird.
Weitere Informationen finden Sie unter Optimierung für Microsoft Teams.

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`.

Mit dem VDA (Mindestversion 1912) können Sie in Microsoft 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`.

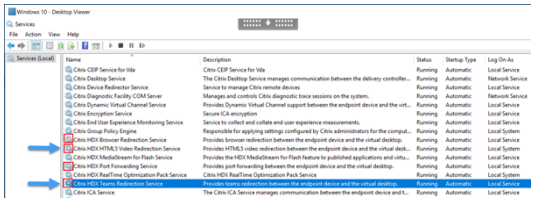
Weitere Informationen finden Sie im Knowledge Center-Artikel CTX253754 unter *Monitoring*.

## Problembehandlung

Dieser Abschnitt enthält Tipps zur Behandlung von Problemen, die bei der Verwendung der Optimierung für Microsoft Teams auftreten können. Weitere Informationen finden Sie unter CTX253754.

### Virtual Delivery Agent

Von BCR_x64.msi werden vier Dienste installiert. Nur zwei sind für die Microsoft Teams- Umleitung auf dem VDA verantwortlich.



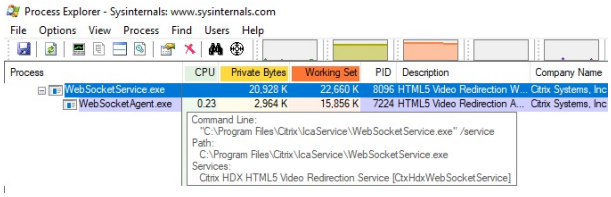
- **Citrix HDX Teams Redirection Service** richtet den virtuellen Kanal ein, der in Microsoft Teams verwendet wird. Der Dienst basiert auf CtxSvcHost.exe.
- **Citrix HDX HTML5 Video Redirection Service** wird als WebSocketService.exe ausgeführt und überwacht 127.0.0.1:9002 TCP. WebSocketService.exe führt 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.** Beim Start von Microsoft Teams 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 Browserinhaltsum-leitung zwischen dem Endpunktgerät und dem virtuellen Desktop. |
| Citrix Portweiter-leitungsdienst | "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 Browserinhaltsum-leitung. |
| 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 oder HdxRtcEngine.exe. Dies geschieht, wenn Microsoft Teams auf dem VDA gestartet wird und der Benutzer versucht, in der Eigenvorschau einen Anruf zu tätigen oder auf die 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 oder HdxRtcEngine.exe und die webrpc.dll-Binärdateien?
2. Wenn Sie Schritt 1 überprüft haben, gehen Sie folgendermaßen vor, um zu prüfen, ob HdxTeams.exe bzw. HdxRtcEngine.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 bzw. HdxRtcEngine.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.

   Ort:/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.

   Ort: $TMPDIR/hdxrtcengine/<W_M_D_H_M_S_Y>/hdxrtcengine.log

   HdxRtcEngine-Protokollierung ist standardmäßig aktiviert.

3. Webrpc-Protokolle - die wichtigsten Protokolle, die die Ausführung des Wrapups der webrtc-Bibliothek aufzeichnen.

   Ort: /Users/<USERNAME>/Library/Logs/HdxRtcEngine/<W_M_D_H_M_S_Y>/webrpc.log

**Linux-Protokolle:**

Die Linux-Protokolle sind in den Ordnern /tmp/webrpc/<current date>/ and /tmp/hdxrtcengine/<current date>/.
Webrtc-Protokoll: /tmp/webrpc/<current date>/webrtc.log
Kernel-Protokoll: /var/log/syslog

**ICE/STUN/TURN/-Protokolle:**

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 HdxRtcEngine.exe sind die folgenden Einträge für ICE (Interactive Connectivity Establishment) relevant. Diese Einträge müssen vorhanden sein, damit ein Anruf erfolgreich eingerichtet wurde. Sehen Sie sich folgenden Beispielausschnitt für die Sammelphase an:

```
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:

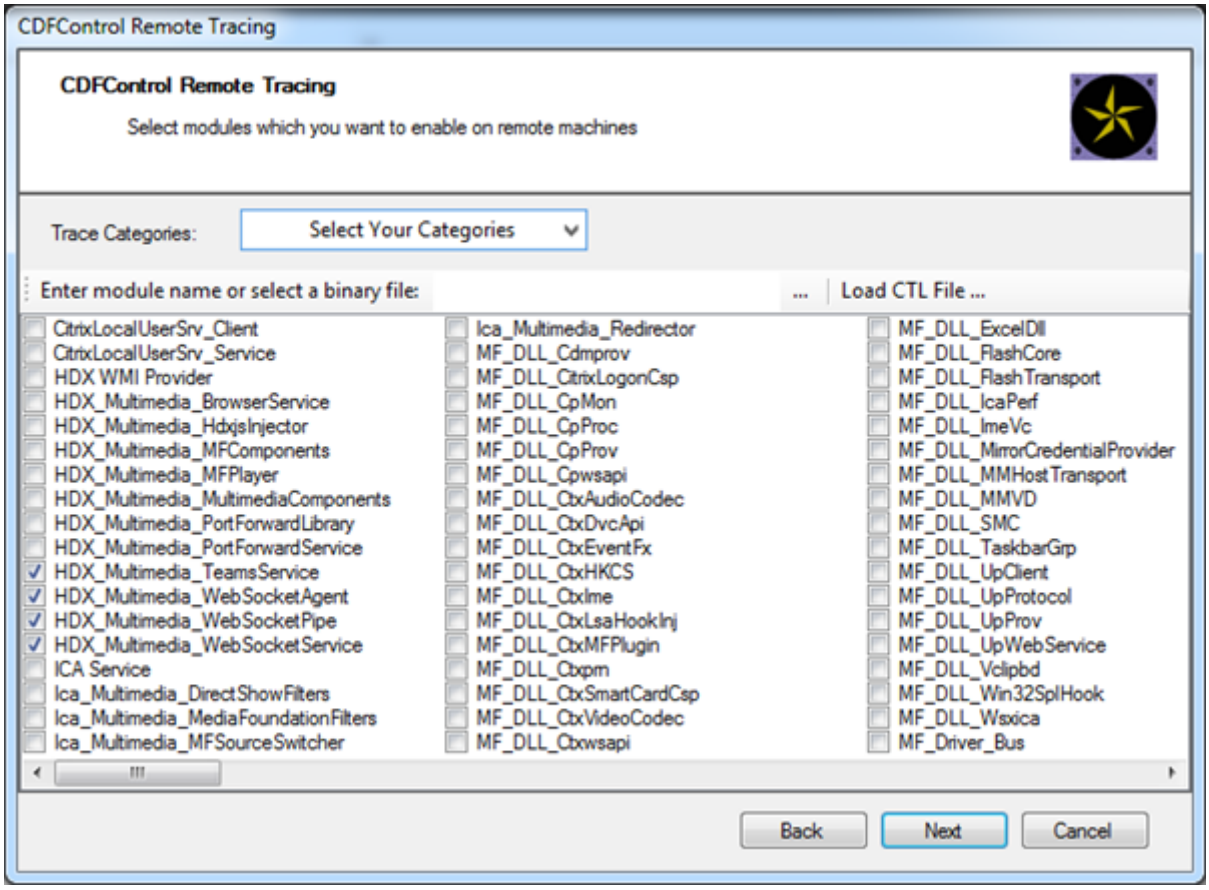
 

1. Host
2. Peer reflexiv
3. Server reflexiv
4. Transport-Relay

Wenn ein Problem auftritt und Sie es reproduzieren können, empfehlen wir, in Microsoft 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.

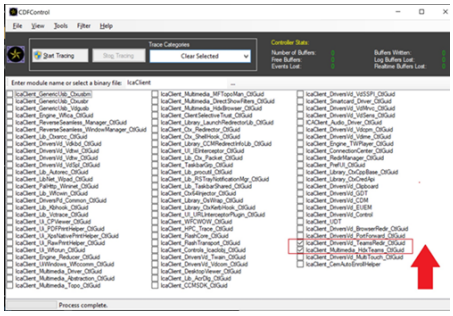
Empfehlungen zur Erzeugung von CDF-Tracingberichten finden Sie im Knowledge Center-Artikel Recommendations for Collecting the CDF Traces.

**VDA-seitige CDF-Tracingberichte –aktivieren Sie die folgenden CDF-Trace-Anbieter:**




**Workspace-App-seitige CDF-Tracingberichte –aktivieren Sie die folgenden CDF-Trace-Anbieter:**



- IcaClient_DriversVd_TeamsRedir (optional)
- IcaClient_Multimedia_HdxTeams (erfordert die Citrix Workspace-App 2012 oder höher)

## Windows Media-Umleitung

June 27, 2024

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 Fea-

ture 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

June 27, 2024

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.

### Clientordner umleiten

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.

# Clientordner umleiten

June 27, 2024

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 2022
- 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)

Informationen zum Aktivieren der Clientordnerumleitung auf dem Server finden Sie unter Clientordnerumleitung in der Liste der über die Registrierung verwalteten Features.

Geben Sie auf dem Benutzergerät an, welche Ordner umgeleitet werden sollen.

1. Stellen Sie sicher, dass die neueste Version der Citrix Workspace-App installiert ist.
2. Starten Sie vom Installationsverzeichnis der Citrix Workspace-App aus CtxCFRUI.exe.

3. Wählen Sie das Optionsfeld **Benutzerdefiniert** und fügen Sie Ordner hinzu oder bearbeiten oder entfernen Sie Ordner.
4. Trennen Sie die Sitzungen und stellen Sie dann neue Verbindungen her, damit die Einstellung wirksam wird.

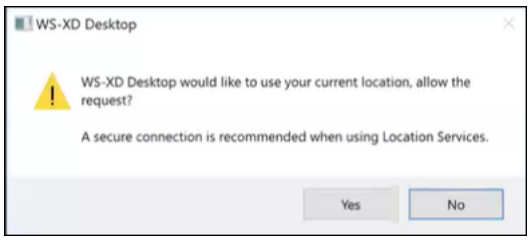
## Clientstandort umleiten

June 27, 2024

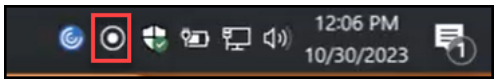
Wenn die Clientstandortumleitung aktiviert ist, können vom VDA gehostete Apps und Desktopsitzungen nahtlos auf den aktuellen Standort des Clients zugreifen. Auf einem Multisitzungsbetriebssystem (TS VDA oder Multisitzungs-WS-VDA) hat jede Sitzung ihren eigenen eindeutigen Speicherort, der vom verbundenen Client bereitgestellt wird. Mit diesem Feature verfügen Anwendungen auf dem VDA, die vom Standort abhängig sind, über den genauen Standort des Clients.

Weitere Informationen finden Sie in der Microsoft-Dokumentation.

Nachdem die Clientstandortumleitung aktiviert ist und der Standortzugriff sowohl auf der Server- als auch auf der Clientseite zulässig ist, fordert der Client Sie auf, seinen aktuellen Standort mit dem folgenden Dialogfeld zu teilen, wenn Sie eine Anwendung oder einen Desktop mit Zugriff auf den Standort starten:




Wenn Sie die Clientstandortumleitung aktivieren, wird das folgende Symbol in der Taskleiste des Clients angezeigt, sofern bzw. sobald die vom VDA gehostete App oder der Desktop aktuelle Standortinformationen abfragt.




### Systemanforderungen

Server:

- OS VDA mit Einzelsitzung (Win10/11) oder Mehrfachsitzung (Win 11 22H2 und Server 2022 23H2 oder höher)
- Citrix Workspace-App für Windows, iOS oder Android

### Konfiguration

Die Clientstandortumleitung muss mithilfe der Citrix-Richtlinie aktiviert werden, damit das Feature funktioniert. Die Clientstandortumleitung ist standardmäßig deaktiviert.

Gehen Sie wie folgt vor, um die Umleitung des Client-Standorts zu aktivieren:

Auf der Windows VDA- und Client-Seite:

1. Aktivieren Sie unter **Einstellungen > Datenschutz > Standort** die folgenden Optionen:
    - **Zugriff auf den Standort auf diesem Gerät zulassen**
    - **App-Zugriff auf Ihren Standort zulassen**
    - **Desktop-Apps den Zugriff auf Ihren Standort erlauben**
2. Aktivieren Sie für Multisitzungs-OS die Einstellung **Standort-Außerkraftsetzung**.

Auf der Controller-/DDC-Seite:

Aktivieren Sie die Richtlinie **Studio > Richtlinien > Standort > Einstellungen > Anwendungen können physischen Clientgerätstandort verwenden**.
Weitere Informationen finden Sie unter Richtlinieneinstellungen für Clientsensoren.

## Bidirektionale Inhaltsumleitung

June 27, 2024

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

Browser:

- Google Chrome mit der Citrix Browserumleitung-Erweiterung (verfügbar im Google Chrome Web Store)
- Microsoft Edge (Chromium) mit der Citrix Browserumleitung-Erweiterung (verfügbar im Google Chrome Web Store)

### Konfiguration

Ab Version 2311 von Citrix Virtual Apps and Desktops wird die bidirektionale Inhaltsumleitung nur über Citrix Studio konfiguriert. In früheren Versionen waren Richtlinieneinstellungen sowohl auf dem Clientendpunkt als auch in Studio konfiguriert. Die bidirektionale Inhaltsumleitung ist standardmäßig deaktiviert.

Informationen zur VDA-Konfiguration finden Sie unter Bidirektionale Inhaltsumleitung in den **ICA-Richtlinieneinstellungen**.

Damit die Browserumleitung funktioniert, müssen die Browsererweiterungen über die angezeigten Befehle im ursprünglichen Browser (von dem die URL umgeleitet wird) registriert werden. Führen Sie die Befehle wie erforderlich auf dem VDA und dem Client aus, basierend auf dem verwendeten Browser.

| Browser | VDA | Client |
|---|---|---|
| Google Chrome | %ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirect.exe /regChrome | %ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe /regChrome |
| Microsoft Edge | %ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirect.exe /regEdge | %ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe /regEdge |
| Alle verfügbaren Browser | %ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirect.exe /regall | %ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe /regall |

So heben Sie die Registrierung einer Browsererweiterung auf:

| Browser | VDA | Client |
| --- | --- | --- |
| Google Chrome | %ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirect.exe /unregChrome | %ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe /unregChrome |
| Microsoft Edge | %ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirect.exe /unregEdge | %ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe /unregEdge |
| Alle verfügbaren Browser | %ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirect.exe /unregall | %ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe /unregall |

> **Hinweis:**
>
> Der Registrierungsbefehl veranlasst Chrome- und Edge-Browser die Benutzer beim ersten Start aufzufordern, die Citrix Browserumleitungserweiterung zu aktivieren. Die Browsererweiterung kann auch manuell im Google Chrome Web Store installiert werden. Informationen zu Microsoft Edge finden Sie auch unter Erweiterung zu Microsoft Edge aus dem Chrome Web Store hinzufügen.

### Platzhalterumleitung vom Citrix VDA zum Client

Die bidirektionale Inhaltsumleitung unterstützt die Verwendung von Platzhaltern bei der Definition der umzuleitenden URLs. Lesen Sie zum Konfigurieren der bidirektionalen Inhaltsumleitung die Anweisungen zur [Konfiguration] unter (/en-us/citrix-virtual-apps-desktops/2402-ltsr/general-content-redirection/bidirectional-content-redirection-configuration/bidirectional-content-redirection#configuration).

### Umleitung benutzerdefinierter Protokolle vom VDA zum Client

Die bidirektionale Inhaltsumleitung unterstützt die Umleitung benutzerdefinierter Protokolle vom Citrix VDA zum Client. Andere Protokolle als HTTP oder HTTPS werden unterstützt. Lesen Sie zum Konfigurieren der bidirektionalen Inhaltsumleitung die Anweisungen zur [Konfiguration] unter (/en-us/citrix-virtual-apps-desktops/2402-ltsr/general-content-redirection/bidirectional-content-redirection-configuration/bidirectional-content-redirection#configuration).

Stellen Sie in Web Studio das benutzerdefinierte Protokoll unter **Bidirektionale Inhaltsumleitung** ein.

> **Hinweis:**
>
> - Sie müssen über Administratorrechte verfügen, um diese Befehle ausführen zu können.
> - Beim Client muss eine Anwendung registriert sein, damit das Protokoll verarbeitet werden kann. Andernfalls wird die URL zum Client umgeleitet und kann nicht gestartet werden.
> - Benutzerdefinierte Protokoll-URLs, die Sie in den Browsern Chrome und Edge eingeben oder starten, werden nicht unterstützt und nicht umgeleitet.
> - Die folgenden Protokolle werden nicht unterstützt: `rtsp://`, `rtspu://`, `pnm://`, `mms://`.

### 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.
- Vergewissern Sie sich, 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.
- 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.

## Host-zu-Client-Umleitung

June 27, 2024

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.

```
1 <?xml version="1.0" encoding="UTF-8"?>
```

```
2
3  <DefaultAssociations>
4
5  <Association Identifier="http" ProgId="ServerFTAHTML" ApplicationName="
       ServerFTA" />
6
7  <Association Identifier="https" ProgId="ServerFTAHTML" ApplicationName=
       "ServerFTA" />
8
9  </DefaultAssociations>
10 <!--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. Erstellen 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: `http`, `https`, `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 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.

## Lokaler App-Zugriff und URL-Umleitung

June 27, 2024

### 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 neu 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. URL-Sperr- und Positivlisten werden nicht 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:

- Edge, neueste Version
- Firefox, neueste Version und Extended Support Release
- Chrome, neueste Version

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. Standardmäßig ist der lokale App-Zugriff nicht zulässig.

### 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 auch die Richtlinie für URL-Positiv- und -Sperrlisten für die URL-Umleitung konfigurieren. Weitere Informationen finden Sie unter Einstellungen der Richtlinie "Lokaler App-Zugriff".

### Aktivieren von lokalem App-Zugriff und URL-Umleitung

Führen Sie die folgenden Schritte aus, um den lokalen App-Zugriff für alle lokalen Anwendungen zu aktivieren:

1. Melden Sie sich bei Web Studio an und klicken Sie im linken Bereich auf **Richtlinien**.
2. Klicken Sie in der Aktionsleiste auf **Richtlinie erstellen**.
3. Geben Sie im Fenster "Richtlinie erstellen"den Begriff "Lokalen App-Zugriff zulassen"im Suchfeld ein und klicken Sie auf **Auswählen**.
4. 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.
5. 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.
6. Klicken Sie im Fenster "Einstellung bearbeiten"auf **Hinzufügen**, um die URLs hinzuzufügen, und klicken Sie auf **OK**.
7. 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.

8. Klicken Sie im Fenster "Einstellung bearbeiten"auf **Hinzufügen**, um die URLs hinzuzufügen, und klicken Sie auf **OK**.
9. Klicken Sie auf der Seite "Einstellungen"auf **Weiter**.
10. Weisen Sie die Richtlinie auf der Seite "Benutzer und Maschinen"den entsprechenden Bereitstellungsgruppen zu und klicken Sie auf **Weiter**.
11. 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 über den Registrierungs-Editor oder über das PowerShell-SDK bereitstellen.

Informationen zum Registrierungs-Editor finden Sie unter Lokaler App-Zugriff für veröffentlichte Anwendungen in der Liste der über die Registrierung verwalteten Features.

Verwendung des 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 DaaS Remote PowerShell SDK, um Zugriff auf **Anwendung für lokalen App-Zugriff hinzufügen** in einer Cloudservicebereitstellung zu erhalten. Weitere Informationen finden Sie unter Citrix DaaS 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. Melden Sie sich bei Web Studio an und wählen Sie im linken Bereich **Anwendungen**.
2. 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 in der Aktionsleiste auf **Anwendung für lokalen App-Zugriff hinzufügen** klicken. Klicken Sie auf **Aktualisieren**, um in der Aktionsleiste die Option “Anwendung für lokalen App-Zugriff hinzufügen”anzuzeigen.
3. 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 zur ausführbaren Datei für die Anwendung auf der lokalen Maschine des Benutzers ein und geben Sie den Pfad zu dem Ordner ein, in dem sich die Anwendung befindet. 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\HDX\bin\VDARedirector.exe /regAll

#### URL-Interception in Browsern

- Standardmäßig wird die angegebene URL von Internet Explorer umgeleitet. Wenn die URL nicht in der Sperrliste enthalten ist und dennoch vom Browser oder der Website an eine andere URL-Adresse umgeleitet wird, wird die endgültige URL nicht umgeleitet. Sie wird nicht umgeleitet, selbst wenn sie in der Sperrliste enthalten ist.

Zum richtigen Funktionieren der URL-Umleitung müssen Sie bei entsprechender Aufforderung durch den Browser das Add-On aktivieren. Wenn die mit Internetoptionen verbundenen Add-Ons bzw. die angeforderten Add-Ons deaktiviert sind, funktioniert die URL-Umleitung nicht richtig.

- Firefox-Add-Ons leiten URLs immer um.

Wenn ein Add-On installiert wurde, bietet Firefox auf einer neuen Registerkarte die Möglichkeit, die Add-On-Installation zuzulassen oder zu verhindern. Lassen Sie das Add-On zu, damit das Feature funktioniert.

- Chrome-Add-Ons leiten die endgültige URL stets um, wenn es sich um geleitete und nicht eingegebene URLs handelt.

Die Erweiterungen wurden extern installiert. Wenn Sie die Erweiterung deaktivieren, funktioniert die URL-Umleitung in Google Chrome nicht. Wenn die URL-Umleitung im Inkognito-Modus erforderlich ist, lassen Sie durch Auswählen dieser Option in den Browsereinstellungen zu, dass die Erweiterung im Inkognito-Modus ausgeführt wird.

#### Konfigurieren des Verhaltens von lokalen Anwendungen bei der Abmeldung und Trennung

> **Hinweis:**
>
> Wenn Sie die Einstellungen nicht mit dem unten aufgeführten Verfahren konfigurieren, werden

> lokale Anwendungen standardmäßig weiter ausgeführt, wenn ein Benutzer sich abmeldet oder die Verbindung zum virtuellen Desktop trennt. Nach der Wiederverbindung werden lokale Anwendungen wieder integriert, wenn sie auf dem virtuellen Desktop verfügbar sind.

Informationen zum Konfigurieren des Verhaltens lokaler Anwendungen beim Abmelden und Trennen finden Sie unter Verhalten lokaler Anwendungen beim Abmelden und Trennen in der Liste der über die Registrierung verwalteten Features.

## Generische USB-Umleitung und Clientlaufwerke

June 27, 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 Einstel-

lungen für die Citrix Richtlinie "USB-Geräte" für die generische USB-Umleitung und für die optimierte Unterstützung.
- Die Citrix Richtlinieneinstellung unter 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.

### 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, Windows Server 2016, Windows Server 2019 oder Windows Server 2022 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.

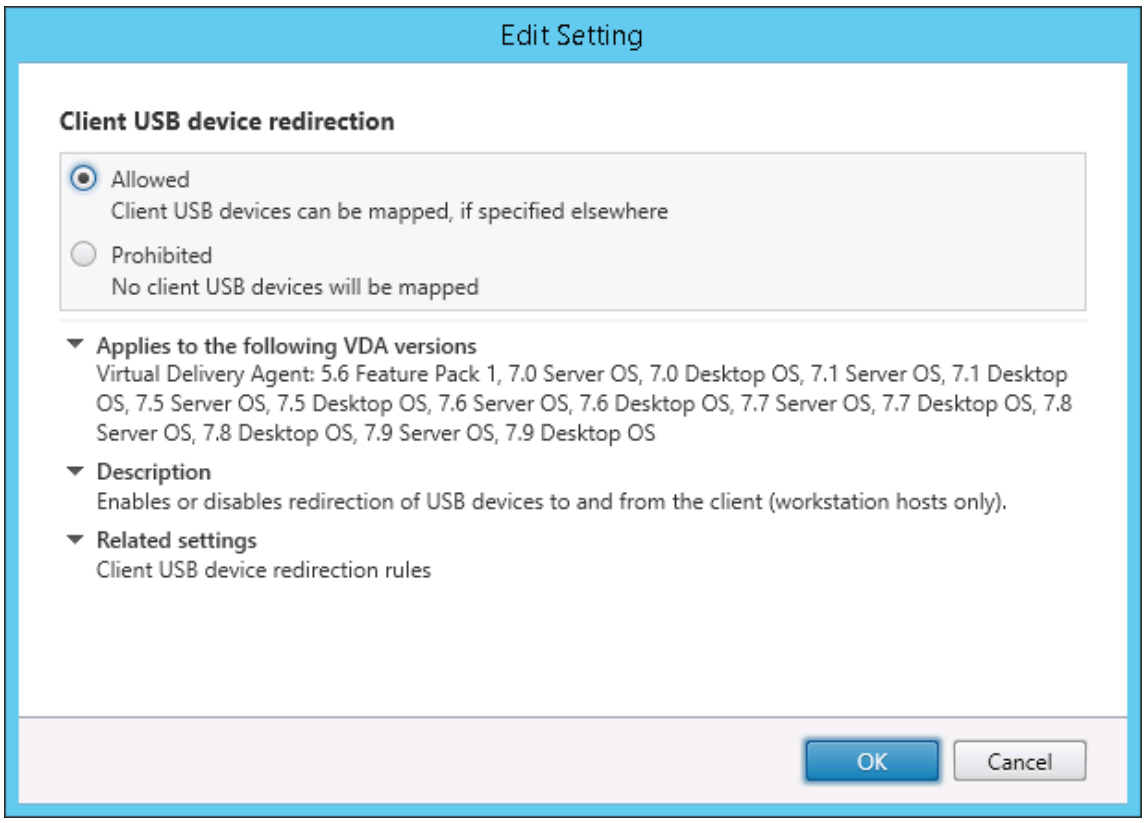
### Aktivieren der generischen USB-Umleitung

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.

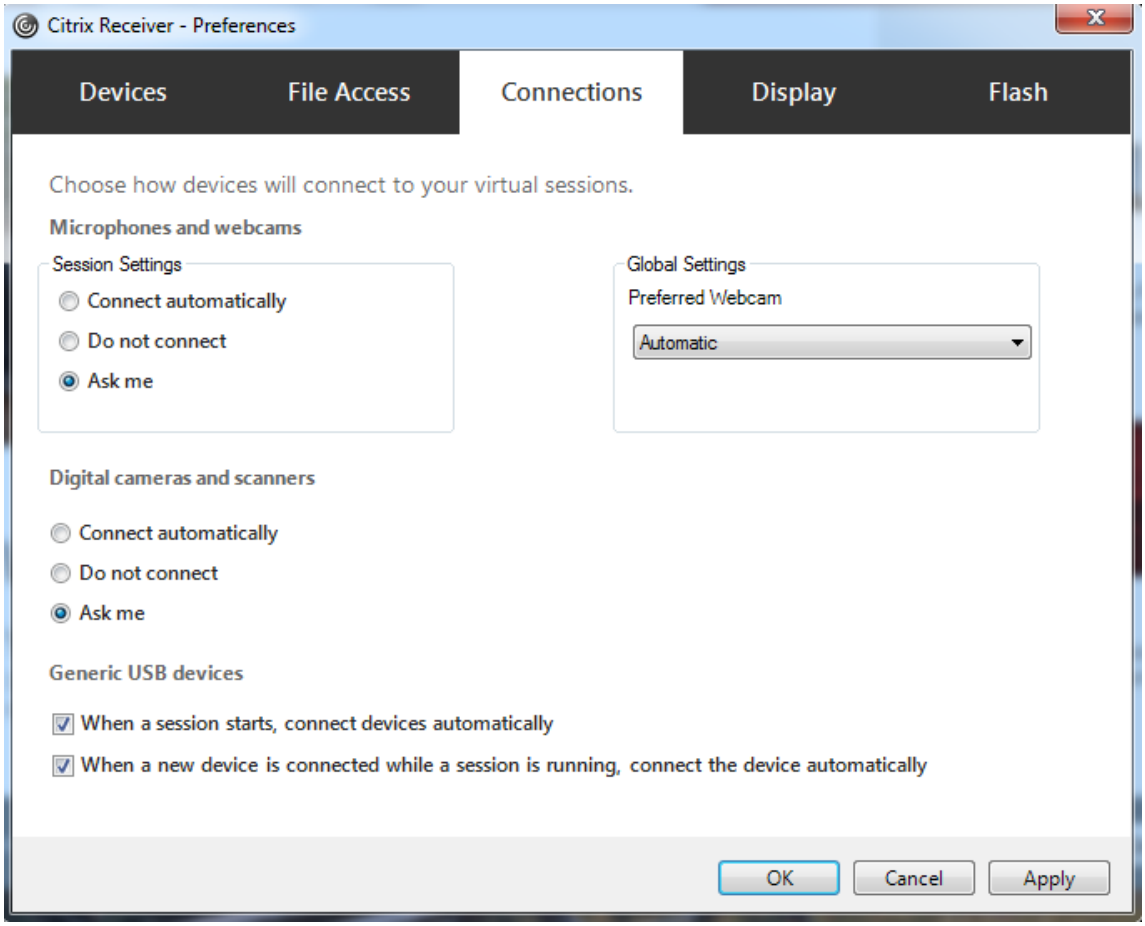



2. Optional: Zum Aktualisieren der Liste der zur Umleitung verfügbaren USB-Geräte fügen Sie die Einstellung Regeln für die Client-USB-Geräteumleitung einer Richtlinie hinzu und stellen Sie die USB-Richtlinienregeln ein.

   Wenn die Richtlinieneinstellungen angegeben sind, führen Sie in der Citrix Workspace-App folgende Schritte aus:

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.

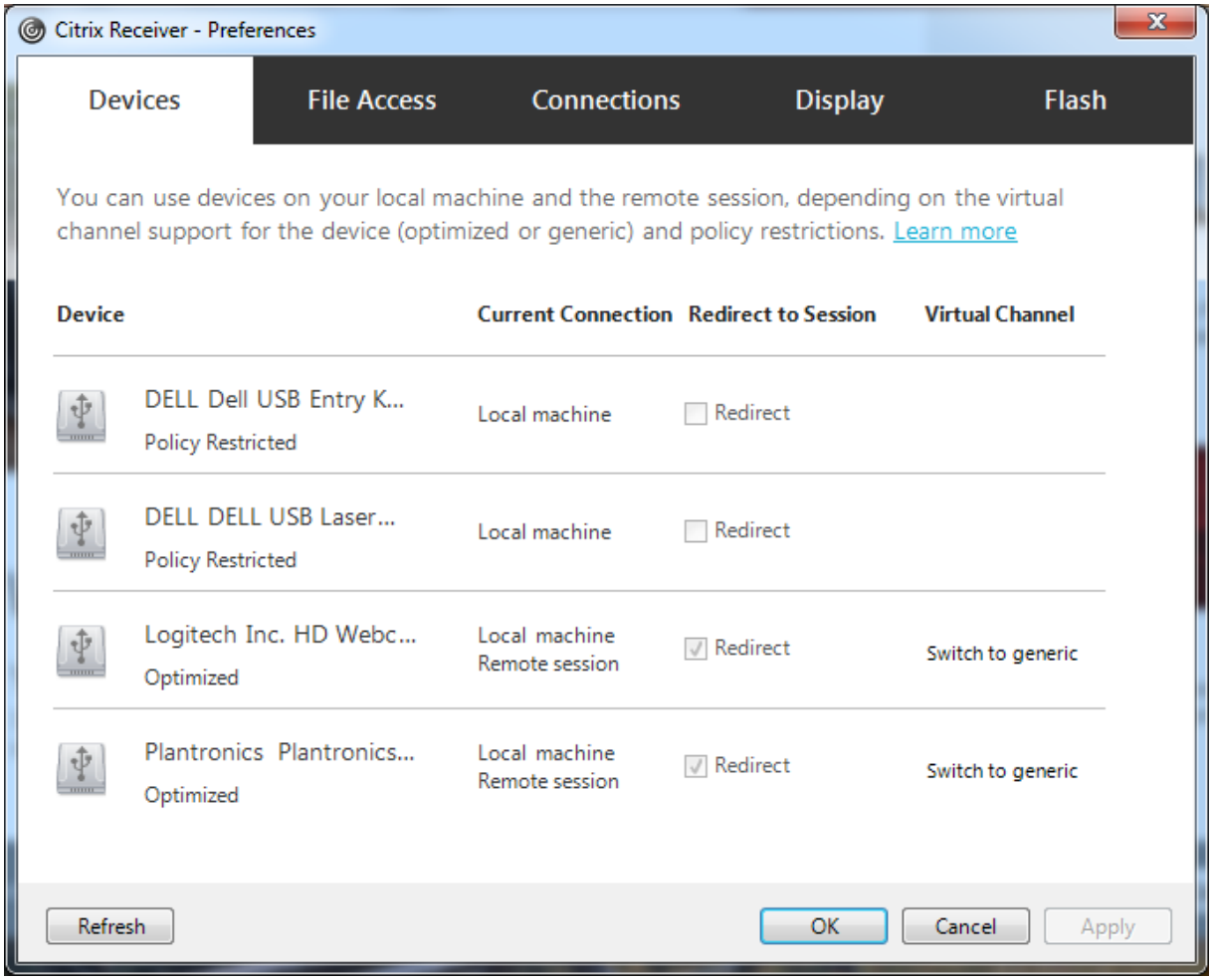
Informationen zur USB-Unterstützung Für Thin Clients und die erforderliche Konfiguration erhalten Sie vom Hersteller.

### 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 fest, welche die USB-Standardrichtlinienregeln außer Kraft setzen.

Citrix DaaS (früher Citrix Virtual Apps and Desktops Service):

- In den meisten Fällen laden Sie das MSI für die Citrix Gruppenrichtlinien-Verwaltungskonsole (`CitrixGroupPolicyManagement_x64.msi`) herunter installieren es in Ihrem Active Directory und verwalten dann die AD-Gruppenrichtlinien. (Installieren Sie das MSI nicht auf einem VDA.)
- Bearbeiten Sie für die Citrix Workspace-App für Windows die Benutzergeräteregistrierung. Das Installationsmedium enthält eine administrative Vorlage (ADM-Datei), mit der Sie Benutzergeräte über folgende Active Directory-Gruppenrichtlinie ändern können: dvd root `\os\lang\Support\Configuration\icaclient_usb.adm`

On-Premises-Citrix Virtual Apps and Desktops:

- VDA: Bearbeiten Sie die Administrator-Überschreibungsregeln für Maschinen mit Multisitzungs-OS mit den Gruppenrichtlinienregeln. Die Gruppenrichtlinien-Verwaltungskonsole ist auf dem Installationsmedium enthalten:
  - x64: DVD-Stamm`\os\lang\x64\Citrix Policy\CitrixGroupPolicyManagement_x64.msi`
  - x86: DVD-Stamm `\os\lang\x86\Citrix Policy\CitrixGroupPolicyManagement_x86.msi`
- Bearbeiten Sie für die Citrix Workspace-App für Windows die Benutzergeräteregistrierung. Das Installationsmedium enthält eine administrative Vorlage (ADM-Datei), mit der Sie Benutzergeräte über folgende 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. Erstellen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

Die Standardregeln des Produkts werden in HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\GenericUSB 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 HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\PortICA\GenericUSE 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:**
>
> - Ab Citrix Virtual Apps and Desktops Version 2212 ist für einige USB-Geräte die Verwendung der generischen USB-Umleitung deaktiviert. Sie müssen diese Geräte explizit unter Angabe der Hersteller-ID (VID) und Produkt-ID (PID) hinzufügen.
> - 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.

# Drucken

June 27, 2024

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 Einstellungen 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.

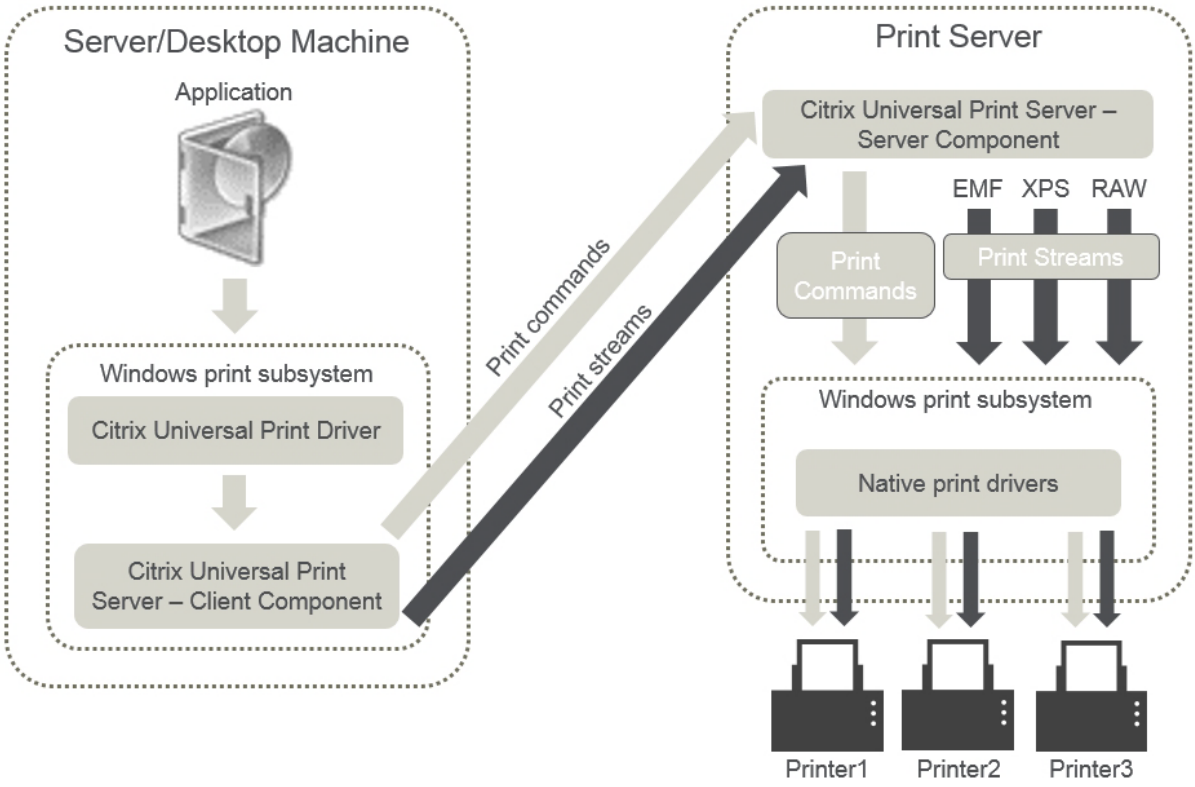
Der universelle Druckserver umfasst als Feature die folgenden Komponenten:

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.

- **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

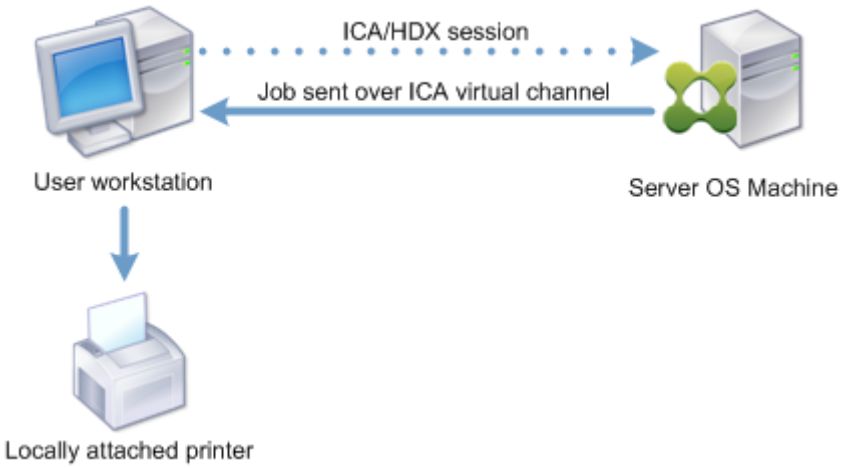
Der Begriff Druckpfad umfasst den Pfad, über den Druckaufträge weitergeleitet werden, und den Speicherort, an dem Druckaufträge gespoolt werden. Beide Aspekte dieses Konzepts sind wichtig. Die Weiterleitung wirkt sich auf den Netzwerk-Datenverkehr aus. Das Spooling wirkt sich auf die Auslastung der lokalen 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**

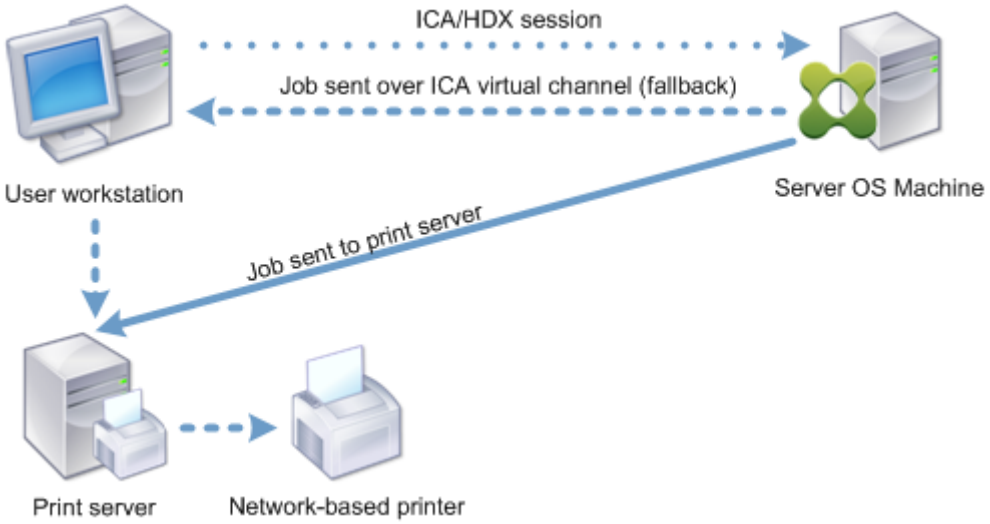
Standardmäßig werden alle für Netzwerkdrucker bestimmten Druckaufträge von der Multisitzungs-OS-Maschine über das Netzwerk direkt an den Druckserver weitergeleitet. In folgenden Situationen werden jedoch Druckaufträge automatisch über die ICA-Verbindung geleitet:

- 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:

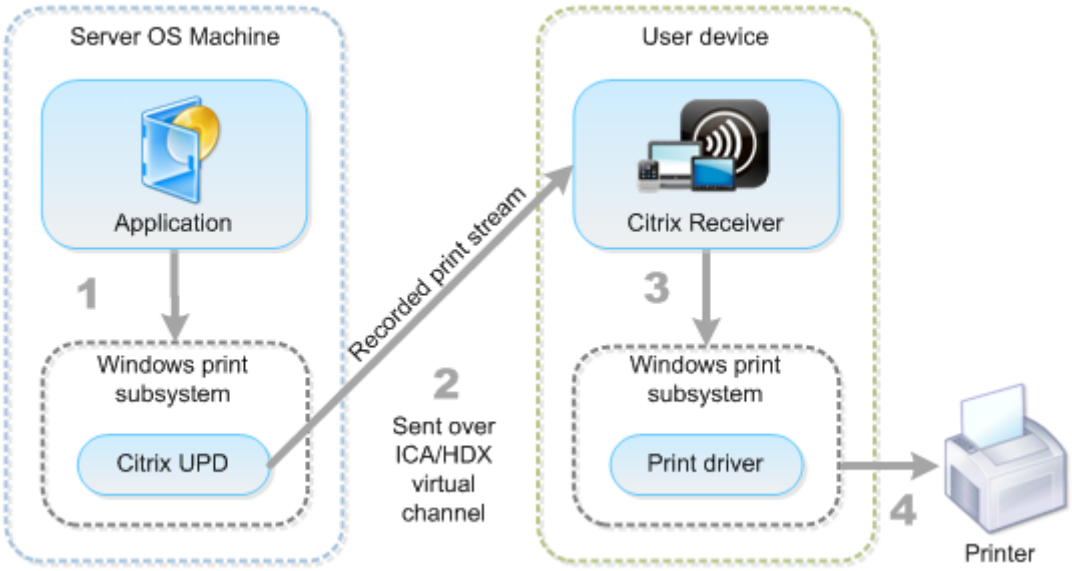
 

- Enhanced Metafile Format (**EMF**), Standard. EMF ist die 32-Bit-Version von Windows Metafile Format (WMF). Der EMF-Treiber kann nur von Windows-Clients verwendet werden.
- XML-Papierspezifikation (**XPS**). Der Windows XPS-Treiber verwendet XML zum Erstellen eines plattformunabhängigen elektronischen 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.



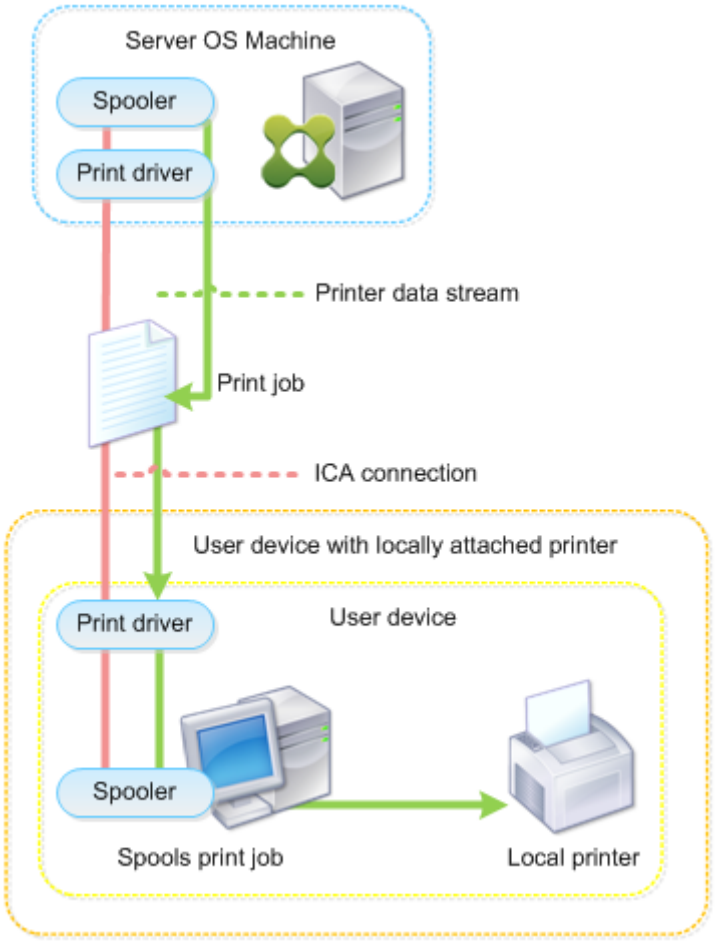

Legen Sie bei der Planung der Strategie zur Treiberverwaltung fest, ob Sie gerätespezifische Treiber,

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
- Druckumgebung pflegen

## Druckkonfigurationsbeispiele

June 27, 2024

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.

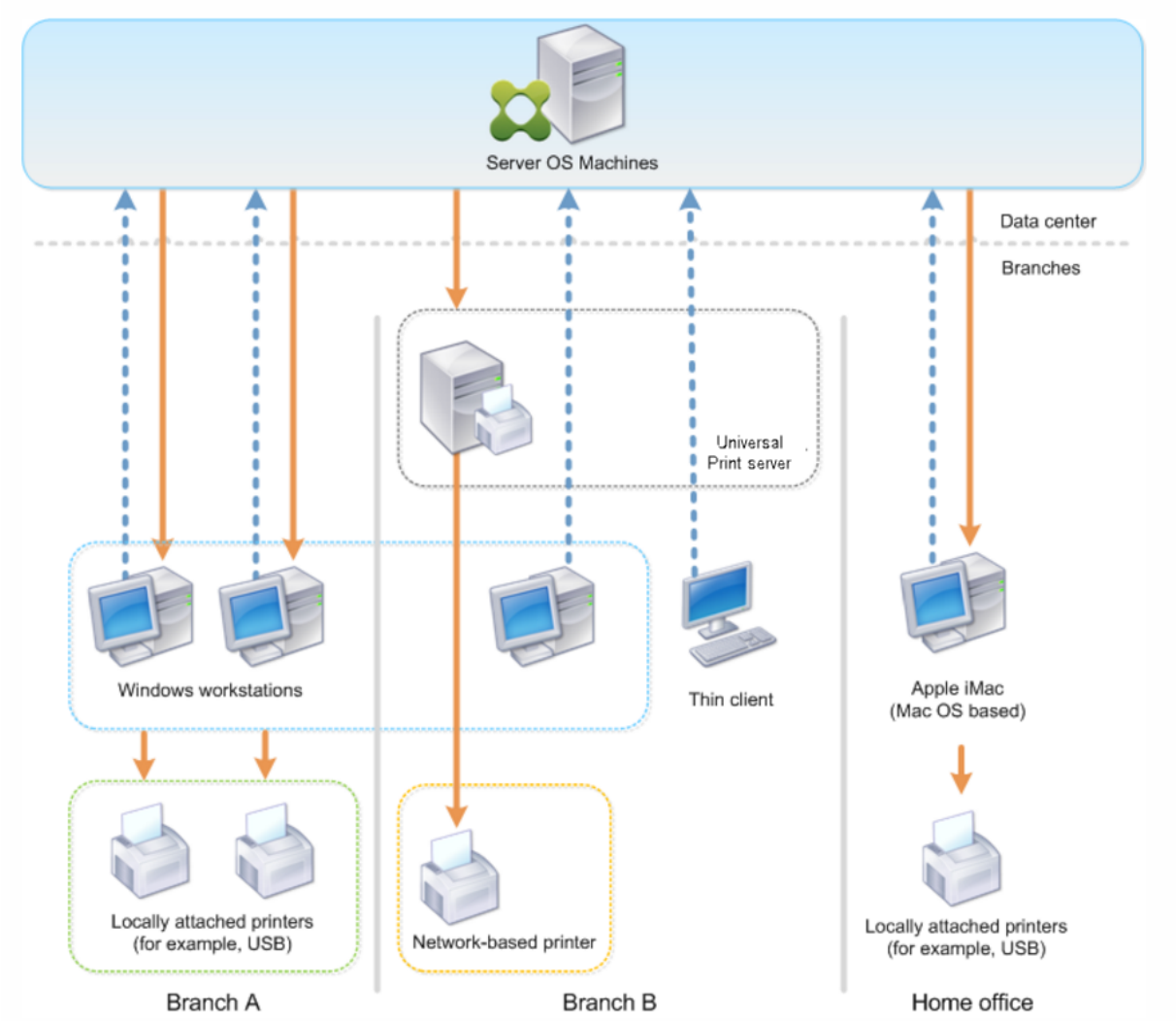
### Beispiel einer Druckbereitstellung

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.

### Citrix Universeller 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

June 27, 2024

### 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

June 27, 2024

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

June 27, 2024

### Citrix Universeller 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. Erstellen 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

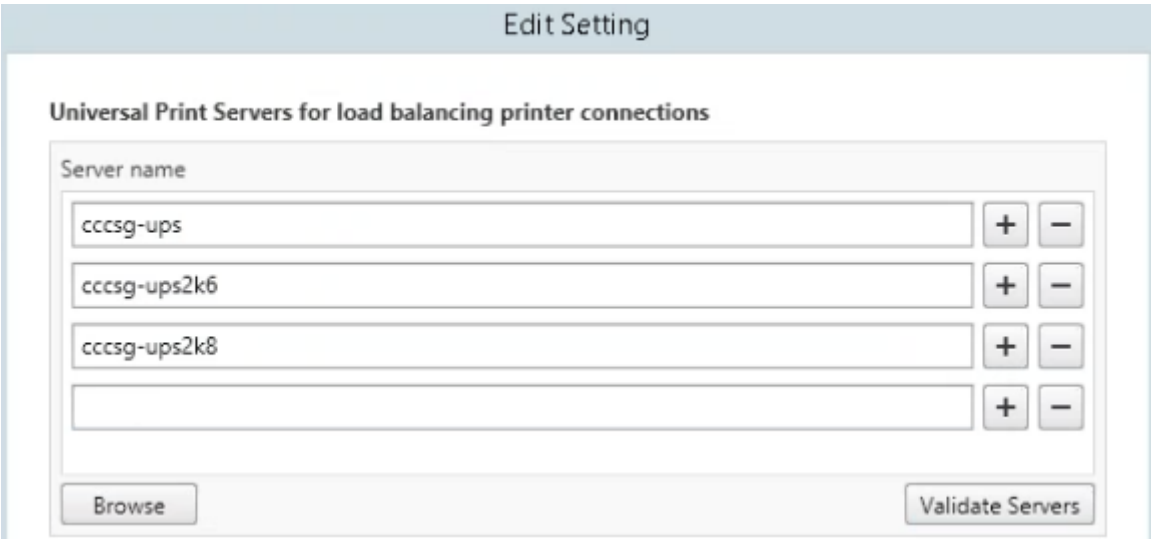
 

universeller Druckserver den folgenden Registrierungsschlüssel erstellen und die Portnummer ändern:

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.

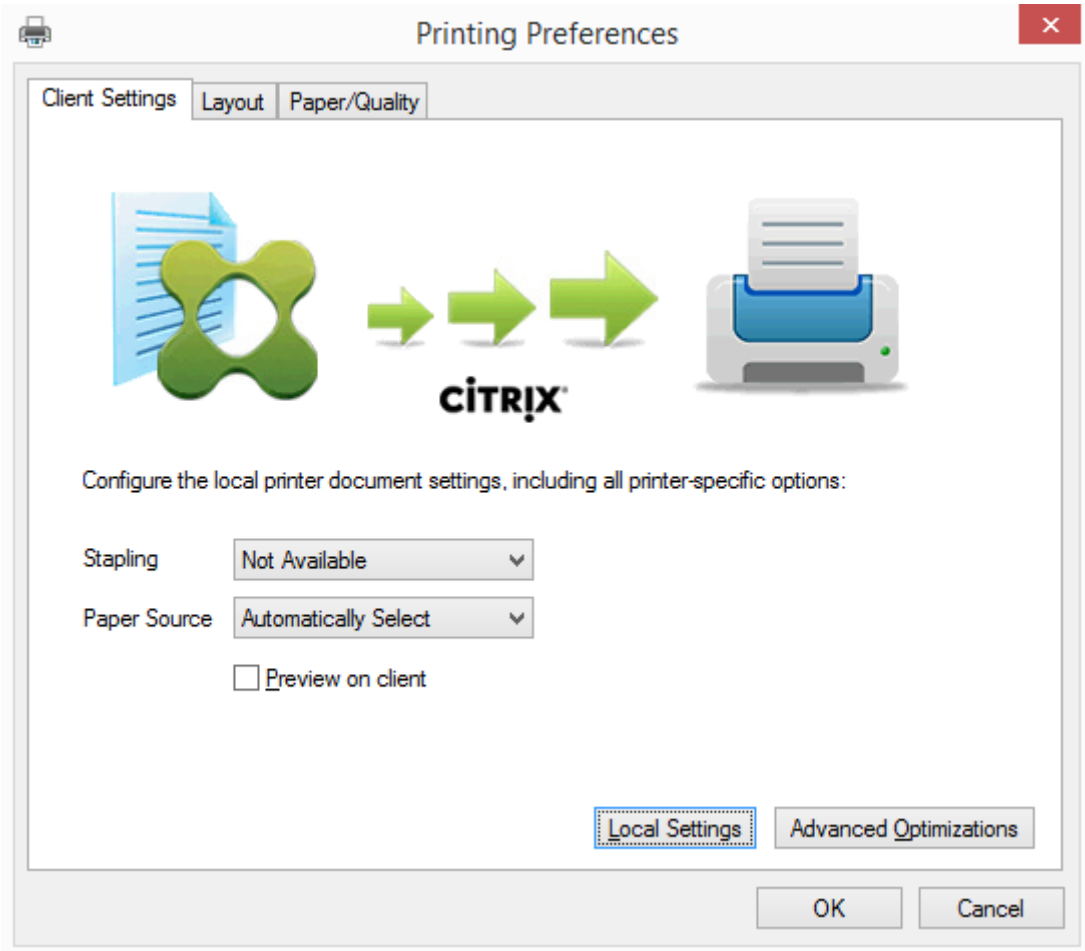
| Richtlinieneinstellung | Interaktion |
| --- | --- |
| Clientdruckerumleitung, automatisches Erstellen von Clientdruckern | Wenn der universelle Druckserver aktiviert ist, werden Clientnetzwerkdrucker mit dem universellen Druckertreiber statt den systemeigenen Treibern erstellt. Den Benutzern wird 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:

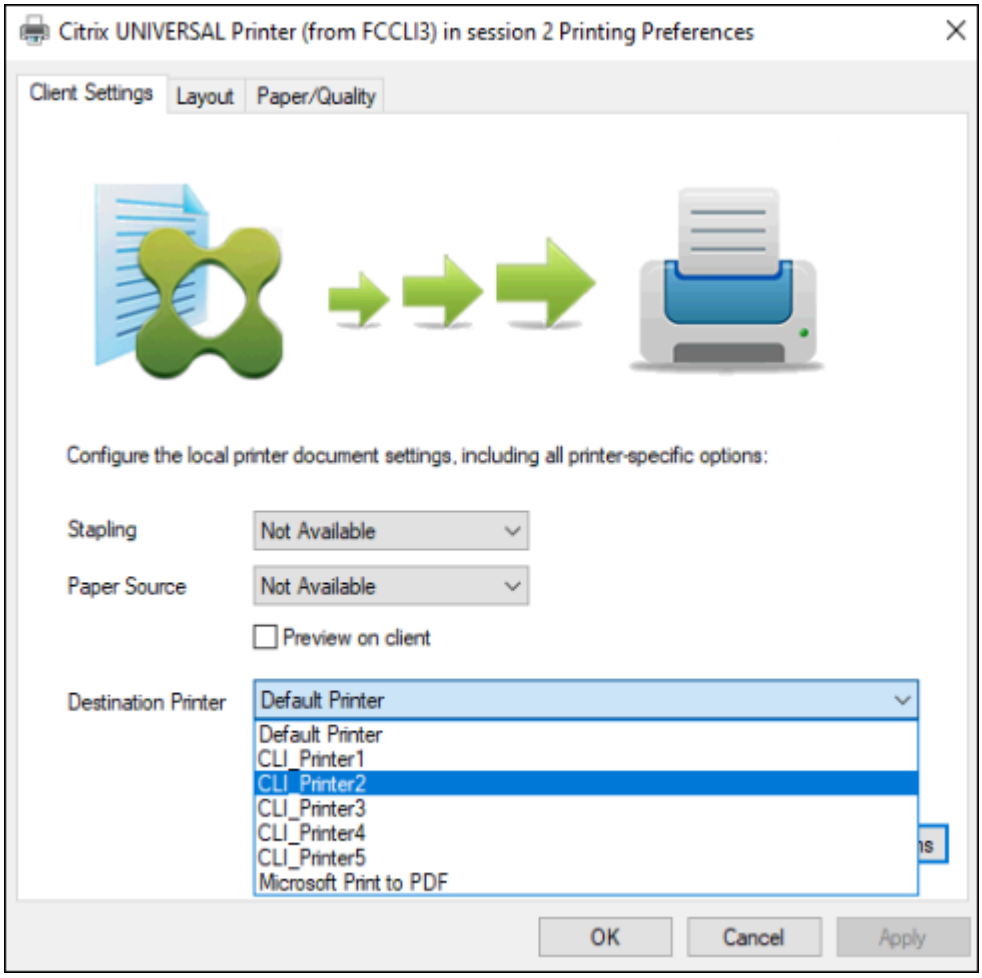
- **Citrix Universeller Drucker** - ein generischer Drucker, der zu Beginn einer Sitzung erstellt wird und nicht an ein Druckgerät gebunden ist. Wenn Sie den Citrix Universellen Drucker automatisch erstellen und nur diesen Drucker verwenden, kann dies den Ressourcenverbrauch reduzieren und die Anmeldezeiten für Benutzer verkürzen. 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 Citrix Workspace-Apps benötigen, die nicht unter Windows ausgeführt werden, verwenden Sie einen der anderen universellen Druckertreiber, die Postscript- oder PCL-basiert sind.

  Mit dem Citrix Universellen Drucker können Sie den Standarddrucker des Clients oder einen bestimmten Clientdrucker als Druckziel auswählen. Um einen bestimmten Drucker für einen Druckauftrag auszuwählen, öffnen Sie das Dialogfeld **Druckeinstellungen**. Wählen Sie das Dropdownmenü **Zieldrucker**. Die Option **Standarddrucker** sendet Druckaufträge an den Standarddrucker des Clients. Ebenfalls aufgeführt sind alle vom Client umgeleiteten Drucker, die an den Endpunkt angeschlossen sind, auf dem die Sitzung ausgeführt wird. Der von Ihnen gewählte Drucker wird als Zieldrucker für alle zukünftigen Druckaufträge gespeichert.




- **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.

## Druckumgebung pflegen

June 27, 2024

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 |

| | | Druckmodell |
|---|---|---|
| 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.

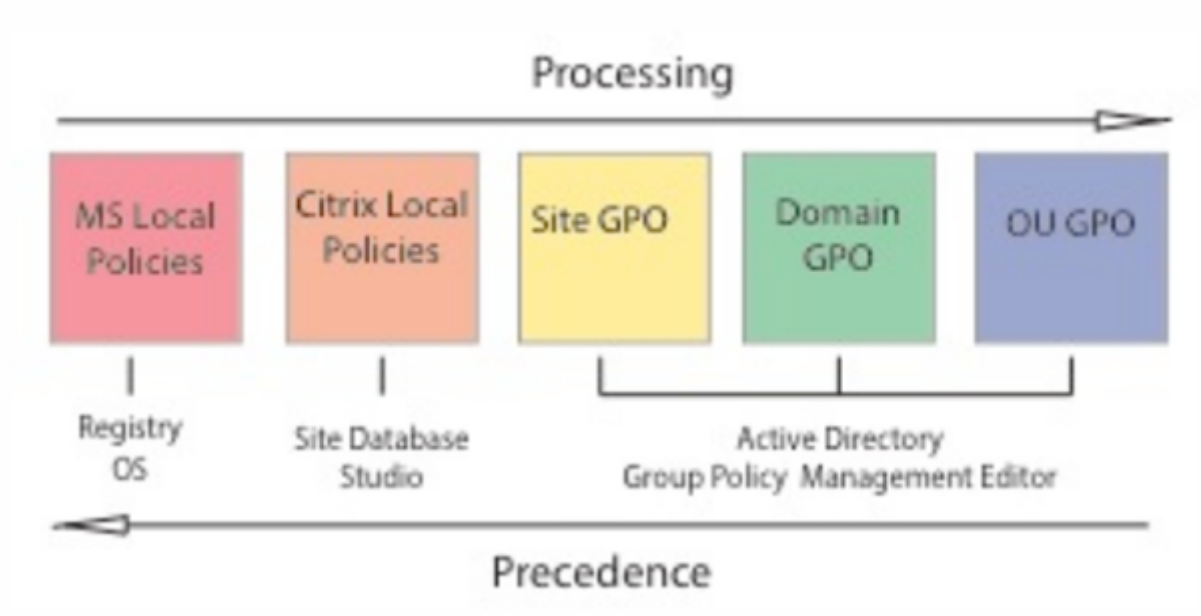
## Richtlinien

June 27, 2024

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 Ebene der Sitegruppenrichtlinienobjekte überschreibt alle lokalen Richtlinien von Microsoft und Citrix, die mit ihnen in Konflikt stehen.

Alle lokalen Citrix Richtlinien werden in der Web 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 (GPMC) festlegen, um Einstellungen zu konfigurieren. Sie können sie außerdem auf eine Zielgruppe von Benutzern auf unterschiedlichen Ebenen des Netzwerks anwenden.

Diese Gruppenrichtlinienobjekte werden in Active Directory gespeichert. 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. Ab-

hängig 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 bestimmen, für wen oder was die Richtlinie gilt.

> **Hinweis:**
>
> Das Verwenden von Windows- und Citrix-Richtlinien im gleichen GPO wird nicht unterstützt.

## Richtlinien einsetzen

June 27, 2024

> **Hinweis:**
>
> Sie können Ihre Citrix Virtual Apps and Desktops-Bereitstellung mithilfe von zwei Verwaltungskonsolen verwalten: Web Studio (webbasiert) und Citrix Studio (Windows-basiert). Dieser Artikel behandelt nur Web Studio. Informationen zu Citrix Studio finden Sie im entsprechenden Artikel in Citrix Virtual Apps and Desktops 7 2212 oder früher.

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 mit Citrix Richtlinien verwenden.

- **Web Studio.** Wenn Sie ein Citrix Administrator ohne Berechtigung zum Verwalten von Gruppenrichtlinien sind, verwenden Sie Web Studio, um Richtlinien für Ihre Site zu erstellen. Mit Web Studio erstellte Richtlinien werden in der Sitedatenbank gespeichert und Updates werden per Push auf den VDA übertragen, wenn der VDA beim Broker registriert wird oder ein Benutzer eine Verbindung mit dem VDA herstellt.
- **Editor für lokale Gruppenrichtlinien** (Snap-In der Microsoft Management Console). Wenn Sie in Ihrer Netzwerkumgebung Active Directory verwenden und zur Verwaltung von Gruppenrichtlinien berechtigt sind, 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:**
>
> Wie empfehlen, einige Richtlinieneinstellungen mit dem Editor für lokale Gruppenrichtlinien zu konfigurieren. Dazu gehören Einstellungen, die sich auf Registrieren von VDAs bei einem Controller beziehen, und Einstellungen zu Microsoft App-V-Servern.
> Zusätzliche Richtlinienvalidierungen wurden hinzugefügt. Daher kann ein direktes Upgrade zum Verlust von Richtliniendaten führen, wenn ungültige Richtlinieneinstellungen vorhanden sind. Wenn Sie die Richtlinien mit einer anderen Methode als Web Studio erstellen oder bearbeiten, empfiehlt Citrix, die neueste Version des SDK und des Snap-Ins zu verwenden.

### Reihenfolge und Priorität bei der Richtlinienverarbeitung

Gruppenrichtlinieneinstellungen (GPOs) werden in der folgenden Reihenfolge verarbeitet:

1. Lokale GPO
2. GPO für Virtual Apps and Desktops-Site (in der Sitedatenbank gespeichert)
3. GPOs auf Siteebene
4. GPOs auf Domänenebene
5. Organisationseinheiten

Bei einem Konflikt überschreiben Richtlinieneinstellungen, die zuletzt verarbeitet wurden, vorher verarbeitete Einstellungen. Es gilt folgende Rangfolge für Richtlinieneinstellungen:

1. Organisationseinheiten

2. GPOs auf Domänenebene
3. GPOs auf Siteebene
4. GPO für Virtual Apps and Desktops-Site (in der Sitedatenbank gespeichert)
5. Lokale GPO

Beispiel: Ein Citrix Administrator erstellt in Web Studio eine Richtlinie (Richtlinie A), mit der die Clientdateiumleitung für das Vertriebsteam 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 Vertriebsmitarbeiter sich an den virtuellen Desktops anmelden, wird Richtlinie B angewendet und Richtlinie A ignoriert. Der Grund dafür ist, dass Richtlinie B auf der Domänenebene und Richtlinie A auf der Ebene der Virtual Apps and Desktops-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. Diese Einstellung umfasst Einstellungen, die sich auf typische RDP-Clientverbindungseinstellungen beziehen. Beispiele für RDP-Clientverbindungseinstellungen sind Desktophintergrund, Menüanimationen und das Anzeigeverhalten bei Drag & Drop.

Wenn Sie mehrere Richtlinien verwenden, können Sie Richtlinien, deren Einstellungen Konflikte verursachen, Prioritäten zuweisen. Weitere Informationen 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.

> **Hinweis:**
>
> Sie öffnen den Citrix Gruppenrichtlinien-Modellierungsassistenten, indem Sie zu der Registerkarte **Richtlinien > Modellierung** gehen und in der Aktionsleiste auf **Modellierungsassistenten starten** klicken. Die Registerkarte **Modellierung** ist auf Kundenwunsch in Web Studio verfügbar.

### 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 Web Studio sind die Richtlinieneinstellungen je nach Funktionalität bzw. Feature, für die bzw. das sie gelten, in Kategorien eingeteilt. Beispielsweise umfasst 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 linken Bereich von Web Studio **Richtlinien** auswählen.

  - Die Registerkarte **Richtlinien** listet alle Richtlinien auf. Bei Auswahl einer Richtlinie werden unten folgende Registerkarten angezeigt:
    - Übersicht –Name, Priorität, Status (aktiviert/deaktiviert) und Beschreibung
    - Einstellungen –Liste aller konfigurierten Einstellungen
    - Zugewiesen zu –Benutzer- und Maschinenobjekte, denen die Richtlinie zugewiesen wurde.
      Weitere Informationen finden Sie unter Erstellen von Richtlinien.
  - Auf der Registerkarte **Vorlagen** sehen Sie von Citrix bereitgestellte Vorlagen und benutzerdefinierte Vorlagen, die Sie erstellt haben. Bei Auswahl einer Vorlage werden unten folgende Registerkarten angezeigt:
    - Beschreibung (wofür Sie die Vorlage verwenden können)
    - Einstellungen (Liste der konfigurierten Einstellungen). Weitere Informationen finden Sie unter Richtlinienvorlagen.
  - Mit der Registerkarte **Vergleich** können Sie die Einstellungen einer Richtlinie oder Vorlage mit den Einstellungen 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.

Suchen nach einer Einstellung in einer Richtlinie oder Vorlage

1. Wählen Sie die Richtlinie oder Vorlage aus.
2. Wählen Sie in der Aktionsleiste die Option **Richtlinie bearbeiten** oder **Vorlage bearbeiten**.
3. Geben Sie auf der Seite **Einstellungen** den Namen der Einstellung im **Suchfeld** ein.

   Sie können Ihre Suche verfeinern, indem Sie Folgendes auswählen:

   - Eine bestimmte Produktversion
   - Eine Kategorie (z. B. Bandbreite)
   - Schlüsselwörter im Namen der Einstellung
   - Das Kontrollkästchen **Nur ausgewählte anzeigen**
   - Sie suchen nur nach Einstellungen, 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.

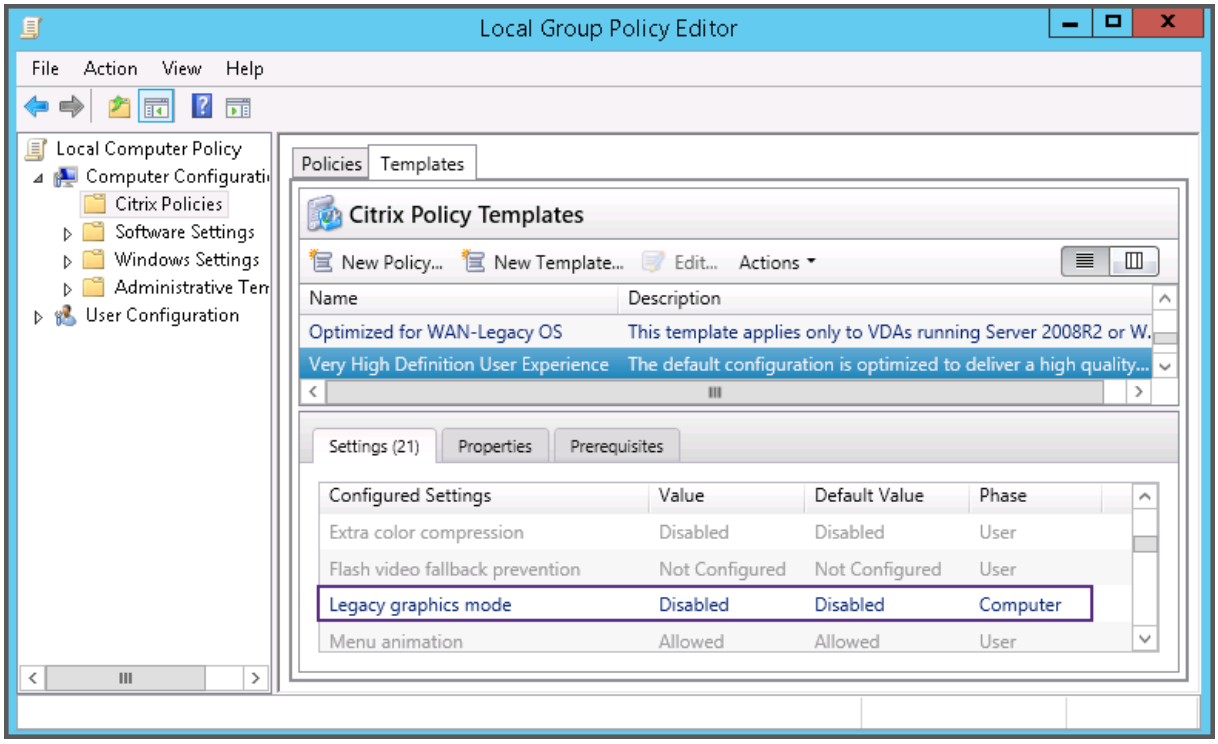
Sie können die Suche verfeinern, indem Sie eine bestimmte Produktversion oder Kategorie auswählen. Für eine ungefilterte Suche wählen Sie **Alle Einstellungen**.

Eine Richtlinie ist nach ihrer Erstellung unabhängig von der verwendeten Vorlage. Sie können in das Feld **Beschreibung** eingeben, auf welcher Vorlage die neue Richtlinie basiert.

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

June 27, 2024

> **Hinweis:**
>
> Sie können Ihre Citrix Virtual Apps and Desktops-Bereitstellung mithilfe von zwei Verwaltungskonsolen verwalten: Web Studio (webbasiert) und Citrix Studio (Windows-basiert). Dieser Artikel behandelt nur Web Studio. Informationen zu Citrix Studio finden Sie im entsprechenden Artikel in Citrix Virtual Apps and Desktops 7 2212 oder früher.

Vorlagen sind Sammlungen von Einstellungen, deren Verwendung bei der Erstellung von Richtlinien empfohlen wird, um bestimmte Ergebnisse zu erzielen. Um beispielsweise Richtlinien für die Bereitstellung einer High-Definition-Benutzererfahrung für Endbenutzer zu erstellen, können die in der Vorlage “Besonders gute High Definition-Benutzererfahrung”definierten Einstellungen als Referenz und Ausgangspunkt für die Erstellung solcher Richtlinien verwendet werden.

Vorlagen sind keine Richtlinien. Vorlagen sind eine ergänzende Dokumentation für Citrix-Richtlinieneinstellungen. Sie demonstrieren die kollektiven Funktionen bestimmter benutzerbezogener Einstellungen.

Die Verwendung von Vorlagen ist optional. Administratoren können Richtlinien erstellen, ohne Vorlagen zu verwenden. Vorlagen sind nützlich für Administratoren, die eine allgemeine Vorstellung davon haben, wie eine Site konfiguriert werden sollte, sich aber nicht sicher sind, welche Einstellungen sie verwenden sollen, um die gewünschte Konfiguration zu erreichen.

Administratoren können die Vorlagen entweder mithilfe einer vorhandenen Vorlage oder einer vorhandenen Richtlinie oder von Grund auf neu erstellen.

### ADMX/ADML

Die hier beschriebenen Vorlagen für Citrix-Gruppenrichtlinien haben nichts mit den Windows-Richtlinienvorlagen zu tun. Bei den hier beschriebenen Vorlagen und den Vorlagen für Windows-Richtlinien handelt es sich um zwei unterschiedliche Konzepte. Die Citrix-Gruppenrichtlinienvorlagen sind keine ADMX-Dateien.

### Integrierte Citrix Vorlagen

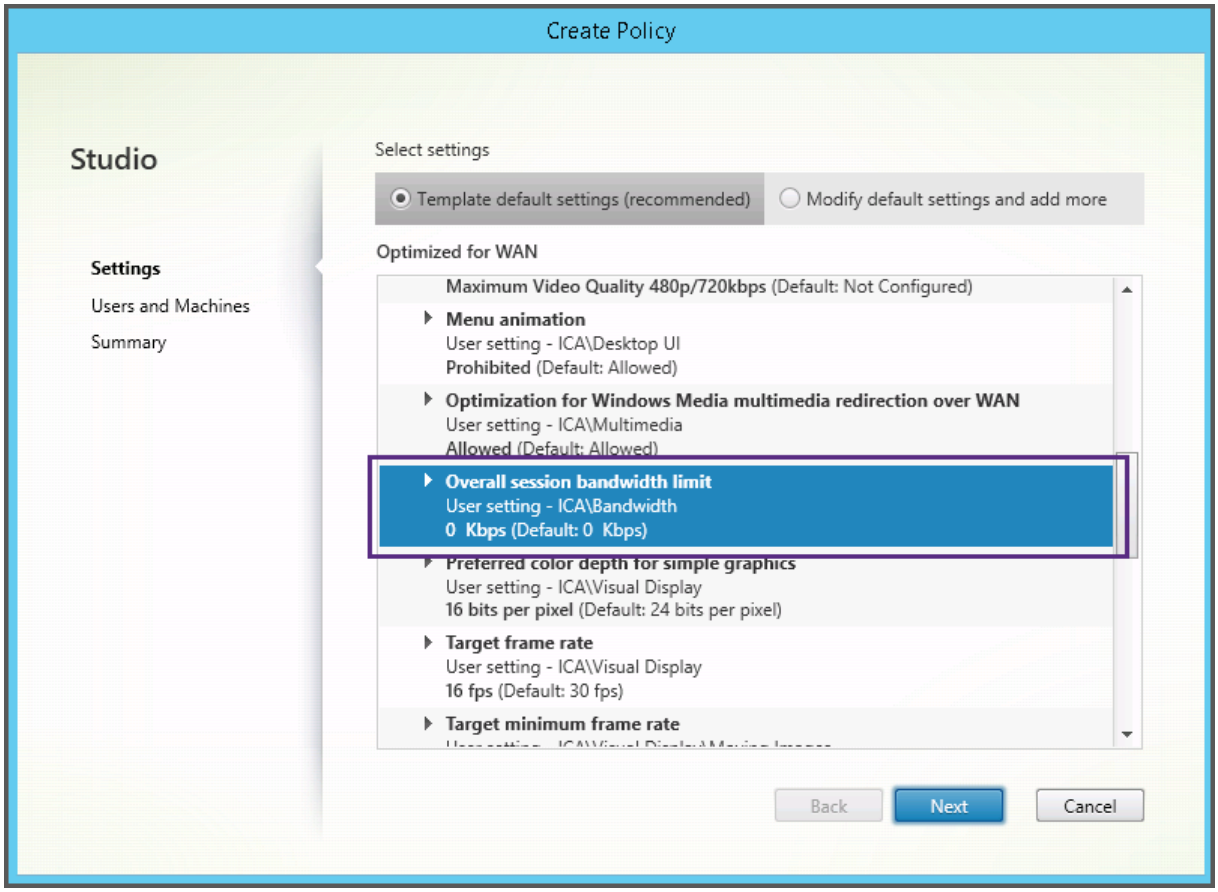
Die folgenden Richtlinienvorlagen sind verfügbar:

- **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.

### Vorlagen mit Web Studio erstellen und verwalten

Erstellen einer Vorlage basierend auf einer Vorlage:

1. Melden Sie sich bei Web Studio an und wählen Sie im linken Bereich **Richtlinien**.
2. Wählen Sie die Registerkarte **Vorlagen** und dann die Vorlage, mit der Sie eine Vorlage erstellen möchten.
3. Wählen Sie die Registerkarte **Vorlage erstellen**. Die Seite **Einstellungen auswählen** wird angezeigt.
4. Wählen und konfigurieren Sie die Richtlinieneinstellungen, die Sie in die Vorlage einschließen möchten.
5. Klicken Sie auf **Weiter**. Das Fenster **Zusammenfassung** wird angezeigt.
6. Geben Sie einen Namen für die Vorlage ein.
7. Klicken Sie auf **Fertigstellen**. Die neue Vorlage wird auf der Registerkarte **Vorlagen** angezeigt.

Erstellen einer Vorlage basierend auf einer Richtlinie:

1. Melden Sie sich bei Web Studio an und wählen Sie im linken Bereich **Richtlinien**.
2. Wählen Sie die Registerkarte **Richtlinien** und dann die Richtlinie, mit der Sie die Vorlage erstellen möchten.
3. Klicken Sie auf die Registerkarte **Mehr**.
4. Wählen Sie **Als Vorlage speichern**. Die Seite **Einstellungen auswählen** wird angezeigt.
5. Wählen und konfigurieren Sie die neuen Richtlinieneinstellungen, die Sie in die Vorlage einschließen möchten.
6. Klicken Sie auf **Weiter**. Das Fenster **Zusammenfassung** wird angezeigt.
7. Geben Sie einen Namen und eine Beschreibung für die Vorlage ein und klicken Sie auf **Fertig stellen**.

### Vorlagen und delegierte Administration

Vorlagen in Web Studio werden in der Site-Datenbank gespeichert, im Gegensatz zu den Vorlagen in Citrix Studio, die als Dateien im Benutzerprofilordner des aktuellen Administrators mit einer `.gpt`-Erweiterung gespeichert werden. Citrix Studio-Vorlagen, die von einem Administrator erstellt wurden, sind für andere Administratoren oder für denselben Administrator auf einer anderen Maschine nicht sichtbar. Web Studio-Vorlagen sind für alle Administratoren sichtbar, die über Berechtigungen und delegierte Verwaltung verfügen.

# Richtlinien erstellen

June 27, 2024

> **Hinweis:**
>
> Sie können Ihre Citrix Virtual Apps and Desktops-Bereitstellung mithilfe von zwei Verwaltungskonsolen verwalten: Web Studio (webbasiert) und Citrix Studio (Windows-basiert). Dieser Artikel behandelt nur Web Studio. Informationen zu Citrix Studio finden Sie im entsprechenden Artikel in Citrix Virtual Apps and Desktops 7 2212 oder früher.

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. Sie können auch die gleichen Kriterien verwenden wie für Windows Active Directory-Gruppenrichtlinien.

Wenn Sie bereits eine Richtlinie für eine Gruppe erstellt haben, sollten Sie möglichst diese Richtlinie bearbeiten, statt eine andere Richtlinie zu erstellen. Nach dem Bearbeiten der Richtlinie konfigurieren Sie die entsprechenden Einstellungen. Vermeiden Sie es, eine Richtlinie zu erstellen, deren einziger Zweck ist, eine bestimmte Einstellung zu aktivieren oder bestimmte Benutzer von der Richtlinie auszunehmen.

Sie können eine Richtlinie basierend auf einer Richtlinienvorlage erstellen und die Einstellungen nach Bedarf anpassen. Sie können die Richtlinie aber auch ohne Vorlage erstellen und alle benötigten Einstellungen hinzufügen.

In Web Studio werden neu erstellte Richtlinien auf “Deaktiviert”festgelegt, sofern das Kontrollkästchen **Richtlinie aktivieren** nicht explizit aktiviert wird.

Beim Erstellen der Richtlinie und Konfigurieren der Einstellungen bietet das System eine Option zum Anzeigen des Einstellungstyps. Sie können den folgenden Einstellungstyp anzeigen:

- Alle Einstellungen: alle anzeigen, die für alle VDA-Versionen gelten
- Nur aktuelle Einstellungen: zeigt Einstellungen an, die für die aktuelle VDA-Version spezifisch sind
- Nur Legacy-Einstellungen: nur Einstellungen für veraltete VDA-Versionen anzeigen

Einstellungen beim Konfigurieren der Einstellungen anzeigen:

1. Melden Sie sich bei Web Studio an und wählen Sie im linken Bereich **Richtlinien**.
2. Klicken Sie auf der Registerkarte **Richtlinien** auf **Richtlinie erstellen**.
3. Klicken Sie in der Tabelle **Einstellungen auswählen** auf das Dropdownmenü neben **Einstellungen**.
4. Wählen Sie eine der folgenden Optionen aus der Dropdownliste:

- Alle Einstellungen: alle Einstellungen für alle VDA-Versionen anzeigen
- Nur aktuelle Einstellungen: nur Einstellungen für aktuelle VDA-Versionen anzeigen
- Nur Legacy-Einstellungen: nur Einstellungen für veraltete VDA-Versionen anzeigen

1. In der Tabelle **Einstellungen** sind die Einstellungen aufgeführt, die gemäß dem vorherigen Schritt verfügbar sind.

### 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. Sowohl diese Einstellung als auch die Einstellung **Clientnetzlaufwerke** müssen der Richtlinie hinzugefügt werden, damit Benutzer auf Netzlaufwerke zugreifen können. 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 es darf nur der Standardwert der Einstellung beim Anwenden der Richtlinie verwendet

werden. Diese Auswahl ist unabhängig von dem Wert, der vor dem Aktivieren von "Standardwert verwenden"eingegeben wurde.

Wenn die sichere Standardeinstellung aktiviert ist, wird die Priorität der Richtlinieneinstellungen während der VDA-Installation wie folgt beeinflusst:

- Die benutzerdefinierte Einstellung hat die höchste Priorität
- Die sichere Standardeinstellung hat die zweite Priorität
- Die Standardeinstellung hat die niedrigste Priorität

So sehen Sie die sichere Standardeinstellung für eine Richtlinie:

1. Melden Sie sich bei Web Studio an.
2. Klicken Sie im linken Navigationsbereich auf **Richtlinien**.
3. Klicken Sie auf der Registerkarte **Richtlinien** auf **Richtlinie erstellen**.
4. Wenn Sie in der Tabelle **Einstellungen auswählen** den Mauszeiger über die Einstellungen bewegen, für die die Option **Zugelassen?** als aktueller Wert gilt, wird **Sicherer Standardwert: Nicht zugelassen** angezeigt.

   Sichere Standardeinstellung

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, weisen Sie sie Benutzern und Maschinenobjekten zu. Die Richtlinie wird 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 Sie keine Zuweisungen angeben oder Zuweisungen angeben, diese aber deaktivieren, wird die Richtlinie auf **alle** Verbindungen angewendet.

> **Hinweis:**
>
> Richtlinienzuweisungen werden auch als Richtlinienfilter bezeichnet. Weitere Informationen finden Sie in den folgenden Artikeln:
>
> - Create, modify, or delete a filter for a policy
> - How do filters get applied?

In der folgenden Tabelle werden verfügbare Zuweisungen aufgelistet:

| Name | Anwendung der Richtlinie basierend auf |
|---|---|
| Zugriffssteuerung | Zugriffssteuerungsbedingungen, unter denen Clients eine Verbindung herstellen<br>*Verbindungstyp*: ob die Richtlinie auf Verbindungen anzuwenden ist, die mit oder ohne NetScaler Gateway hergestellt wurden.<br>*NetScaler Gateway-Farmname*: Name des virtuellen NetScaler Gateway-Servers.<br>*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 |

| Name | Anwendung der Richtlinie basierend auf |
| --- | --- |
| 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. Anwendungstags sind nicht enthalten. |
| 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 Web 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 Citrix Richtlinien mit dem Editor für lokale Gruppenrichtlinien verwalten, gelten Einstellungen, die Sie der Richtlinie "Ungefiltert"hinzufügen, für alle Sites und Verbindungen. Die Sites und Verbindungen müssen zu dem Geltungsbereich der Gruppenrichtlinienobjekte gehören, die 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. Diese Konfiguration basiert darauf, dass 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. Der Modus ist auf Zulassen eingestellt.
  - Zuweisung B bestimmt das Konto des Verkaufsleiters. Der Modus ist auf Verweigern eingestellt.

  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. Der Modus ist auf Zulassen eingestellt.
  - Zuweisung D ist eine Client-IP-Adressenzuweisung, die 10.8.169.* festlegt (das Unternehmensnetzwerk). Der Modus ist auf Zulassen eingestellt.

  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. Der Modus ist auf Zulassen eingestellt.
  - Zuweisung F ist eine Zugriffssteuerungszuweisung, die NetScaler Gateway-Verbindungsbedingungen angibt. Der Modus ist auf Zulassen eingestellt.

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 Web Studio

1. Melden Sie sich bei Web Studio an und wählen Sie im linken Bereich **Richtlinien**.
2. Wählen Sie die Registerkarte **Vorlagen** und wählen Sie dann eine Vorlage.
3. Wählen Sie in der Aktionsleiste **Richtlinie aus Vorlage erstellen**.
4. Standardmäßig verwendet die neue Richtlinie alle Standardeinstellungen der Vorlage. In diesem Fall ist **Standardeinstellungen der Vorlage (empfohlen)** ausgewählt. Um die Einstellungen zu ändern, wählen Sie **Standardeinstellungen bearbeiten und erweitern**, 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:
   - **Ausgewählte Benutzer- und Maschinenobjekte**. Hiermit wird die Richtlinie ausgewählten Benutzer- und Maschinenobjekten zugewiesen. Klicken Sie dann auf **Zuweisen**, um die Benutzer- und Maschinenobjekte auszuwählen, auf die die Richtlinie angewendet wird.
   - **Alle Objekte in der Site**. Hiermit wird die Richtlinie auf alle Benutzer- und Maschinenobjekte in der Site angewendet.
6. Geben Sie einen Namen für die Richtlinie ein. 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 deaktiviert. Sie können sie aktivieren. 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.

### Richtlinie mit Web Studio erstellen

1. Melden Sie sich bei Web Studio an und wählen Sie im linken Bereich **Richtlinien**.
2. Wählen Sie die Registerkarte **Richtlinien**.
3. Wählen Sie in der Aktionsleiste **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 dann die Benutzer- und Maschinenobjekte auswählen, auf die die Richtlinie angewendet werden soll.
   - 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**. |
| 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**. |

| Aufgabe | Anweisung |
| --- | --- |
| 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**. |

## Richtliniensätze

June 27, 2024

Richtliniensätze sind Objekte in Citrix Virtual Apps and Desktops, die Richtlinien aggregieren, um einen vereinfachten, rollenbasierten Zugriff und eine einfache Verwaltung zu ermöglichen. Sie können Richtliniensätze anhand der logischen Unterteilungen Ihres Administratorteams und Unternehmens erstellen. Sie können beispielsweise einen Richtliniensatz für jede geografische Region, Geschäftseinheit oder für einen bestimmten Anwendungsfall erstellen. Nach der Erstellung werden Richtliniensätzen Bereiche und Bereitstellungsgruppen zugewiesen, sodass nur autorisierte Administratoren Richtlinien für ihre jeweiligen Benutzer und Maschinen verwalten können.

> **Hinweis:**
>
> Bevor Sie die Richtliniensätze aktivieren, empfiehlt Citrix, Folgendes zu beachten:
>
> - Zusätzliche Richtlinienvalidierungen wurden hinzugefügt. Daher kann ein direktes Upgrade zum Verlust von Richtliniendaten führen, wenn ungültige Richtlinieneinstellungen vorhanden sind.
> - Verwenden Sie das GPO-Scanner-Tool und nehmen Sie vor dem Upgrade die erforderlichen Änderungen vor, um die ungültigen Daten zu erkennen. Weitere Informationen finden Sie unter CTX676686.

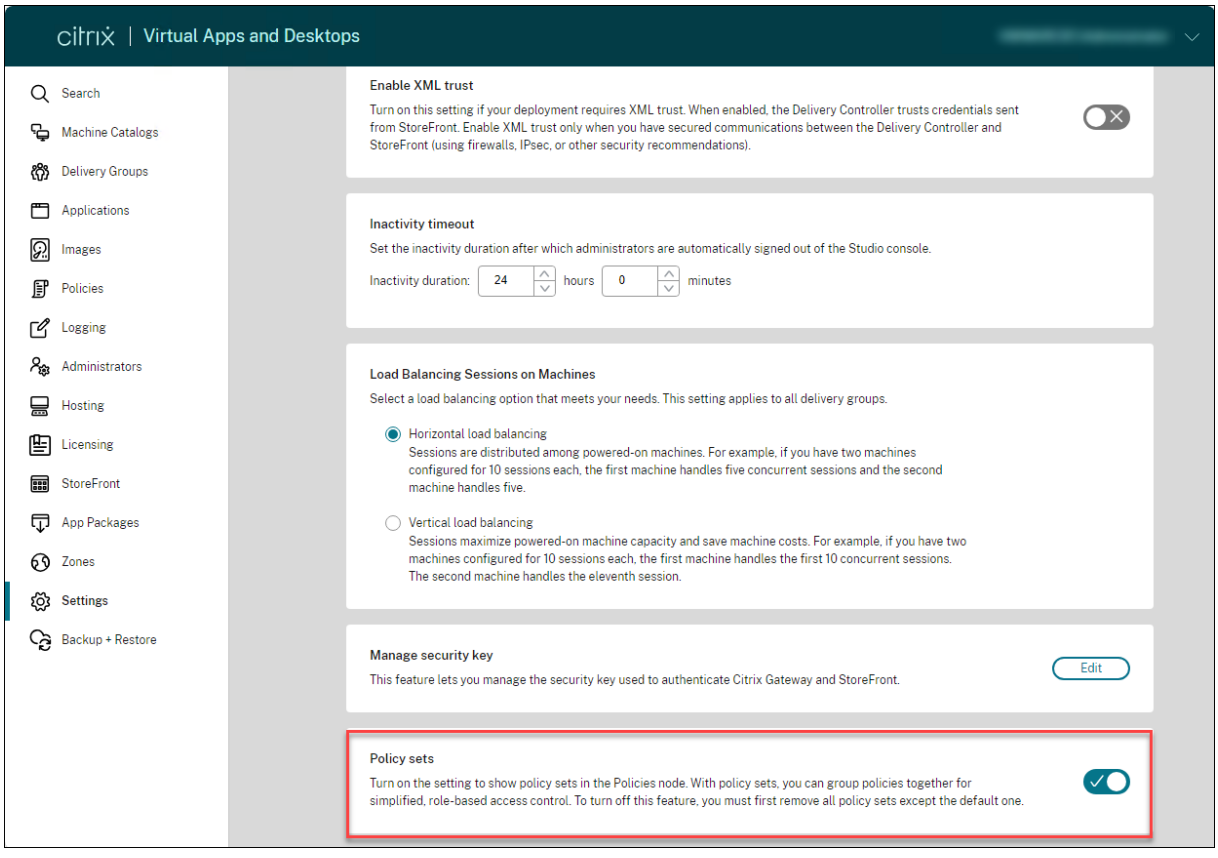
> - Für alle zukünftigen Upgrades empfiehlt Citrix, das neueste SDK zu verwenden. Wenn Sie ein älteres SDK für die Aktualisierung von Richtlinien verwenden, können Sie den Richtlinieneinstellungen möglicherweise ungültige Daten hinzufügen, wodurch das Risiko besteht, dass Richtliniendaten verloren gehen.

### Vorteile

- Rollenbasierte Zugriffssteuerung für verteilte Administratorenteams
- Vereinfachte Fusionen, Übernahmen und Konsolidierungen
- Kleinerer Fehlerbereich
- Mehrmandanten-Unterstützung für Richtlinien

### Richtliniensätze aktivieren

Gehen Sie auf der Registerkarte **Verwalten** in Citrix Virtual Apps and Desktops zu **Einstellungen** und aktivieren Sie die Einstellung **Richtliniensätze**.




> **Hinweis:**
>
> Sie müssen Richtliniensätze aktivieren, bevor Sie einen Richtliniensatz erstellen.

### Featurevergleich

| Vor der Anwendung von Richtliniensätzen | Nach der Anwendung von Richtliniensätzen |
|---|---|
| Richtlinien, Einstellungen, Filter und Richtlinienprioritäten für die gesamte Site werden an einer Stelle in Citrix Studio konfiguriert. | Richtlinien, Einstellungen, Filter und Richtlinienprioritäten werden für jeden Richtliniensatz separat konfiguriert. |
| Wenn Sie eine Richtlinie verwalten, müssen Sie jede Richtlinie verwalten. | Volladministratoren können die Verwaltung eines bestimmten Richtliniensatzes individuell an untergeordnete Administratoren delegieren. |
| Richtlinien in großen und dezentralen Umgebungen werden komplex und schwer zu verwalten. | Richtlinien in großen und dezentralen Umgebungen können einfach aufgeteilt und verwaltet werden. |

### Wie funktionieren Richtliniensätze?

#### Allgemeiner Überblick

- Richtliniensätze werden Bereitstellungsgruppen zugewiesen.
- Richtliniensätze haben einen oder mehrere Bereiche.
- Bereitstellungsgruppen, denen kein Richtliniensatz zugewiesen ist, erhalten den Standardrichtliniensatz.
- Einer Bereitstellungsgruppe kann nur ein Richtliniensatz zugewiesen werden.
- Mehrere Bereitstellungsgruppen können denselben Richtliniensatz verwenden.
- Richtliniensätze sind zwar Bereitstellungsgruppen zugewiesen sind, die Richtlinien behalten jedoch ihre Filter bei

Weitere Informationen finden Sie unter Wie werden Filter angewendet? Die Art und Weise, wie Richtlinienzuweisungen oder Richtlinienfilter funktionieren, hat sich für Richtliniensätze nicht geändert. Das heißt, sie funktionieren genauso wie bei Richtlinien.

#### Standardrichtliniensatz

- Wenn die Einstellung “Richtliniensatz”aktiviert wird, werden alle vorhandenen Richtlinien im Standardrichtliniensatz zusammengefasst.
- Jede Bereitstellungsgruppe erhält den Standardrichtliniensatz, es sei denn, die Administratoren erstellen einen Richtliniensatz und weisen ihn einer Bereitstellungsgruppe zu.
- Sobald einer Bereitstellungsgruppe ein bestimmter Richtliniensatz zugewiesen ist, erhält sie keine Richtlinien mehr aus dem Standardrichtliniensatz.

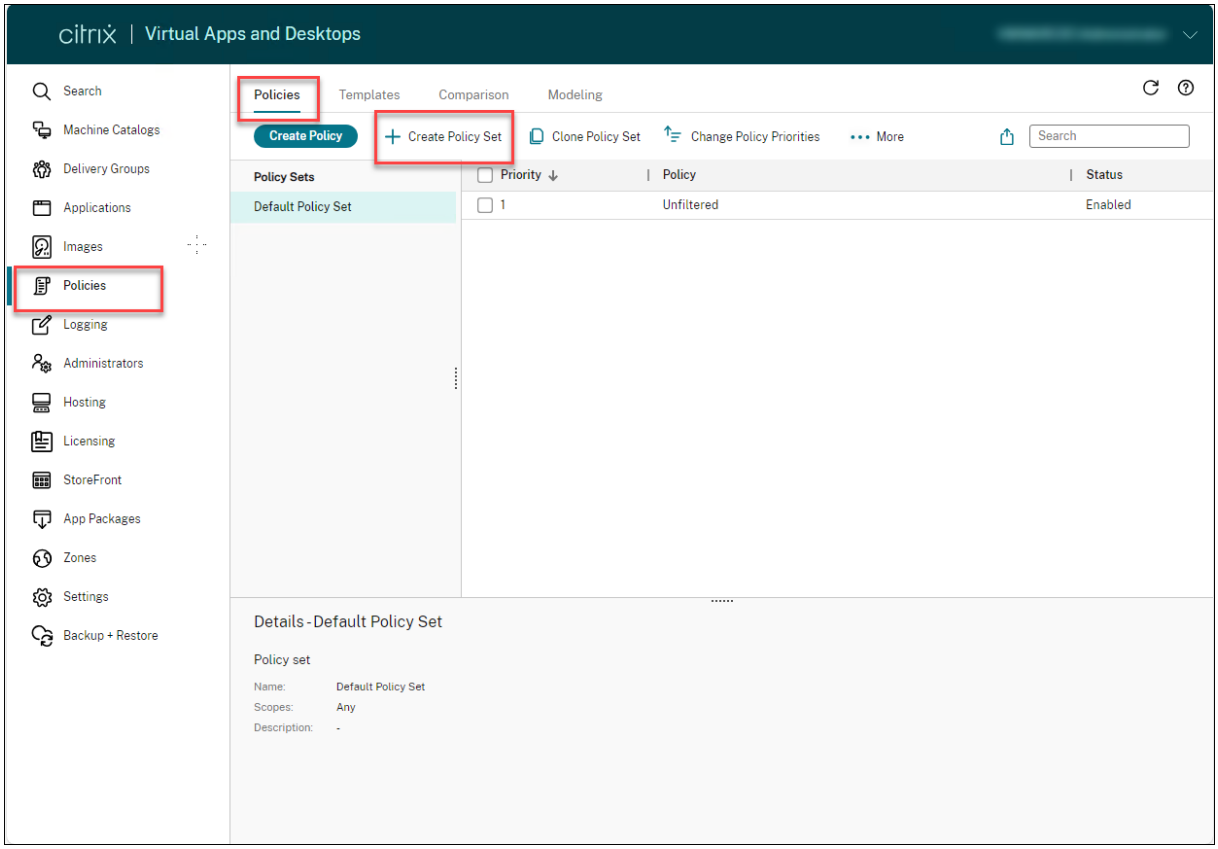
### Richtliniensatzerstellung

Richtliniensätze können auf zweierlei Art erstellt werden:

- Richtliniensatz erstellen: Diese Aktion erstellt einen leeren Richtliniensatz.
- Richtliniensatz klonen: Diese Aktion erstellt einen Richtliniensatz, der auf einem vorhandenen Richtliniensatz basiert.

### Richtliniensätze erstellen

1. Melden Sie sich bei Web Studio an und wählen Sie im linken Bereich **Richtlinien**.




1. Wählen Sie **Richtliniensatz erstellen**. Die Registerkarte **Einführung** wird angezeigt.
2. Klicken Sie auf **Weiter** oder auf die Registerkarte **Name und Beschreibung**.
3. Geben Sie den Namen und die Beschreibung für den Richtliniensatz ein.
4. Klicken Sie auf **Weiter** oder auf die Registerkarte **Zuweisungen**.
5. Wählen Sie eine oder mehrere Bereitstellungsgruppen aus, denen Sie den Richtliniensatz zuweisen möchten.
6. Klicken Sie auf **Weiter** oder auf die Registerkarte **Bereiche**.
7. Wählen Sie die Bereiche des Richtliniensatzes aus.

8. Klicken Sie auf **Erstellen**. Der Richtliniensatz wird mit der ausgewählten Zuweisung und dem ausgewählten Bereich erstellt.

### Richtliniensätze klonen

1. Melden Sie sich bei Web Studio an und wählen Sie im linken Bereich **Richtlinien**.
2. Wählen Sie **Richtliniensatz klonen**.
3. Ändern Sie den Namen des Richtliniensatzes.
4. Ändern oder erstellen Sie Zuweisungen für den Richtliniensatz und klicken Sie auf **Weiter**.
5. Wählen oder deaktivieren Sie die Richtlinien für den geklonten Richtliniensatz.
6. Ändern Sie den Bereich der Richtlinie.
7. Klicken Sie auf **Erstellen**. Der Richtliniensatz wird erstellt.

### Richtliniensätze bearbeiten

1. Melden Sie sich bei Web Studio an und wählen Sie im linken Bereich **Richtlinien**.
2. Wählen Sie **Richtliniensatz bearbeiten**.
3. Ändern Sie den Namen des Richtliniensatzes und klicken Sie auf **Weiter**.
4. Ändern oder erstellen Sie Zuweisungen für den Richtliniensatz und klicken Sie auf **Weiter**.
5. Ändern Sie den Bereich der Richtlinie.
6. Klicken Sie auf **Erstellen**.

### Richtliniensatzzuweisung

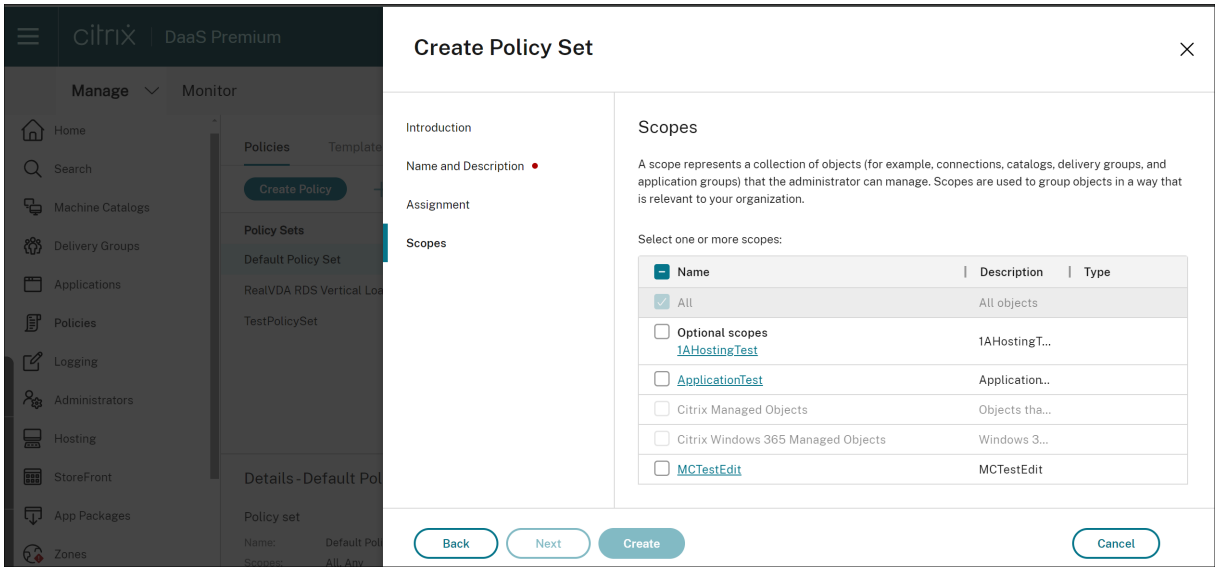
Richtliniensätze werden Bereitstellungsgruppen zugewiesen. Sie können Zuweisungen konfigurieren, wenn der Richtliniensatz erstellt oder bearbeitet wird. Sie können Zuweisungen auch beim Erstellen oder Bearbeiten von Bereitstellungsgruppen konfigurieren.

### Richtliniensatzbereiche

Administratoren können den Bereich eines Richtliniensatzes so definieren, dass nur autorisierte Administratoren ihn anzeigen oder bearbeiten können. Sie können Bereiche konfigurieren, wenn der Richtliniensatz erstellt oder bearbeitet wird.

Mit der Einführung von Richtliniensätzen können Sie Citrix Richtlinien auch mithilfe der API erstellen und verwalten. Weitere Informationen finden Sie unter So erstellen Sie einen Richtliniensatz in Citrix DaaS.




# Vergleichen, Priorisieren und Problembehandlung für Richtlinien

June 27, 2024

> **Hinweis:**
>
> Sie können Ihre Citrix Virtual Apps and Desktops-Bereitstellung mithilfe von zwei Verwaltungskonsolen verwalten: Web Studio (webbasiert) und Citrix Studio (Windows-basiert). Dieser Artikel behandelt nur Web Studio. Informationen zu Citrix Studio finden Sie im entsprechenden Artikel in Citrix Virtual Apps and Desktops 7 2212 oder früher.

Sie können mit mehreren Richtlinien Ihre Umgebung an die Anforderungen der Benutzer, basierend auf deren Aufgabengebiet, geografischem Standort oder Verbindungstyp anpassen. Beispielsweise erlegen Sie aus Sicherheitsgründen Benutzergruppen, die regelmäßig mit sensiblen Daten interagieren, Beschränkungen auf.

Sie können auch 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 Folgendes festlegen:

- Wie Sie die Richtlinienpriorität festlegen
- Wie Sie Ausnahmen erstellen
- Wie Sie die gültige Richtlinie bei einem Richtlinienkonflikt anzeigen.

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 hat immer Vorrang vor allen anderen Einstellungen und Richtlinien. Die höchste Verschlüsselungseinstellung umfasst das Betriebssystem und die Spiegelungseinstellung mit der größten Einschränkung.

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. Diese Einstellung umfasst Einstellungen, die sich auf typische Remotedesktopprotokoll-Clientverbindungseinstellungen (RDP) beziehen. Zu typischen RDP-Einstellungen gehören Desktophintergrund, Menüanimationen und das Anzeigeverhalten bei Drag & Drop.

Manche Richtlinieneinstellungen, wie Secure ICA, müssen mit den Richtlinien und 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 müssen beispielsweise den gleichen Verschlüsselungsgrad verwenden, den Sie an anderer Stelle in der Umgebung verwenden.

> **Hinweis:**
>
> Bei Double-Hop-Szenarien stellen Einzelsitzungs-OS-VDAs im zweiten Hop eine Verbindung zu einem Multisitzungs-OS-VDA her. In diesem Fall wirken die Citrix Richtlinien auf dem Einzelsitzungs-OS-VDA so, als wäre dieser das Benutzergerät. Beispiel: Richtlinien legen fest, dass Bilder auf dem Benutzergerät zwischengespeichert werden. Die Bilder, die für den zweiten Hop in einem Double-Hop-Szenario zwischengespeichert werden, werden dann auf der Maschine mit dem Einzelsitzungs-OS-VDA zwischengespeichert.

## Assistenten für die Richtlinienmodellierung verwenden

Mithilfe der Richtlinienmodellierung können Sie aktivierte Richtlinien mit Filtern für Planungs- und Testzwecke simulieren. Nur aktivierte Richtlinien mit Filtern werden modelliert. Deaktivierte Richtlinien werden niemals angewendet und aktivierte Richtlinien ohne Filter werden immer angewendet.

Führen Sie die folgenden Schritte aus, um den **Modellierungsassistenten** zu öffnen:

1. Wählen Sie in der linken Navigationsleiste **Richtlinien** aus.
2. Wählen Sie die Registerkarte **Modellierung**.
3. Wählen Sie **Richtlinienmodellierung** in der Aktionsleiste aus.
4. Lesen Sie die **Einführung** und klicken Sie auf **Weiter**.

5. Wählen Sie Benutzer oder Computer aus. Sie können nach Containern oder Benutzern oder Computern suchen. Klicken Sie auf **Weiter**.
6. Wählen Sie Ihre Filterbeweise aus. Sie können Ihre Simulation optional detaillierter gestalten, indem Sie zusätzliche Details wie **Bereitstellungsgruppe**, **Tags**, **Client-IP-Adresse** usw. eingeben. Klicken Sie auf **Weiter**.
7. Überprüfen Sie die Zusammenfassung Ihrer Auswahl und klicken Sie auf **Ausführen**.

Wenn Sie auf **Ausführen** klicken, erstellt der Assistent einen Bericht mit den Modellierungsergebnissen. Beim Anzeigen des Berichts haben Sie folgende Möglichkeiten:

- Wählen Sie im Dropdownmenü aus, ob Sie **Alle Einstellungen**, **Computereinstellungen**oder **Benutzereinstellungen** anzeigen möchten.
- Verwenden Sie die Suchleiste, um nach bestimmten Einstellungen zu suchen.
- Klicken Sie auf eine Einstellung, um deren Details anzuzeigen. Wenn beispielsweise nicht alle Benutzereinstellungen für eine Richtlinie angewendet wurden, wird im Bereich **Details** der Grund hierfür angezeigt.
- Klicken Sie auf **Exportieren**, um die Modellierungsergebnisse im JSON-Format, HTML-Format oder beidem zu exportieren.

Nach ausgeführter Richtlinienmodellierung stehen Ihnen weitere Optionen zur Verfügung. Sie haben folgende Möglichkeiten:

- **Modellierungsbericht anzeigen:** Dadurch wird der o. g. Modellierungsbericht geöffnet, sodass Sie ihn erneut ansehen oder exportieren können.
- **Richtlinienmodellierung erneut ausführen**: Hiermit können Sie die Richtlinienmodellierung mit den zuvor ausgewählten Kriterien erneut ausführen und neue Modellierungsergebnisse generieren. Dies ist nützlich, wenn sich Richtlinien geändert haben und Sie sehen möchten, wie sich diese Änderungen auf Ihr aktuelles Modell auswirken.
- **Modellierungsbericht löschen**: Dadurch wird der aktuelle Modellierungsbericht gelöscht.

### 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, sodass optimale Verfahren eingehalten werden. Außerdem ist ggf. ein Vergleich von Einstellungen in einer Richtlinie oder Vorlage mit den Standardeinstellungen von Citrix erforderlich.

1. Melden Sie sich bei Web Studio an und wählen Sie im linken Bereich **Richtlinien**.
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**. Um zur Standardansicht zurückzukehren, wählen Sie **Gemeinsame Einstellungen anzeigen**.

### 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 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 entsprechend ihrer Priorität und Bedingung zusammengefasst. Zum Beispiel, ob die Einstellung deaktiviert oder aktiviert ist. 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 linken Bereich die Option **Richtlinien**. Achten Sie darauf, die Registerkarte **Richtlinien** auszuwählen.
2. Wählen Sie auf der Registerkarte **Richtlinien** auf der Aktionsleiste **Richtlinienprioritäten ändern**. Die Seite **Richtlinienprioritäten ändern** wird angezeigt.
3. Ändern Sie in der Prioritätsliste die Priorität für eine Richtlinie auf eine der nachstehend beschrieben Arten:

    - Ziehen Sie die Richtlinie an die gewünschte Position.
    - Um sie um eine Position nach oben oder unten zu verschieben, klicken Sie auf das Pfeilsymbol nach oben oder unten.
    - Um sie an den Anfang oder das Ende der Liste zu verschieben, klicken Sie auf das Pfeilsymbol "Oben"oder "Unten".
    - Um die Prioritätsnummer zu ändern, klicken Sie auf das Symbol **Bearbeiten**, geben Sie eine Nummer ein und klicken Sie dann auf **Speichern**.

4. Klicken Sie auf **Speichern**.

### 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 kann eine Richtlinie folgende Zuweisungen enthalten:

- Zuweisung A ist eine Client-IP-Adressenzuweisung, die den Bereich 208.77.88.* angibt, festlegt. Der Modus ist auf "Zulassen"eingestellt.
- Zuweisung B ist eine Benutzerzuweisung, die ein spezifisches Benutzerkonto angibt. Der Modus ist auf Verweigern eingestellt.

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.

### Ermitteln der auf eine Verbindung angewendeten Richtlinien

Eine Verbindung reagiert möglicherweise 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 den Richtlinienergebnissatz berechnen und so ermitteln, wie die Richtlinieneinstellungen am Ende für eine Verbindung zusammengeführt werden.

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. Sie können Bedingungen für ein Verbindungsszenario angeben. Beispiel:
  - Domänencontroller
  - Benutzer
  - Citrix Richtlinienzuweisungsbeweiswerte
  - Simulierte Umgebungseinstellungen wie etwa eine langsame Netzwerkverbindung
    Der von dem Assistenten erstellte Bericht listet die Citrix Richtlinien auf, die in dem Szenario wirksam werden. Da Sie beim Controller als Domänenbenutzer angemeldet

sind, berechnet der Assistent die Ergebnisse 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. Mit dem Tool "Gruppenrichtlinienergebnisse"können Sie den aktuellen Status von GPOs in Ihrer Umgebung bewerten und einen Bericht generieren. In dem Bericht wird beschrieben, wie diese Objekte, einschließlich Citrix Richtlinien, derzeit auf einen bestimmten Benutzer und Controller angewendet werden.

Sie können den Assistenten für die Citrix Gruppenrichtlinienmodellierung in Web Studio starten. Sie können das Tool "Gruppenrichtlinienergebnisse"auch über die Gruppenrichtlinien-Verwaltungskonsole in Windows starten.

Mit Web Studio erstellte Site-Richtlinieneinstellungen sind in den folgenden Fällen nicht im Richtlinienergebnissatz enthalten:

- Wenn Sie den Assistenten für die Citrix Gruppenrichtlinienmodellierung von der Gruppenrichtlinien-Verwaltungskonsole aus ausführen
- Wenn Sie das Tool "Gruppenrichtlinienergebnisse"in der Gruppenrichtlinien-Verwaltungskonsole ausführen

Um zu prüfen, ob Sie den umfassendsten Richtlinienergebnissatz erhalten, empfiehlt Citrix das Starten des Assistenten für die Citrix Gruppenrichtlinienmodellierung über Web Studio, es sei denn, Sie erstellen Richtlinien nur über die Gruppenrichtlinien-Verwaltungskonsole.

### 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. Diese Situation tritt in folgenden Fällen auf:

- 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

June 27, 2024

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 | Zulässig | Alle VDA-Versionen |
| Zum Schreiben in Clientzwischenablage zugelassene Formate | Keine Formate angegeben | VDA 7.6 bis aktuelle Version |
| 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 |
| Client-zu-Sitzung-Übertragungsgröße für Zwischenablage beschränken | Deaktiviert | VDA 2009 |
| Sitzung-zu-Client-Übertragungsgröße für Zwischenablage beschränken | Deaktiviert | VDA 2009 |
| Verlusttoleranzmodus | Zulässig | VDA 2003. Hinweis: Der Verlusttoleranzmodus ist noch nicht verfügbar. Diese Version des VDA unterstützt das Feature, wenn sie verfügbar wird. |

| Name | Standardeinstellung | VDA |
| --- | --- | --- |
| Schwellenwerte für Verlusttoleranzmodus | Bei verfügbarem Verlusttoleranzmodus: Paketverlust: 5 %, Latenz: 300 ms (RTT) | VDA 2003 bis aktuelle Version |
| Rendezvous-Protokoll | 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 |
| 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 für virtuelle Kanäle | Aktiviert | VDA 2109 bis aktuelle Version |

### ICA/Adobe Flash-Bereitstellung/Flash-Umleitung

| Name | Standardeinstellung | VDA |
| --- | --- | --- |
| Verhinderung von Fallback auf Flash-Video | Nicht konfiguriert | VDA 7.6 FP3 bis aktuelle Version |
| Fehler bei Verhinderung von Fallback auf Flash-Video (*.swf) | | VDA 7.6 FP3 bis aktuelle Version |

### ICA/Audio

| Name | Standardeinstellung | VDA |
|---|---|---|
| Adaptives Audio | Aktiviert | Gilt sowohl für Einzelsitzungs-OS- als auch Multisitzungs-OS-Sitzungen von VDAs mit Citrix Virtual Apps and Desktops 2109 oder höher. |
| Audio über UDP - Echtzeitübertragung (Audio over UDP Real-time Transport) | Zulässig | Alle VDA-Versionen |
| Audio Plug & Play | Zulässig | VDA für Multisitzungs-OS 7 bis aktuelle Version |
| Audioqualität | Hoch - High Definition-Audio | Alle VDA-Versionen |
| Clientaudioumleitung | Zulässig | Alle VDA-Versionen |
| Clientmikrofonumleitung | Zulässig | Alle VDA-Versionen |
| Verlusttoleranzmodus für Audio | Nicht zugelassen | VDA-Versionen 2402 und höher |

### ICA/automatische Wiederverbindung von Clients

| Name | Standardeinstellung | VDA |
|---|---|---|
| Automatische Wiederverbindung von Clients | Zulässig | Alle VDA-Versionen |
| Authentifizierung bei automatischer Wiederverbindung von Clients | Keine Authentifizierung erforderlich | Alle VDA-Versionen |
| Protokollierung der automatischen Wiederverbindung von Clients | Kein Protokollieren von Wiederverbindungsereignissen | Alle VDA-Versionen |
| Timeout für autom. Wiederverbindung 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 |
| 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 |

| Name | Standardeinstellung | VDA |
| --- | --- | --- |
| 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 |
| 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 |

| Name | Standardeinstellung | VDA |
|---|---|---|
| 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 konfigurieren | Deaktiviert | VDA 2311 bis aktuelle Version |

### ICA/Browserinhaltsumleitung

| Name | Standardeinstellung | VDA |
|---|---|---|
| Browserinhaltsumleitung | Zulässig | VDA 7.16 bis aktuelle Version |
| ACL-Konfiguration für die Browserinhaltsumleitung | `https://www.youtube.com/*` | VDA 7.16 bis aktuelle Version |
| Unterstützung der integrierten Windows-Authentifizierung für die Browserinhaltsumleitung | Nicht zugelassen | VDA 2106 bis aktuelle Version |
| Proxykonfiguration für die Browserinhaltsumleitung | Leer | VDA 7.16 bis aktuelle Version |
| Webproxyauthentifizierung für die Browserinhaltsumleitung mit serverseitigem Abruf | Nicht zugelassen | VDA 2012 bis aktuelle Version |

### ICA/Clientsensoren

| Name | Standardeinstellung | VDA |
|---|---|---|
| Anwendungen können physischen Clientgerätstandort 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 | Medium | VDA 5.6, VDA für Einzelsitzungs-OS 7 bis 7.15 |
| Desktophintergrund | Zulässig | Alle VDA-Versionen |
| Menüanimation | Zulässig | Alle VDA-Versionen |
| Fensterinhalt beim Verschieben anzeigen | Zulässig | 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 | Zulässig | VDA für Multisitzungs-OS 7 bis aktuelle Version |

### ICA/Dateiumleitung

| Name | Standardeinstellung | VDA |
|---|---|---|
| Clientlaufwerke automatisch verbinden | Zulässig | Alle VDA-Versionen |
| Clientlaufwerkumleitung | Zulässig | Alle VDA-Versionen |
| Lokale Clientfestplattenlaufwerke | Zulässig | Alle VDA-Versionen |
| Clientdiskettenlaufwerke | Zulässig | Alle VDA-Versionen |
| Clientnetzlaufwerke | Zulässig | Alle VDA-Versionen |
| Optische Clientlaufwerke | Zulässig | Alle VDA-Versionen |
| Clientwechseldatenträger | Zulässig | 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 | Zulässig | 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 | 65.536 KBit | VDA 5, 5.5, 5.6 FP1, VDA für Single-Session OS 7 bis aktuelle Version |

| Name | Standardeinstellung | VDA |
| --- | --- | --- |
| 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 |
| Grafikstatusanzeige | Deaktiviert | VDA 7.16 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 |
| Bildschirmfreigabe | Deaktiviert | VDA 2112 |
| Videocodec zur Komprimierung verwenden | Videocodec verwenden, wenn bevorzugt | VDA 7.6 FP3 bis aktuelle Version |
| Hardwarecodierung für Videocodec verwenden | Aktiviert | VDA 7.11 bis aktuelle Version |

### ICA/Grafik/Zwischenspeicherung

| Name | Standardeinstellung | VDA |
| --- | --- | --- |
| Schwellenwert für persistenten Cache | 3.000.000 Bit/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/Tastatur und IME

| Name | Standardeinstellung | VDA |
| --- | --- | --- |
| Client-Tastaturlayoutsynchronisierung und Verbesserung des IME | Deaktiviert | Gilt nur für 1912 LTSR CU2 und höher. |
| Unicode-Tastaturlayoutzuordnung aktivieren | Nicht zugelassen | Gilt nur für 1912 LTSR CU2 und höher. |
| Meldungsfeld für Tastaturlayoutwechsel ausblenden | Nicht zugelassen | Gilt nur für 1912 LTSR CU2 und höher. |

### 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 |
| 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 |
| Touchoptimierten Desktop starten | Zulässig | 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 |
| Videoqualität beschränken | Nicht konfiguriert | VDA für Multisitzungs-OS 7 bis aktuelle Version, VDA für Einzelsitzungs-OS 7 bis aktuelle Version |
| Microsoft Teams-Umleitung | Zulässig | VDA für Multisitzungs-OS 1906 bis aktuelle Version, VDA für Einzelsitzungs-OS 1906 bis aktuelle Version |
| Multimediakonferenzen | Zulässig | Alle VDA-Versionen |
| Optimierung von Windows Media-Multimediaumleitung über WAN | Zulässig | 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 Inhaltsabruf von Windows Media | Zulässig | VDA für Multisitzungs-OS 7 bis aktuelle Version, VDA für Einzelsitzungs-OS 7 bis aktuelle Version |
| Windows Media-Umleitung | Zulässig | 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 | Zulässig | VDA für Multisitzungs-OS 7 bis aktuelle Version |
| 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 2003 |

### 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 | Zulässig | 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 | Nur im Profil speichern, wenn sie nicht auf dem Client gespeichert sind | Alle VDA-Versionen |
| Gespeicherte und wiederhergestellte Clientdrucker | Zulässig | 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 | Beste 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 | Einfach | 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 |
| Remote-PC-Zugriff –Timer für getrennte Sitzung | Deaktiviert | VDA für Einzelsitzungs-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 | Zulässig | 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 |
| --- | --- | --- |
| Client-TWAIN-Geräteumleitung | Zulässig | VDA 5.5, 5.6 FP1, VDA für Multisitzungs-OS 7 bis aktuelle Version, VDA für Einzelsitzungs-OS 7 bis aktuelle Version |
| TWAIN-Komprimierungsgrad | Medium | 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 | Zulässig | 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 | Medium | 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 | None | 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 | 2.147.483.647 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 |

> **Hinweis:**
>
> Die Richtlinie **Mindestframeratesollwert** ist veraltet.

### ICA/Visuelle Anzeige/Festbilder

| Name | Standardeinstellung | VDA |
|---|---|---|
| Zusätzliche Farbkomprimierung | Deaktiviert | Alle VDA-Versionen |
| Schwellenwert für zusätzliche Farbkomprimierung | 8.192 KBit/s | Alle VDA-Versionen |
| Heavyweight-Komprimierung | Deaktiviert | Alle VDA-Versionen |
| Grad der verlustreichen Komprimierung | Medium | Alle VDA-Versionen |
| Schwellenwert für verlustreiche Komprimierung | 2.147.483.647 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 |
| CPU-Auslastung ausschließlich Prozesspriorität | Unter normal oder gering | 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 |

| Name | Standardeinstellung | VDA |
| --- | --- | --- |
| Ausgeschlossene Gruppen | Deaktiviert. Mitglieder aller Benutzergruppen werden verarbeitet. | Alle VDA-Versionen |
| Unterstützung von Offlineprofilen | Deaktiviert | Alle VDA-Versionen |
| Pfad zu Benutzerspeicher | Windows | Alle VDA-Versionen |
| Anmeldungen lokaler Administratoren verarbeiten | Deaktiviert | Alle VDA-Versionen |
| Verarbeitete Gruppen | Deaktiviert. Mitglieder aller Benutzergruppen werden verarbeitet. | Alle VDA-Versionen |

### Profilverwaltung/Plattformübergreifende Einstellungen

| Name | Standardeinstellung | VDA |
| --- | --- | --- |
| Benutzergruppen für plattformübergreifende Einstellungen | Deaktiviert. Alle in Verarbeitete Gruppen angegebenen Benutzergruppen werden verarbeitet | Alle VDA-Versionen |
| Plattformübergreifende Einstellungen aktivieren | Deaktiviert | Alle VDA-Versionen |
| Pfad zu plattformübergreifenden Definitionen | Deaktiviert. Kein Pfad angegeben. | Alle VDA-Versionen |
| Pfad zum Speicher für plattformübergreifende Einstellungen | Deaktiviert. Windows\PM_CM wird verwendet. | Alle VDA-Versionen |
| Quelle für Erstellung plattformübergreifender Einstellungen | Deaktiviert | Alle VDA-Versionen |

### Profilverwaltung/Dateisystem/Ausschlüsse

| Name | Standardeinstellung | VDA |
| --- | --- | --- |
| Ausschlussliste - Verzeichnisse | Deaktiviert. Alle Ordner im Benutzerprofil werden synchronisiert. | Alle VDA-Versionen |
| Ausschlussliste - Dateien | Deaktiviert. Alle Dateien im Benutzerprofil werden synchronisiert. | Alle VDA-Versionen |

### Profilverwaltung/Dateisystem/Synchronisierung

| Name | Standardeinstellung | VDA |
| --- | --- | --- |
| Zu synchronisierende Verzeichnisse | Deaktiviert. Nur nicht ausgeschlossene Ordner werden synchronisiert. | Alle VDA-Versionen |
| Zu synchronisierende Dateien | Deaktiviert. Nur nicht ausgeschlossene Dateien werden synchronisiert. | Alle VDA-Versionen |
| Zu spiegelnde Ordner | Deaktiviert. Es werden keine Ordner gespiegelt. | Alle VDA-Versionen |

### Profilverwaltung/Ordnerumleitung

| Name | Standardeinstellung | VDA |
| --- | --- | --- |
| Administratorzugriff gewähren | Deaktiviert | Alle VDA-Versionen |
| Domänennamen einschließen | Deaktiviert | Alle VDA-Versionen |

### Profilverwaltung/Ordnerumleitung/AppData(Roaming)

| Name | Standardeinstellung | VDA |
| --- | --- | --- |
| AppData(Roaming)-Pfad | Deaktiviert. Kein Speicherort angegeben. | Alle VDA-Versionen |

| 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 |
| Anmeldung | 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 verbindliches 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 | 10 GB. Ein Benutzerlayer ist ein Datenträger mit schlanker Speicherzuweisung, der auf die festgelegte Größe erweitert wird. Benutzerlayer werden nie verkleinert. | 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 | None | VDA 7.6 bis aktuelle Version |

## Referenz für Richtlinieneinstellungen

June 27, 2024

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 |

| Beschränken der Bandbreite | Richtlinieneinstellung |
|---|---|
| Drucken | Bandbreitenlimit für Druckerumleitung oder Bandbreitenlimit für Druckerumleitung (Prozent) |
| TWAIN-Geräte (wie Kameras oder Scanner) | Bandbreitenlimit für TWAIN-Geräteumleitung oder Bandbreitenlimit für TWAIN-Geräteumleitung (Prozent) |
| USB-Geräte | Bandbreitenlimit für Client-USB-Geräteumleitung oder Bandbreitenlimit für Client-USB-Geräteumleitung (Prozent) |

### Umleitung von Clientlaufwerken und Benutzergeräten

| Aufgabe | Richtlinieneinstellung |
|---|---|
| Steuern, ob Laufwerke des Benutzergeräts verbunden werden, wenn Benutzer sich am Server anmelden | Clientlaufwerke automatisch verbinden |
| Steuern der Datenübertragung mit Kopier- und Einfügeoperationen zwischen dem Server und der lokalen Zwischenablage | Clientzwischenablagenumleitung |
| Steuern der Laufwerkzuordnung des Benutzergeräts | Clientlaufwerkumleitung |
| Steuern, ob die lokalen Festplatten des Benutzers in einer Sitzung verfügbar sind | Lokale Clientfestplattenlaufwerke und Clientlaufwerkumleitung |
| Steuern, ob die lokalen Diskettenlaufwerke des Benutzers in einer Sitzung verfügbar sind | Clientdiskettenlaufwerke und Clientlaufwerkumleitung |
| Steuern, ob die Netzlaufwerke des Benutzers in einer Sitzung verfügbar sind | Clientnetzlaufwerke und Clientlaufwerkumleitung |
| 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 |

| Aufgabe | Richtlinieneinstellung |
| --- | --- |
| 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 |
| 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 |
| 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 |

| Aufgabe | Richtlinieneinstellung |
| --- | --- |
| Steuern, ob Benutzer auf Drucker zugreifen können, die an die Benutzergeräte angeschlossen sind | Clientdruckerumleitung |
| Steuern, ob bei der automatischen Erstellung von Client- und Netzwerkdruckern native Windows-Treiber installiert werden | Automatische Installation von mitgelieferten Druckertreibern |
| Steuern, wann der universelle Druckertreiber verwendet wird | Verwendung universeller Druckertreiber |
| Wählen des Druckers anhand von Sitzungsinformationen eines mobilen Benutzers | Standarddrucker |
| Lastausgleich und Failover-Schwellenwert für universellen Druckserver festlegen | Universelle Druckserver für den Lastausgleich; Außer-Betrieb-Schwellenwert für universelle Druckserver |

> **Hinweis:**
>
> Richtlinien können nicht zum Aktivieren eines Bildschirmschoners in einer Desktop- oder Anwendungssitzung verwendet werden. Wenn Benutzer einen Bildschirmschoner benötigen, muss dieser auf dem Benutzergerät eingerichtet werden.

## ICA-Richtlinieneinstellungen

June 27, 2024

> **Hinweis:**
>
> Diese Seite enthält Beschreibungen und unterstützte Konfigurationswerte für ICA-Richtlinieneinstellungen. Weitere Informationen zur Arbeit mit Richtlinien finden Sie unter Arbeiten mit Richtlinien.

### Adaptiver Transport

Diese Einstellung steuert den Datentransport über EDT als primäre Methode und über TCP als Fallback.

Standardmäßig ist der adaptive Transport aktiviert (**Bevorzugt**) und EDT wird, sofern möglich, mit Fallback auf TCP verwendet. Sie können die Einstellung nach Bedarf ändern:

- **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.

### Drag & Drop-Einstellung

Diese Einstellung ermöglicht oder verhindert das Ziehen von Dateien zwischen dem Client und virtuellen Anwendungen oder Desktops. Die Drag & Drop-Richtlinie ist standardmäßig deaktiviert. Sie können diese Richtlinie bei Bedarf aktivieren.

### 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:

- Prüfen Sie, dass **Clientzwischenablagenumleitung** auf **Zugelassen** festgelegt ist.
- Prüfen Sie, 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** auf **Nicht zugelassen** oder **Schreiben in Clientzwischenablage einschränken** auf **Deaktiviert** 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.

#### Client-zu-Sitzung-Übertragungsgröße für Zwischenablage beschränken

Diese Einstellung legt die maximale Datenmenge in der Zwischenablage fest, die ein Benutzer durch einmaliges Kopieren und Einfügen von einem Clientendpunkt in eine virtuelle Sitzung übertragen kann.

Um die Übertragungsgröße der Zwischenablage zu begrenzen, aktivieren Sie die Einstellung **Client-zu-Sitzung-Übertragungsgröße für Zwischenablage beschränken**. Geben Sie dann im Feld **Größenbeschränkung** einen Wert in Kilobyte ein, um die Größe der Datenübertragung zwischen der lokalen Zwischenablage und einer Sitzung zu definieren.

Diese Einstellung ist standardmäßig deaktiviert, d. h. es gibt keine Beschränkung für Client-zu-Sitzung-Übertragungen.

#### HDX Direct

HDX Direct ermöglicht es dem Client, automatisch eine direkte Verbindung zum Sitzungshost herzustellen, wenn eine direkte Kommunikation verfügbar ist. Verbindungen werden mit einer Verschlüsselung auf Netzwerkebene sicher hergestellt.

#### HDX Direct-Modus

HDX Direct kann verwendet werden, um direkte Verbindungen mit Sitzungshosts für interne und externe Clients herzustellen. Diese Einstellung legt fest, ob HDX Direct nur für interne Clients oder sowohl für interne als auch für externe Clients verfügbar ist.

Wenn HDX Direct auf **Nur intern** gesetzt ist, versucht HDX Direct, nur direkte Verbindungen für Clients im internen Netzwerk herzustellen.

Wenn HDX Direct auf **Intern** und **Extern** gesetzt ist, wird die Herstellung direkter Verbindungen für interne und externe Clients versucht.

Standardmäßig ist HDX Direct nur für interne Clients eingerichtet.

#### HDX Direct-Portbereich

Der Portbereich, der von HDX Direct für Verbindungen von externen Benutzern verwendet wird. Standardmäßig verwendet HDX Direct den Portbereich: 55000—55250.

#### Sitzung-zu-Client-Übertragungsgröße für Zwischenablage beschränken

Diese Einstellung legt die maximale Datenmenge in der Zwischenablage fest, die ein Benutzer durch einmaliges Kopieren und Einfügen von einer virtuellen Sitzung zu einem Clientendpunkt übertragen kann.

Um die Übertragungsgröße der Zwischenablage zu begrenzen, aktivieren Sie die Einstellung **Sitzung-zu-Client-Übertragungsgröße für Zwischenablage beschränken**. Geben Sie dann im Feld **Größenbeschränkung** einen Wert in Kilobyte ein, um die Größe der Datenübertragung zwischen einer Sitzung und der lokalen Zwischenablage zu definieren.

Diese Einstellung ist standardmäßig deaktiviert, d. h. es gibt keine Beschränkung für Sitzung-zu-Client-Übertragungen.

#### Schreiben in Clientzwischenablage einschränken

Wenn diese Einstellung auf **Aktiviert** festgelegt ist, können Hostzwischenablagedaten nicht für den Clientendpunkt freigegeben werden. Durch Aktivieren der Einstellung **Zum Schreiben in Clientzwischenablage zugelassene Formate** können Sie bestimmte Formate zulassen.

Diese Einstellung ist standardmäßig auf **Deaktiviert** festgelegt.

#### Schreiben in Sitzungszwischenablage einschränken

Wenn diese Einstellung auf **Aktiviert** festgelegt ist, können Clientzwischenablagedaten nicht für die Benutzersitzung freigegeben werden. Durch Aktivieren der Einstellung **Zum Schreiben in Sitzungszwischenablage zugelassene Formate** können Sie bestimmte Formate zulassen.

Diese Einstellung ist standardmäßig auf **Deaktiviert** festgelegt.

#### Zum Schreiben in Sitzungszwischenablage zugelassene Formate

Wenn die Einstellung **Schreiben in Sitzungszwischenablage einschränken** auf **Aktiviert** festgelegt ist, können Hostzwischenablagedaten 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:

- Prüfen Sie, dass **Clientzwischenablagenumleitung** auf **Zugelassen** festgelegt ist.
- Prüfen Sie, 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 **Clientzwischenablageumleitung** auf **Nicht zugelassen** oder **Schreiben in Sitzungszwischenablage einschränken** auf **Deaktiviert** 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.

### 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.

### FIDO2-Umleitung

Mit dieser Einstellung aktivieren oder deaktivieren Sie die FIDO2-Umleitung. Mit der FIDO2-Umleitung können Benutzer die Vorteile der lokalen FIDO2-Endpunktkomponenten in einer virtuellen Maschine zu nutzen. Auf Geräten mit TPM 2.0 und Windows Hello können Benutzer sich mit FIDO2-Sicherheitsschlüsseln oder integrierter Biometrie bei ihrer virtuellen Sitzung authentifizieren.

Wenn die Einstellung auf **Zugelassen** festgelegt ist, können die Benutzer die FIDO2-Authentifizierung unter Nutzung der lokalen Endpunktfunktionen durchführen. Standardmäßig ist diese Einstellung auf **Zugelassen** festgelegt.

### 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 120.000 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)

Diese Einstellung aktiviert oder deaktiviert Folgendes:

- Dynamische Tastaturlayoutsynchronisierung
- Eingabemethoden-Editor (IME)
- Unicode-Tastaturlayoutzuordnung
- Ein- oder Ausblenden der Benachrichtigung beim Tastaturlayoutwechsel

1. Wählen Sie in Web 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. Wenn Sie die Anzeige der Nachricht unterdrücken, müssen die Benutzer einen Moment mit der Eingabe warten, um eine falsche Zeicheneingabe zu vermeiden.

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 Trennen von Clientsitzungen abgewartet wird.

Durch diese Einstellung wird auch die Zeitdauer der Benutzerabmeldung vom Server erhöht.

### Verlusttoleranzmodus

> **Wichtig:**
>
> - Das Feature erfordert mindestens Citrix Workspace App 2002 für Windows. Diese Version des VDA unterstützt das Feature, wenn sie verfügbar wird.
> - Der Verlusttoleranzmodus für Grafiken wird von Citrix Gateway und Citrix Gateway Service nicht unterstützt. Der Modus ist nur mit direkten Verbindungen verfügbar.

Diese Einstellung aktiviert oder deaktiviert den Verlusttoleranzmodus für Grafiken.

Der Verlusttoleranzmodus für Grafiken ist standardmäßig **Zulässig**.

Wenn der Modus zulässig ist, wird er aktiviert, sobald Paketverlust und Latenz einen bestimmten Schwellenwert überschreiten. Sie können die Schwellenwerte mit der Richtlinie Verlusttoleranzmodus - Schwellenwerte festlegen.

### Schwellenwerte für Verlusttoleranzmodus

Ist der Verlusttoleranzmodus verfügbar, definiert diese Einstellung die Schwellenwerte für Netzwerkmetriken, bei deren Überschreiten die Sitzung in den Verlusttoleranzmodus für Grafiken wechselt.

Standardschwellenwerte:

- Paketverlust: 5 %
- Latenz: 300 ms (RTT)

Weitere Informationen finden Sie unter Verlusttoleranzmodus.

### Verlusttoleranzmodus für Audio

Diese Einstellung aktiviert oder deaktiviert den Verlusttoleranzmodus für Audio.

Wenn diese Option aktiviert ist, wird Audio über den Verlusttoleranzmodus gesendet.

Standardmäßig ist der Verlusttoleranzmodus für Audio **verweigert**.

Um die Richtlinie zu aktivieren, ändern Sie die Registrierung der Richtlinie für den Verlusttoleranzmodus für Audio auf **zulässig**.

EDT-Transport ist erforderlich, um den Verlusttoleranzmodus für Audio zu aktivieren.

### Rendezvous-Protokoll

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:**
>
> Ein Feature Toggle in Citrix Cloud und eine HDX-Richtlinieneinstellung steuern dieses Feature. 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. Diese Einstellung hat keine Auswirkungen auf Sitzungen, die direkt zwischen Client und VDA oder über ein On-Premises Citrix Gateway eingerichtet wurden.

Weitere Informationen finden Sie unter Rendezvous-Protokoll.

### Rendezvousproxykonfiguration

Mit dieser Einstellung können Sie einen expliziten Proxy für die Verwendung mit dem Rendezvous-Protokoll konfigurieren. Wenn Sie einen transparenten Proxy verwenden, muss die Einstellung nicht aktiviert werden.

Diese Einstellung ist standardmäßig deaktiviert.

Wenn die Einstellung deaktiviert ist, leitet der VDA ausgehenden Datenverkehr nicht über nicht transparente Proxys weiter, wenn versucht wird, eine Rendezvousverbindung mit dem Gateway Service herzustellen.

Wenn die Einstellung aktiviert ist, versucht der VDA, über den in der Einstellung definierten Proxy eine Rendezvousverbindung mit dem Gateway Service herzustellen.

Der VDA unterstützt HTTP- und SOCKS5-Proxys für Rendezvousverbindungen. Damit der VDA einen Proxy für die Rendezvousverbindung verwendet, müssen Sie diese Einstellung aktivieren. Geben Sie außerdem entweder die Adresse des Proxys oder den Pfad zur PAC-Datei an. Beispiel:

- Proxyadresse: `http://<URL or IP>:<port>` oder `socks5://<URL or IP>:<port>`
- PAC-Datei: `http://<URL or IP>/<path>/<filename>.pac`

  Die VDA-Version 2103 ist die unterstützte Mindestversion für die Proxykonfiguration mit einer PAC-Datei. Weitere Informationen zum PAC-Dateischema für SOCKS5-Proxys finden Sie unter Proxykonfiguration.

> **Hinweis:**
>
> Nur SOCKS5-Proxys unterstützen den Datentransport über EDT. Verwenden Sie für einen HTTP-Proxy TCP als Transportprotokoll für ICA.

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.

## Automatische Wiederverbindung von Clients - Richtlinieneinstellungen

June 27, 2024

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. Beispielsweise kann das Cookie aufgrund einer Verzögerung bei der Wiederverbindung ablaufen oder wenn Anmeldeinformationen erneut 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. Dieser Timer gibt die verbleibende Zeit bis zur Wiederverbindung der Sitzung an. Die Citrix Workspace-App versucht, die Verbindung mit der Sitzung wiederherzustellen, bis die Wiederverbindung erfolgreich war oder der Benutzer die Wiederverbindung abbricht.

Bei Benutzersitzungen versucht die Citrix Workspace-App bei zugelassener automatischer Wiederverbindung 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. Sie können sie deaktivieren, indem Sie die Richtlinie auf **Nicht zugelassen** setzen.

### Authentifizierung bei automatischer Wiederverbindung von Clients

Mit dieser Einstellung legen Sie fest, ob eine Authentifizierung erforderlich ist, 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.

### 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.

### Timeout für autom. Wiederverbindung von Clients

Standardmäßig ist das Timeout der automatischen Wiederverbindung auf 120 Sekunden festgelegt. Der zulässige Höchstwert beträgt 300 Sekunden. Verwenden Sie diese Richtlinie, um einen Wert für das Timeout festzulegen.

### UI-Transparenzstufe während Wiederverbindung

Mit dieser Einstellung können Sie die Transparenzstufe festlegen, die während der Wiederverbindung mit Sitzungszuverlässigkeit auf das XenApp- oder XenDesktop-Sitzungsfenster angewendet wird.

Standardmäßig ist die Transparenz der Benutzeroberfläche beim Wiederverbinden auf 80 % festgelegt.

## Audio - Richtlinieneinstellungen

June 27, 2024

Der Abschnitt **Audio** enthält Richtlinieneinstellungen, mit denen Sie das Senden und Empfangen von Audiodaten auf dem Benutzergerät konfigurieren können, ohne dass es zu Leistungseinbußen kommt.

### Adaptives Audio

Diese Einstellung aktiviert oder deaktiviert adaptives Audio. Wenn Sie diese Richtlinie aktivieren, werden die Einstellungen für die Audioqualität dynamisch angepasst, um die beste Benutzererfahrung zu bieten. Diese Einstellung gilt sowohl für Einzelsitzungs-OS- als auch Multisitzungs-OS-Sitzungen von VDAs mit Citrix Virtual Apps and Desktops 2109 oder höher.

Wenn diese Einstellung nicht zugelassen ist, wird die Richtlinie für die Audioqualität angewendet. Weitere Informationen finden Sie unter Audioqualität.

Standardmäßig ist die Richtlinie für adaptives Audio aktiviert.

### Audio über UDP - Echtzeitübertragung (Audio over 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. Sie ermöglicht aber eine akzeptable Leistung bei Verbindungen mit geringer Bandbreite.
- Wählen Sie Mittel –für Sprache optimiert, um VoIP-Anwendungen bereitzustellen. Diese Einstellung ermöglicht Medienanwendungen bei schwierigen Netzwerkverbindungen mit weniger als 512 KBit/s oder bei erheblicher Überlastung und Paketverlust. 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. Auch bei Überlastung und Paketverlust im Netzwerk.

- 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.

## Bandbreite - Richtlinieneinstellungen

June 27, 2024

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 Einstellungen der **Multistreamrichtlinie** kann zu unerwarteten Ergebnissen führen. Wenn Sie Multistreameinstellungen in einer Richtlinie verwenden, dürfen diese Richtlinieneinstellungen für das Bandbreitenlimit nicht eingeschlossen sein.

### Bandbreitenlimit für die Audioumleitung

Mit dieser Einstellung geben Sie die maximal zulässige Bandbreite für die Wiedergabe oder die Aufnahme von Audio in einer Benutzersitzung an. Die maximal zulässige Bandbreite wird in Kilobit pro Sekunde angegeben.

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 an. Die maximal zulässige Bandbreite wird in Kilobit pro Sekunde angegeben.

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 für Datenübertragungen zwischen einer Sitzung und der lokalen Zwischenablage an. Die maximal zulässige Bandbreite wird in Kilobit pro Sekunde angegeben.

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 Benutzersitzung an. Die maximal zulässige Bandbreite wird in Kilobit pro Sekunde angegeben.

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 an. Die maximal zulässige Bandbreite wird in Kilobit pro Sekunde angegeben.

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 an, die für Druckaufträge über den LPT-Port in einer Benutzersitzung verwendet werden kann. Die maximal zulässige Bandbreite wird in Kilobit pro Sekunde angegeben.

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 Registrierung).

Mit dieser Einstellung geben Sie die maximal zulässige Bandbreite, die für Druckaufträge über den LPT-Port in einer Sitzung verwendet werden darf, als Prozent der Gesamtsitzungsbandbreite an.

Standardmäßig ist kein Maximalwert (Null) angegeben.

Wenn Sie für diese Einstellung und 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 20 MBit/s (20.000 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 an. Die maximal zulässige Bandbreite wird in Kilobit pro Sekunde angegeben.

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 für die Steuerung von TWAIN-Bildverarbeitungsgeräten in veröffentlichten Anwendungen an. Die maximal zulässige Bandbreite wird in Kilobit pro Sekunde angegeben.

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.

## Bidirektionale Inhaltsumleitung - Richtlinieneinstellungen

June 27, 2024

Im Abschnitt **Bidirektionale Inhaltsumleitung** werden Richtlinieneinstellungen zum Aktivieren oder Deaktivieren der Client-zu-VDA- und der VDA-zu-Client-URL-Umleitung behandelt.

Serverrichtlinien werden in Web Studio festgelegt. Ab Version 2311 der Citrix Workspace-App ersetzt diese Einstellung die folgenden drei veralteten Einstellungen in Web Studio:

- Bidirektionale Inhaltsumleitung zulassen
- Für Umleitung an VDA zulässige URLs
- Für Umleitung an Client zulässige URLs

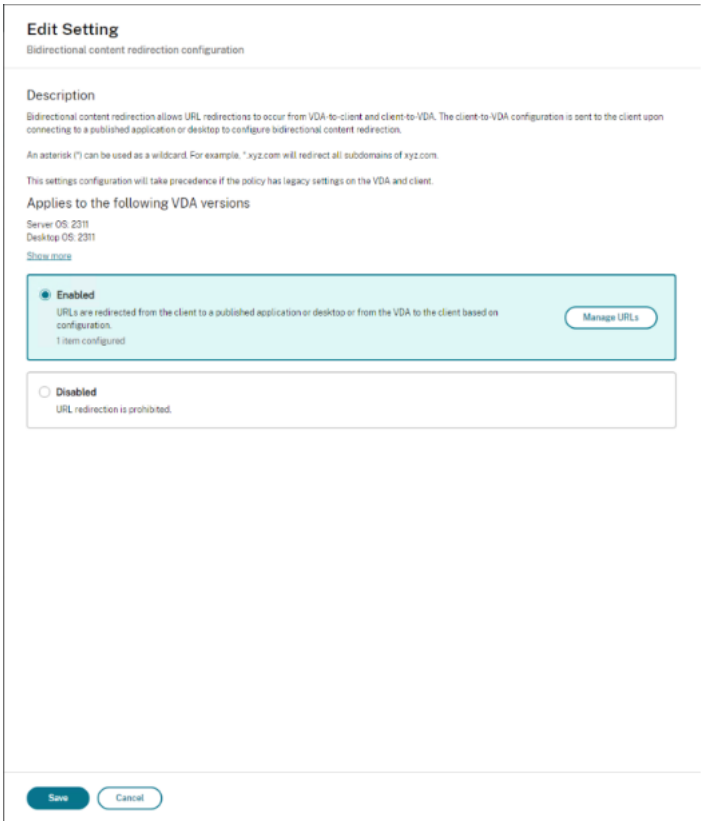
Es ersetzt auch die folgenden drei lokalen Group Policy Object-(GPO)-Einstellungen auf Windows-Clients:

- Bidirektionale Inhaltsumleitung

- Außerkraftsetzungen der bidirektionalen Inhaltsumleitung
- OAuth-Umleitung

Wenn diese Einstellung aktiviert ist, werden die Client-zu-VDA-Einstellungen an den Client gesendet, sobald eine Verbindung zu einer veröffentlichten App oder einem Desktop hergestellt wird, um die bidirektionale Inhaltsumleitung zu konfigurieren.




Wenn diese Einstellung konfiguriert ist, hat sie Vorrang vor den Legacy-Einstellungen in Web Studio und auf dem Client. Citrix empfiehlt, nur die neuen Richtlinieneinstellungen zu verwenden und alle älteren Einstellungen zu löschen, um unerwartetes Verhalten zu vermeiden.

Clientrichtlinien dürfen nicht festgelegt werden, wenn auf dem VDA und dem DDC die Version 2311 oder höher ausgeführt wird. Clientrichtlinien werden ansonsten in der administrativen Gruppenrichtlinienobjektvorlage der Citrix Workspace-App festgelegt.

Citrix bietet Host-zu-Client-Umleitung und lokalen App-Zugriff für die Client-zu-URL-Umleitung. Von Citrix wird jedoch empfohlen, dass Sie die bidirektionale Inhaltsumleitung für domänenverbundene Windows-Clients verwenden.

Citrix empfiehlt, die neue Benutzeroberfläche in Web Studio zur Konfiguration des Features anstelle von Desktop Studio zu verwenden.

### Platzhalterumleitung

Die bidirektionale Inhaltsumleitung unterstützt die Verwendung von Platzhaltern bei der Definition der umzuleitenden URLs. Weitere Informationen über Details und zum Konfigurieren der bidirektionalen Inhaltsumleitung finden Sie in den Anweisungen zur Konfiguration.
Legen Sie in Web Studio die Platzhalter-URL fest, indem Sie die JSON-Zeichenfolge als Wert im `url`-Schlüssel im Array `hostToClientUrls` oder im Array `clientToHostUrls` bearbeiten.

> **Hinweis:**
>
> - Geben Sie in `hostToClientUrls` und `clientToHostUrls` dieselbe URL ein, um Endlosschleifen zu vermeiden.
> - Top-Level-Domänen werden nicht unterstützt. Beispiel: https://www.citrix.* oder http://www.citrix.co* wird nicht umgeleitet.

### Bidirektionale Inhaltsumleitung konfigurieren

Stellen Sie diese Richtlinie auf `Enabled` ein, um mit der Konfiguration des Features zu beginnen, und klicken Sie auf **URLs verwalten**. Stellen Sie die folgenden Konfigurationen ein:

- **VDA-zu-Client-Umleitung**
- **Client-zu-VDA-Umleitung**

#### VDA-zu-Client-Umleitung

Um URLs vom VDA zum Client umzuleiten, geben Sie eine URL pro Zeile ein. Platzhalter sind erlaubt. Mit der OAuth-Umleitung können Sie den Browser auf dem Clientendpunkt verwenden, um die Authentifizierung durchzuführen und das Token zurück an den VDA zu senden.

**Vorteile:**

- Sie vermeiden, diese Anmeldeinformationen in der gehosteten Umgebung zu speichern.
- Sie verwenden biometrische Funktionen, die auf dem Endpunkt und nicht auf dem VDA verfügbar sind.

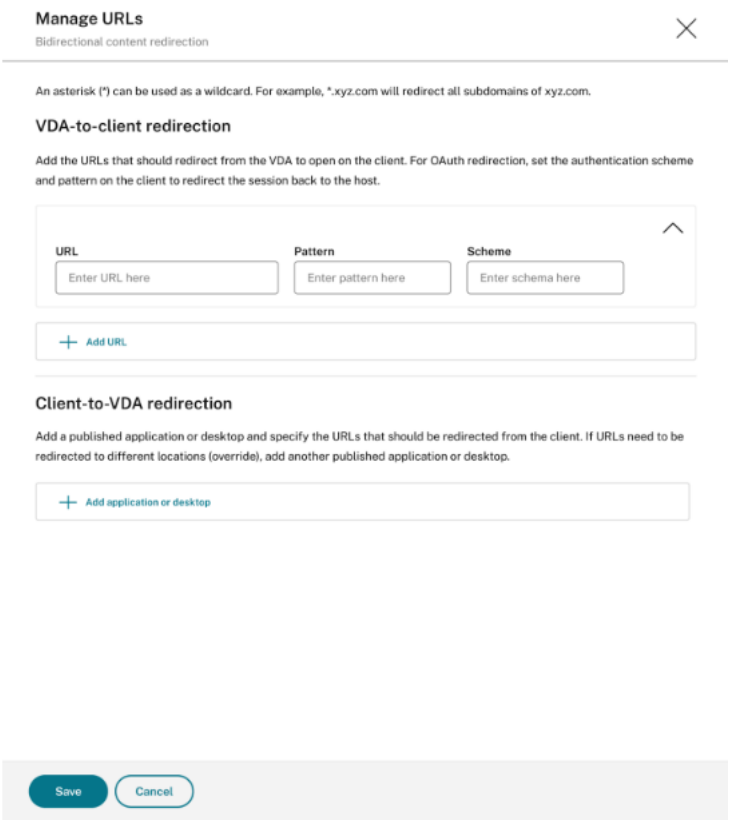
**Konfigurationen:**

Um die VDA-zu-Client-Umleitung für die URL zu konfigurieren, geben Sie Folgendes an:

- **URL** (erforderlich): Fügen Sie die URL hinzu, die vom VDA zum Öffnen auf dem Client umgeleitet werden soll. Legen Sie für die **OAuth-Umleitung** das Authentifizierungsschema und -muster auf dem Client fest, um die Sitzung zurück zum Host umzuleiten.

- **Muster**: (optional) Regulärer URL-Ausdruck, der, wenn er über eine VDA-zu-Client-URL-Umleitung an den Client umgeleitet wird, so verfolgt wird, als ob ein OAuth-Authentifizierungsfluss begonnen hätte. Wenn der Flow abgeschlossen ist (erkannt durch das Öffnen des resultierenden Schemas oder Umleitung-URL-Musters), wird die resultierende URL zurück an den Host-VDA umgeleitet, der diesen Fluss initiiert hat.
- **Schema** (optional): Wenn ein **Schema** angegeben ist, wird erwartet, dass die abschließende URL das Format `<scheme>://<something>` hat. Bedenken Sie, dass Schema nicht angegeben ist (leer). In diesem Fall wird das ursprüngliche resultierende URL-Muster über eine Erfassungsgruppe für reguläre Ausdrücke (muss im Muster angegeben werden) aus dem Muster extrahiert und die ursprüngliche URL wird neu geschrieben, um eine Umleitungs-URL im Format `citrix-oauth-redir://` zu verwenden. Wenn der Datenfluss abgeschlossen ist, wird die ursprüngliche Umleitungs-URL zurück zum Host (VDA) umgeleitet. In diesem Fall muss jeder OAuth-Autorisierungsserver so konfiguriert sein, dass er Umleitungs-URLs im Format `citrix-oauth-redir://byIndex/1 (2, 3, ... N)` zulässt.



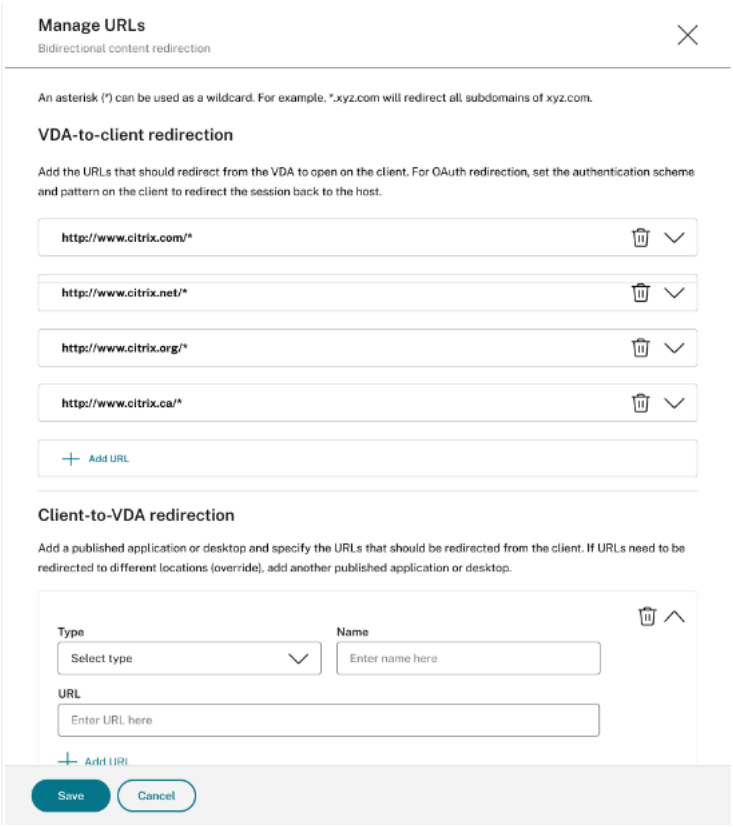

> **Hinweis:**
>
> Obwohl sowohl **Muster** als auch **Schema** optional sind, müssen Sie auch ein **Schema** angeben, wenn **Muster** angegeben ist.

### Client-zu-VDA-Umleitung

Gehen Sie wie folgt vor, um URLs vom Client zum VDA umzuleiten:

1. Konfigurieren Sie das Ziel für Client-URLs.
2. Wählen Sie “Veröffentlichte Anwendung”oder “Veröffentlichter Desktop”aus.
3. Geben Sie den Namen dieser Ressource an.
4. Fügen Sie alle URLs hinzu, die zu dieser Ressource umgeleitet werden müssen.
   Sie können diese Standardressource überschreiben, indem Sie eine neue Anwendung oder einen neuen Desktop hinzufügen und dann die URLs angeben, die zu dieser Ressource umgeleitet werden sollen.




### Desktop Studio

> **Hinweis:**
>
> Citrix empfiehlt, Web Studio zur Konfiguration dieses Features ab Citrix Virtual Apps and Desktops Version 2402 zu verwenden.

Um die bidirektionale Inhaltsumleitung für 2311 zu konfigurieren, erstellen Sie eine JSON-Zeichenfolge mit dem folgenden Format:

```
{

  "version": 1,
  "hostToClientConfig": [
    {

      "hostToClientUrls": [
        {

          "url": "http://www.citrix.com/*"
         }
 ,
        {

          "url": "www.example.com"
         }
 ,
        {

          "url": "https://login.example.org/*",
          "oAuthRedirectionPattern": "https://login.example.org/oauth2
             ?.*",
          "oAuthScheme": "idm.desktop-authentication"
         }

      ]
     }

 ],
  "clientToHostConfig": [
    {

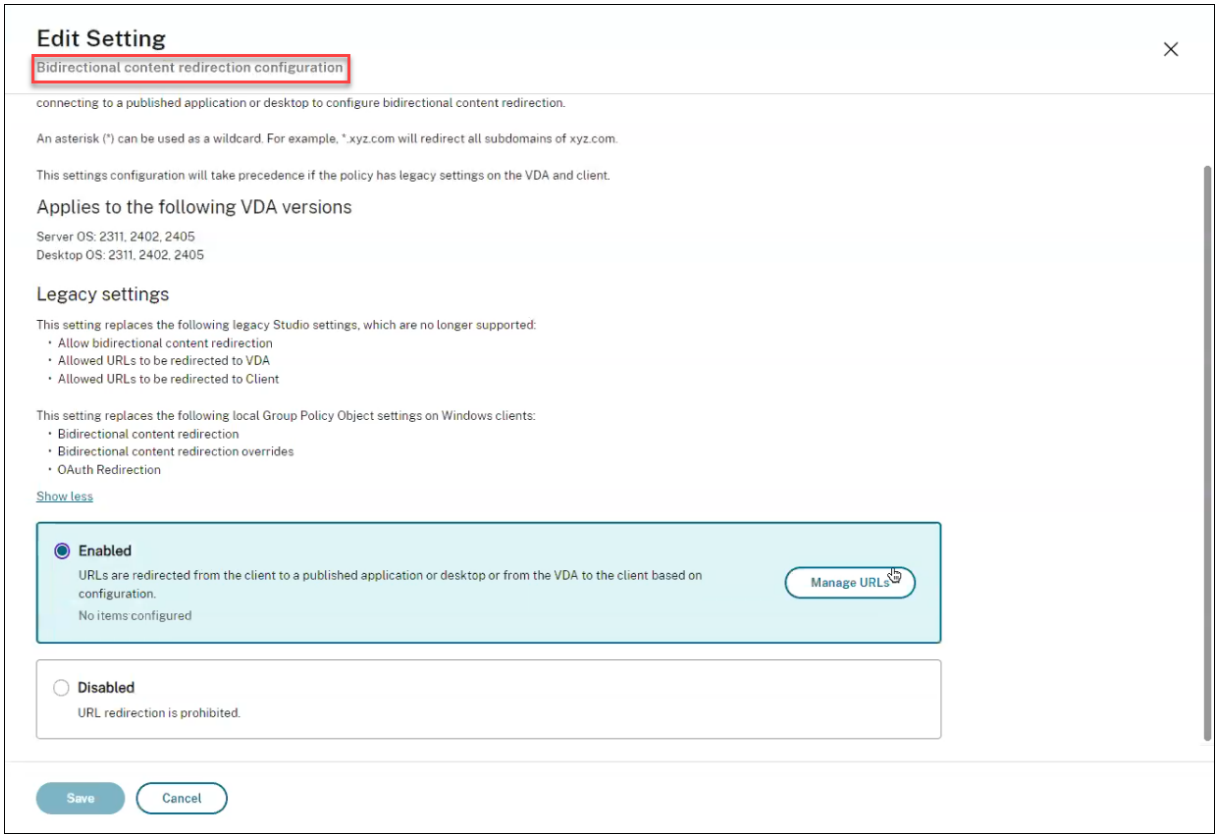
      "publishedAppOrDesktopNameType": "Desktop",
      "publishedAppOrDesktopName": "Win11Desktop",
      "clientToHostUrls": [
        "https://www.example.net",
        "https://*.citrix.example"
      ]
     }
 ,
    {

      "publishedAppOrDesktopNameType": "Application",
      "publishedAppOrDesktopName": "Chrome",
      "clientToHostUrls": [
        "https://tibco.example"
      ]
     }

 ]
}

<!--NeedCopy-->
```

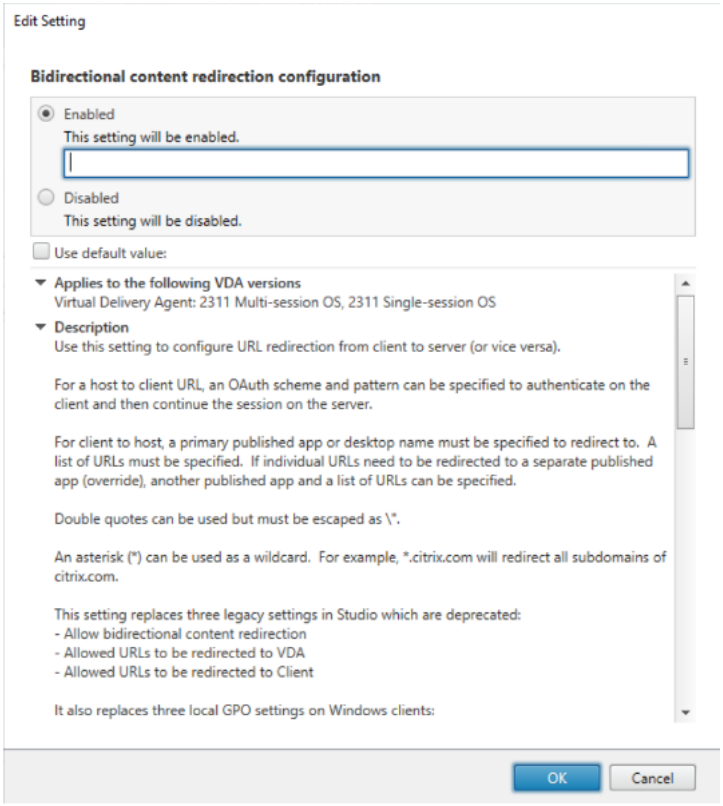
 




Die folgenden Parameter müssen gesetzt werden:

- **version**: (Erforderlich) auf 1 gesetzt.
- Erstellen Sie für die VDA-zu-Client-URL-Umleitung eine einzelne `hostToClientConfig`.
- `hostToClientUrls`: (Erforderlich) Liste der URLs, die vom Host (VDA) zum Client umgeleitet werden sollen. Platzhalter sind erlaubt. Wenn `hostToClientConfig` angegeben ist, aber eine Client-zu-Host-VDA-Umleitung nicht erforderlich ist, muss `clientToHostConfig` mit `publishedAppOrDesktopNameType`, einem leeren `publishedAppOrDesktopName` und einem leeren `clientToHostUrls` angegeben werden.




### OAuth-Umleitung

Mit der OAuth-Umleitung können Sie den Browser auf dem Clientendpunkt verwenden, um die Authentifizierung durchzuführen und das Token zurück an den VDA zu senden.

**Vorteile**:

- Sie vermeiden, diese Anmeldeinformationen in der gehosteten Umgebung zu speichern.
- Sie verwenden biometrische Funktionen, die auf dem Endpunkt und nicht auf dem VDA verfügbar sind.

Um die OAuth-Umleitung für die URL zu konfigurieren, geben Sie die folgenden Parameter an:

- **oAuthRedirectionPattern**: (Optional) Regulärer URL-Ausdruck, der, wenn er über eine VDA-zu-Client-URL-Umleitung an den Client umgeleitet wird, so verfolgt wird, als ob ein OAuth-Authentifizierungsfluss begonnen hätte. Wenn der Flow abgeschlossen ist (erkannt durch das Öffnen des resultierenden Schemas oder Umleitung-URL-Musters), wird die resultierende URL zurück an den Host-VDA umgeleitet, der diesen Fluss initiiert hat.
- **oAuthScheme**: (Optional) Wenn ein Schema angegeben ist, wird erwartet, dass die abschließende URL das Format <scheme>://<something> hat. Bedenken Sie, dass Schema nicht angegeben ist (leer). In diesem Fall wird das ursprüngliche resultierende URL-Muster über eine Erfassungsgruppe für reguläre Ausdrücke (muss im Muster angegeben werden) aus dem

Muster extrahiert und die ursprüngliche URL wird neu geschrieben, um eine Umleitungs-URL im Format `citrix-oauth-redir://` zu verwenden. Wenn der Datenfluss abgeschlossen ist, wird die ursprüngliche Umleitungs-URL zurück zum Host (VDA) umgeleitet. In diesem Fall muss jeder OAuth-Autorisierungsserver so konfiguriert sein, dass er Umleitungs-URLs im Format `citrix-oauth-redir://byIndex/1 (2, 3, ... N)` zulässt.

Für eine Client-zu-VDA-Umleitung erstellen Sie **clientToHostConfig** für jede Ressource, die umgeleitet werden soll.
Geben Sie für jede Ressource die folgenden Parameter an:

- **publishedAppOrDesktopNameType**: (Erforderlich) Entweder ein veröffentlichter Desktop ("Desktop") oder eine veröffentlichte Anwendung ("Anwendung"), die in Studio konfiguriert ist. Wenn die Ressource nicht gültig ist, funktioniert die Umleitung nicht richtig.
- **publishedAppOrDesktopName**: (Erforderlich) Ressourcenname, wie in Web Studio konfiguriert.
- **clientToHostUrls**: (Erforderlich) Liste der URLs, die vom Client zum Host (VDA) umgeleitet werden sollen. Platzhalter sind erlaubt.

### Bekannte Einschränkung

Wenn Sie einen Browser mit PowerShell und einem benutzerdefinierten URL-Schema (nicht HTTP oder HTTPS) starten, werden die benutzerdefinierten URLs nicht an den Client umgeleitet.

## Browserinhaltsumleitung - Richtlinieneinstellungen

June 27, 2024

Der Abschnitt zur Browserinhaltsumleitung 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 Richtlinien für die HTML5-Videoumleitung werden für das Funktionieren der Browserinhaltsumleitung nicht benötigt. Der Citrix HDX HTML5-Videoumleitungsdienst wird jedoch für die Umleitung von Browserinhalten verwendet. Weitere Informationen finden Sie unter Umleitung des Browserinhalts.

> **Hinweis:**
>
> In Web Studio verfügbare Richtlinieneinstellungen 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 Web-Sockets 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.

### Browserinhaltsumleitung

Die Citrix Workspace-App versucht standardmäßig den clientseitigen Abruf und die clientseitige Wiedergabe. Wenn Abruf und Rendering clientseitig fehlschlagen, wird das serverseitige Rendering 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 zur Unterstützung der integrierten Windows-Authentifizierung für die Browserinhaltsumleitung

Die Browserinhaltsumleitung aktiviert das Overlay, das das Aushandlungsschema für die Authentifizierung verwendet. Diese Verbesserung bietet Single Sign-On bei einem Webserver, der mit der integrierten Windows-Authentifizierung (IWA) in derselben Domäne wie der VDA konfiguriert ist.

Wenn diese Option auf **Zugelassen** festgelegt ist, erhält das Overlay-Netz der Browserinhaltsumleitung ein Aushandlungsticket und verwendet hierfür die VDA-Anmeldeinformationen des Benutzers. Der Benutzer authentifiziert sich dann per Single Sign-On beim Webserver.

Wenn diese Option auf **Nicht zugelassen** festgelegt ist, fordert das Overlay-Netzwerk der Browserinhaltsumleitung kein Aushandlungsticket vom VDA an. Der Benutzer authentifiziert sich bei einem

Webserver mit einer Standardauthentifizierung. Bei dieser Authentifizierungsmethode müssen Benutzer bei jedem Zugriff auf den Webserver ihre VDA-Anmeldeinformationen eingeben.

Die Standardeinstellung ist Nicht zugelassen.

### Einstellung für Webproxyauthentifizierung für die Browserinhaltsumleitung mit serverseitigem Abruf

Mit dieser Einstellung wird der von einem Overlay-Netz kommende HTTP-Datenverkehr über einen downstream platzierten Webproxy geleitet. Der downstream platzierte Webproxy 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 dann die Domänenanmeldeinformationen des VDA-Benutzers, um ein Kerberos-Dienstticket zu empfangen. Dieses Dienstticket muss auch in nachfolgenden Anforderungen an den Webproxy enthalten sein.

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.

### ACL-(Access Control List)-Konfigurationsrichtlinieneinstellungen für die Browserinhaltsumleitung

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 auf der Positivliste, deren Inhalt an den Client weitergeleitet wird.

Der Platzhalter * ist zulässig, jedoch nicht im Protokoll- oder Domänenadressteil der URL. Ab Citrix Virtual Apps and Desktops 7 2206 ist der Platzhalter * auch innerhalb des Subdomänenadressteils der URL zulässig.

Zulässig: `http://www.xyz.com/index.html`, `https://www.xyz.com/*`, `http://www.xyz.com/*videos*`, `http://*.xyz.com/`

Nicht zulässig: `http://*.*.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.

> **Hinweis:**
>
> Sie können ACL so konfigurieren, dass BCR Websites zum Endpunkt umleitet, und Authentifizierungsseiten können so konfiguriert werden, dass Identitätsanbieter (IdP) wie Okta und Duo die Authentifizierung für die konfigurierte URL zulassen.

### 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: eine 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. Er verwendet dann Authentifizierungssites 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". Es kann sein, dass URLs für die Einstellung "ACL-Konfiguration für die Browserinhaltsumleitung"und "Sperrlistenkonfiguration für die Browserinhaltsumleitung"festgelegt wurden. In diesem Fall 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 gerendert 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

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.

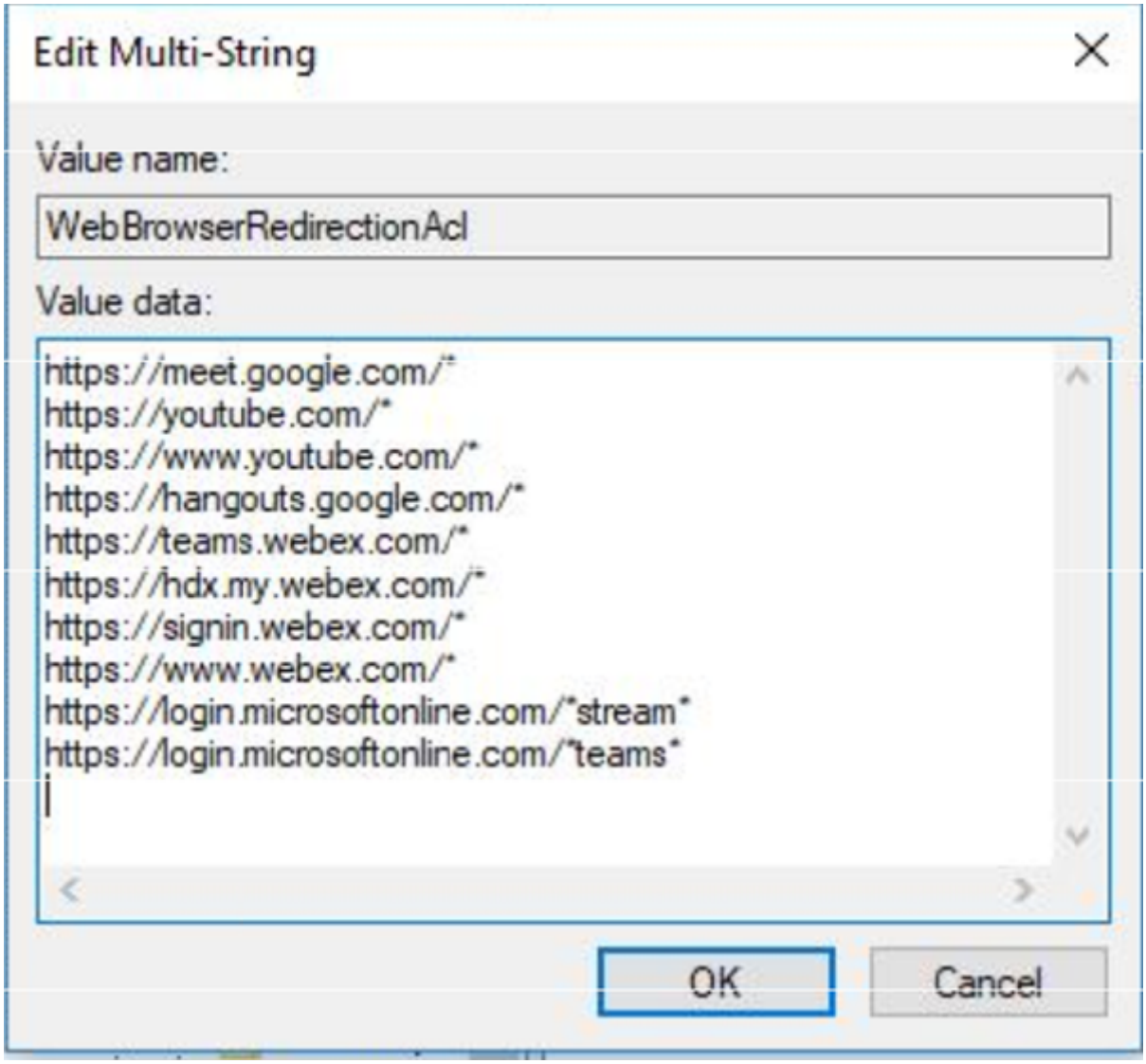
### Außerkraftsetzung von Registrierungsschlüsseln für die Browserinhaltsumleitung

> **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. Erstellen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.
>
> Optionen zur Außerkraftsetzung der Registrierung für Richtlinieneinstellungen:

`\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediastream`

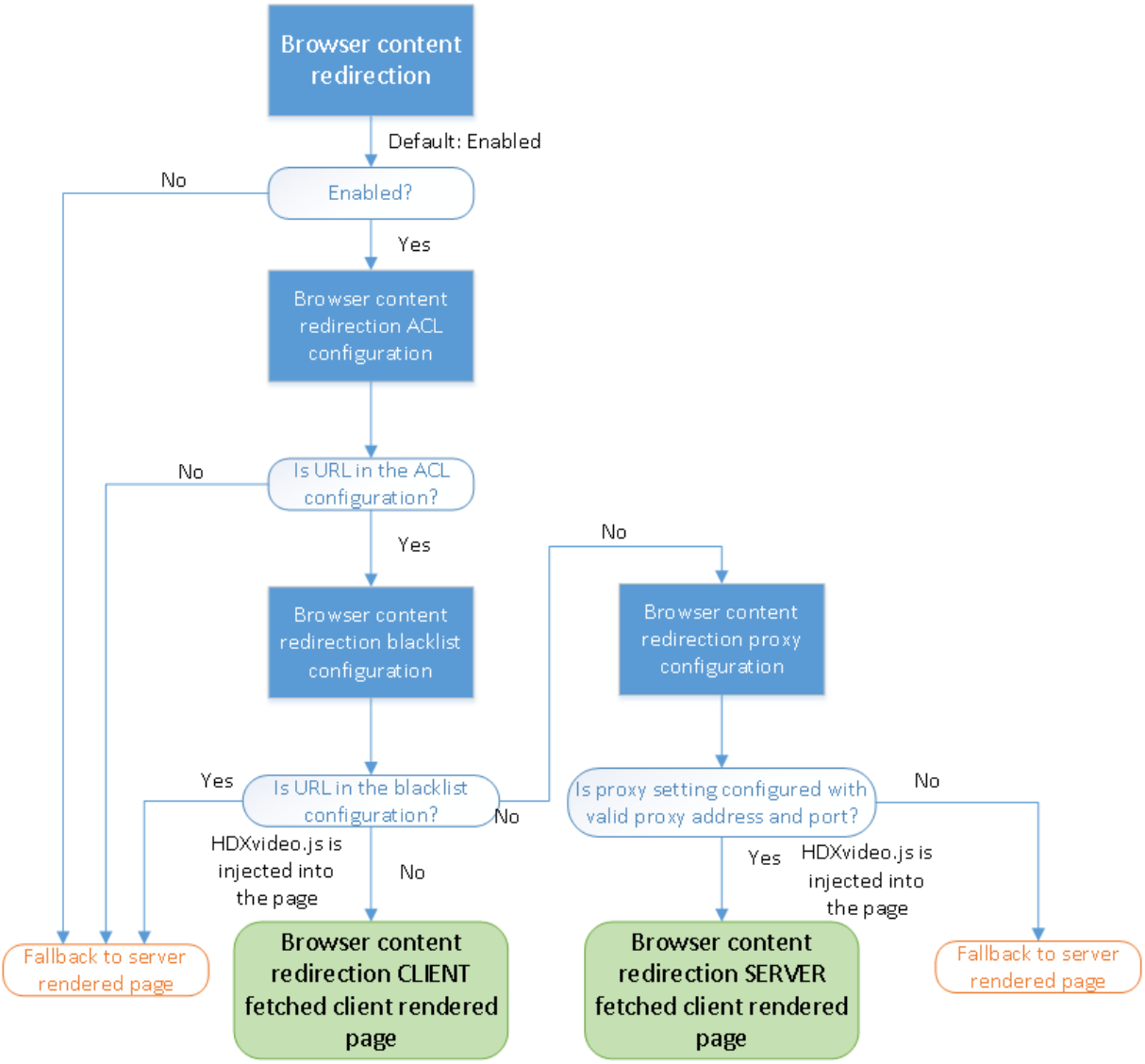
| Name | Typ | Wert |
|---|---|---|
| WebBrowserRedirection | DWORD | 1 = zugelassen, 0 = nicht zugelassen |
| WebBrowserRedirectionAcl | REG_MULTI_SZ | |
| WebBrowserRedirectionAuthenticationSites | REG_MULTI_SZ | |
| WebBrowserRedirectionProxyAddress | REG_SZ | `http://myproxy.citrix.com:8080` oder `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.

## Clientsensoren - Richtlinieneinstellungen

June 27, 2024

Der Abschnitt **Clientsensoren** enthält Richtlinieneinstellungen, mit denen gesteuert wird, wie Informationen über den Mobilgerätsensor in einer Benutzersitzung gehandhabt werden.

### Anwendungen können physischen Clientgerätstandort 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 Option zum Zulassen oder Ablehnen des Features muss bei Ausführung der Anwendung für den Benutzer verfügbar sein.

  - Eine Option zum Löschen von in der Anwendung zwischengespeicherten Standortdaten muss für den Benutzer verfügbar sein. (Die Citrix Workspace-App speichert keine Standortdaten im Cache.)

- Eine standortaktivierte Anwendung muss die Granularität der Standortinformationen verwalten. Dies stellt sicher, dass die erfassten Daten dem Zweck der Anwendung entsprechen. Außerdem werden geltende gesetzliche Vorgaben eingehalten.
- 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.

## Desktopbenutzeroberfläche - Richtlinieneinstellungen

June 27, 2024

Der Abschnitt **Desktopbenutzeroberfläche** enthält Richtlinieneinstellungen für visuelle Effekte, wie Desktophintergrund, Menüanimationen und das Verhalten von Bildinhalten beim Drag & Drop. Mit diesen Richtlinieneinstellungen wird die für Clientverbindungen verbrauchte Bandbreite gesteuert. 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 dient nur der Abwärtskompatibilität bei Verwendung von:
>
> - XenApp 7.15 LTSR
> - XenDesktop 7.15 LTSR
> - früheren VDA-Versionen mit Windows 7 und Windows 2008 R2.

### Desktopgestaltungsumleitung

Mit dieser Einstellung geben Sie an, ob der folgende Grafikprozessor (GPU) für das lokale DirectX-Grafikrendering verwendet werden soll, um eine nahtlosere Windows-Desktopdarstellung zu erzielen:

- Grafikprozessor (GPU) auf dem Benutzergerät
- Oder
- Integrierter Grafikprozessor (IGP) auf dem Benutzergerät

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 wirken sich auf den Desktop aus. Es kann sein, dass Sie auf dem Desktop festgelegt haben, dass vorgenommene Änderungen nach dem Beenden der Sitzung verworfen werden. In diesem Fall steht Benutzern, die Menüanimation aktiviert haben, in späteren Sitzungen keine Menüanimation zur Verfügung. Aktivieren Sie daher für Benutzer, die Menüanimation benötigen, die Microsoft-Einstellung im Hauptimage 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.

## Endbenutzerüberwachung - Richtlinieneinstellungen

June 27, 2024

Der Abschnitt **Endbenutzerüberwachung** enthält Richtlinieneinstellungen 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 der ICA-Roundtripmessung verzögert. Diese Verzögerung dauert so lange, 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 an (in Sekunden), wie oft 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 der ICA-Roundtripmessung verzögert. Diese Verzögerung dauert so lange, 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

## Enhanced Desktop Experience - Richtlinieneinstellungen

June 27, 2024

Durch die Richtlinieneinstellung "Enhanced Desktop Experience"werden Sitzungen auf Serverbetriebssystemen so konfiguriert, dass sie wie lokale Windows 7-Desktops aussehen.

Standardmäßig ist diese Einstellung auf Zugelassen festgelegt.

Wenn ein Benutzerprofil mit dem Design "Windows –klassisch"auf dem virtuellen Desktop vorhanden ist, wird durch diese Richtlinie nicht die verbesserte Desktopdarstellung für diesen Benutzer bereitgestellt. Es kann sein, dass ein Benutzer, dessen Benutzerprofil mit einem Windows 7-Design konfiguriert ist, sich an einem virtuellen Desktop unter Windows Server 2012 anmeldet. Außerdem ist diese Richtlinie nicht konfiguriert oder deaktiviert. In diesem Fall wird der Benutzer in einer Fehlermeldung darauf hingewiesen, dass das Design nicht angewendet werden kann.

In beiden Fällen kann das Problem durch Zurücksetzen des Benutzerprofils gelöst werden.

Wenn Sie die Richtlinie auf einem virtuellen Desktop mit aktiven Benutzersitzungen deaktivieren, ist die Benutzeroberfläche von Sitzungen unter Windows 7 und "Windows - klassisch"inkonsistent. Wenn Sie dies vermeiden möchten, starten Sie den virtuellen Desktop neu, nachdem Sie die Richtlinieneinstellung geändert haben. Löschen Sie dann sämtliche Roamingprofile auf dem virtuellen Desktop. Citrix empfiehlt außerdem, alle anderen Benutzerprofile auf dem virtuellen Desktop zu löschen, um Inkonsistenzen zwischen Profilen zu vermeiden.

Es kann sein, dass Sie in der Umgebung Roamingbenutzerprofile verwenden. Stellen Sie in diesem Fall sicher, dass das Feature "Enhanced Desktop Experience"für alle virtuellen Desktops, die sich ein Profil teilen, 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 Servervetriebssysteme unterscheiden sich. Das Freigeben von Roamingprofilen zwischen beiden Systemtypen kann zu Inkonsistenzen in den Profileigenschaften führen, wenn ein Benutzer zwischen den Systemen wechselt.

## Dateiumleitung - Richtlinieneinstellungen

June 27, 2024

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 diese Einstellung und **Optische Clientlaufwerke**, damit CD-ROM-Laufwerke auf dem Clientgerät automatisch verbunden werden.

Die folgenden Richtlinieneinstellungen hängen zusammen:

- **Clientlaufwerkumleitung**
- **Clientdiskettenlaufwerke**
- **Optische Clientlaufwerke**
- **Lokale Clientfestplattenlaufwerke**
- **Clientnetzlaufwerke**
- **Clientwechseldatenträger**

### 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. Diese Konfiguration ist unabhängig von den einzelnen Dateiumleitungseinstellungen anwendbar. Die einzelnen Dateiumleitungseinstellungen umfassen Clientdiskettenlaufwerke und Clientnetzlaufwerke.

Die folgenden Richtlinieneinstellungen hängen zusammen:

- **Clientdiskettenlaufwerke**
- **Optische Clientlaufwerke**
- **Lokale Clientfestplattenlaufwerke**
- **Clientnetzlaufwerke**
- **Clientwechseldatenträger**

### 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 Clientdiskettenlaufwerke 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 Clientdiskettenlaufwerke 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 Clientnetzlaufwerke nicht zugeordnet werden und Benutzer können auch nicht manuell auf diese Laufwerke zugreifen. Diese Konfiguration ist 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 folgenden Speicherorten auf Dateien zugreifen oder sie speichern können:

- CD-ROM auf dem Benutzergerät
- DVD-ROM auf dem Benutzergerät
- BD-ROM-Laufwerke auf dem Benutzergerät.

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. Diese Konfiguration ist unabhängig von der Einstellung für **optische Clientlaufwerke**.

Konfigurieren Sie außerdem die Einstellung **Clientlaufwerke automatisch verbinden**, damit optische Laufwerke automatisch verbunden werden.

### Clientwechseldatenträger

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. Diese Konfiguration ist unabhängig von der Einstellung für **Clientwechsellaufwerke**.

Konfigurieren Sie außerdem die Einstellung **Clientlaufwerke automatisch verbinden**, damit Wechsellaufwerke 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:

- HTTP
- 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

Mit dieser Einstellung legen Sie fest, ob Benutzer und Anwendungen Folgendes ausführen können:

- Erstellen von Dateien auf zugeordneten Clientlaufwerken
- Ändern von Dateien auf zugeordneten Clientlaufwerken
- Ändern von Ordnern auf zugeordneten Clientlaufwerken

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.

Um die Benutzer festzulegen, für die die Umleitung spezieller Ordner gilt, wählen Sie **Zugelassen** und nehmen diese Einstellung in eine Richtlinie auf, die nach den Benutzern gefiltert wird, denen diese Funktion zur Verfügung stehen soll. Diese Einstellung überschreibt alle anderen Einstellungen für die Umleitung spezieller Ordner.

Daher verhindern Richtlinieneinstellungen, die den Benutzerzugriff auf lokale Festplatten untersagen, auch die Umleitung spezieller Ordner. Diese Situation tritt auf, da die Umleitung spezieller Ordner mit dem Benutzergerät interagieren muss.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, müssen Sie auch für die Einstellung **Lokale Festplattenlaufwerke** die Option "Zugelassen"wählen.

### Dateiübertragungsrichtlinien

In der Standardeinstellung ist die Dateiübertragung aktiviert. Sie ändern diese Richtlinien in Web Studio unter **Benutzereinstellung - ICA-\Dateiumleitung**. Beachten Sie folgende Punkte bei der Verwendung von Dateiübertragungsrichtlinien:

- **Dateiübertragung für die Citrix Workspace-App für Chrome OS/HTML5:** ermöglicht oder verhindert, dass Benutzer Dateien zwischen einer Citrix Virtual Apps and Desktops-Sitzung und ihren Geräten übertragen.
- **Datei für die Citrix Workspace-App für Chrome OS/HTML5 hochladen:** Ermöglicht oder verhindert, dass Benutzer Dateien von ihrem Gerät in eine Citrix Virtual Apps and Desktops-Sitzung hochladen.
- **Datei für die Citrix Workspace-App für Chrome OS/HTML5 herunterladen:** Ermöglicht oder verhindert, dass Benutzer Dateien aus einer Citrix Virtual Apps and Desktops-Sitzung auf ihr Gerät herunterladen.

> **Hinweis:**
>
> Die Dateiübertragungsrichtlinien gelten nur für die Citrix Workspace-App für HTML5 und Chrome OS.

### 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, asynchrone Schreibvorgänge auf Datenträgern nur für Benutzer zu implementieren, die eine Remoteverbindung mit guter Geschwindigkeit für die Dateiübertragungen benötigen. Sie müssen 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.

## Grafiken - Richtlinieneinstellungen

June 27, 2024

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, wie die Einstellungswerte für die Bildqualität verwendet werden.

Diese Einstellung ist standardmäßig deaktiviert.

### Grafikstatusanzeige

Durch diese Einstellung wird das Ausführen der Grafikstatusanzeige in der Benutzersitzung konfiguriert. Mit diesem Tool können Benutzer Informationen über den aktiven Grafikmodus anzeigen. Dazu gehören Angaben zu Videocodec, Hardwarecodierung, Bildqualität und den in der Sitzung verwendeten Monitoren. Mit der Grafikstatusanzeige können Benutzer außerdem den pixelgenauen Modus aktivieren oder deaktivieren.

Citrix Virtual Apps and Desktops ab Release 2103 enthält einen Schieberegler für die Bildqualität, mit dem die Benutzer das geeignete Gleichgewicht zwischen Bildqualität und Interaktivität finden können.

Citrix Virtual Apps and Desktops ab Release 2109 enthält Funktionen zum Konfigurieren eines virtuellen Anzeigelayouts über eine per Grafikstatusanzeige gestartete Benutzeroberfläche.

Die Grafikstatusanzeige ersetzt das Tool für die Qualitätsanzeige früherer Versionen. Diese Richtlinie aktiviert die Qualitätsanzeige für Citrix Virtual Apps and Desktops 7.16 bis 1809.

### Bildschirmfreigabe

Mit dieser Einstellung können Benutzer ihre Sitzungen, einschließlich Bildschirminhalt, Tastaturen und Mäuse, für andere Benutzern freigeben.

Die Einstellung ist standardmäßig deaktiviert.

Der VDA nutzt zum Datenaustausch Ports aus dem TCP-Portbereich. Die Portauswahl beginnt bei der niedrigsten Portnummer, jede weitere Verbindung erfolgt mit der jeweils höheren Portnummer. Über den Port erfolgen eingehende und ausgehende Datenübertragungen.

Standardmäßig ist der TCP-Portbereich auf 52525–52625 festgelegt.

Der für die Bildschirmfreigabe verwendete Port muss der Liste der Firewallausnahmen hinzugefügt werden. Die entsprechende Option wird bei der VDA-Installation als Kontrollkästchen angezeigt. Standardmäßig ist die Option nicht aktiviert.

### Anzeigespeicherlimit

Mit dieser Einstellung geben Sie die maximale Größe des Videopuffers (in Kilobytes) für die Sitzung an.

Das Standardlimit für den Anzeigespeicher ist 65,536 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 65,536 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: Es liegt eine Farbtiefe von 32, eine vertikale Auflösung von 600 und eine horizontale Auflösung von 800 vor. Dies ergibt einen maximal erforderlichen Arbeitsspeicher von (32/8) x (600) x (800) = 1920000 Byte, was einem Anzeigespeicherlimit von 1920 KB entspricht.

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.

Wenn das Speicherlimit für die Sitzung erreicht wird, gibt diese Einstellung an, ob zuerst die Farbtiefe oder die Auflösung herabgesetzt werden soll.

Standardmäßig wird die Farbtiefe zuerst herabgesetzt.

Wenn das Speicherlimit der Sitzung erreicht wird, können Sie die Bildqualität verringern. Wählen Sie hierfür, ob zuerst die Farbtiefe oder die Auflösung herabgesetzt werden soll. 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 bedarfsmäßige Abrufen dieser Abschnitte wird Folgendes erreicht:

- Der Bildlauf auf dem Benutzergerät ist gleichmäßiger.
- Es werden weniger Daten über das Netzwerk auf das Benutzergerät übertragen.
- Es müssen weniger Daten auf dem Benutzergerät verarbeitet werden.

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 Legacy-Grafikmodus wird unterstützt für:

- Windows 7
- Windows Server 2008 R2-VDAs.

Der Legacy-Grafikmodus wird nicht unterstützt für:

- Windows 8.x und 10

- Windows Server 2012, 2012 R2 und 2016.

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. Diese VDAs verwenden einen WDDM-Treiber (Windows Display Driver Model) als primären Anzeigetreiber. 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.

### Videocodec zur Komprimierung verwenden

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. Der Administrator kann diese Richtlinieneinstellung für einzelne Benutzer oder Maschinen konfigurieren, um eine gute Benutzererfahrung zu gewährleisten.

#### 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.

## Caching - Richtlinieneinstellungen

June 27, 2024

Dieser Abschnitt enthält Richtlinieneinstellungen, mit denen Bilddaten auf Benutzergeräten zwischengespeichert werden können, wenn Clientverbindungen eine beschränkte Bandbreite haben.

### Schwellenwert für persistenten Cache

**Hinweis:** Bei Virtual Delivery Agent 7.x gilt diese Richtlinieneinstellung nur, wenn die Richtlinieneinstellung **"Legacygrafikmodus"** aktiviert ist.

Diese Einstellung speichert Bitmaps auf der Festplatte des Benutzergeräts zwischen und ermöglicht die Wiederverwendung großer, häufig verwendeter Bilder.

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

June 27, 2024

> **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 kann jedoch auch mehr Serverressourcen und Bandbreite als andere Grafikmodi verbrauchen.

Standardmäßig ist der Framehawk-Anzeigekanal deaktiviert.

### Portbereich für Framehawk-Anzeigekanal

Mit dieser Richtlinieneinstellung geben Sie den Bereich der UDP-Portnummern an, die vom VDA zum Austausch von Framehawk-Anzeigekanaldaten mit dem Benutzergerät verwendet werden. Die Portnummern werden im Format *niedrigste Portnummer, höchste Portnummer* angegeben. 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.

# Keep-Alive - Richtlinieneinstellungen

June 27, 2024

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-Alive-Meldungen

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.

# Lokaler App-Zugriff - Richtlinieneinstellungen

June 27, 2024

Der Abschnitt **Lokaler App-Zugriff** enthält Richtlinieneinstellungen zum Verwalten lokal installierter Anwendungen mit gehosteten Anwendungen. Diese Richtlinieneinstellungen legen die Integration in einer gehosteten Desktopumgebung fest.

### Lokalen App-Zugriff zulassen

Mit dieser Einstellung legen Sie fest, ob die Integration lokal installierter Anwendungen mit gehosteten Anwendungen zugelassen oder verweigert werden soll. Diese Richtlinieneinstellungen legen die Integration in einer gehosteten Desktopumgebung fest.

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 und in Desktopsitzungen clientseitig kein Batteriestatus im Benachrichtigungsbereich angezeigt.

Standardmäßig ist **Lokalen App-Zugriff zulassen** nicht aktiviert.

### URL-Umleitungssperrliste

Mit dieser Einstellung geben Sie Websites an, die Ziel einer Weiterleitung sind und im lokalen Webbrowser gestartet werden sollen. Dies können beispielsweise folgende Websites sein:

- Websites, für die Gebietsschema-Informationen erforderlich sind (z. B. msn.com oder news-google.com)
- Websites mit reichhaltigen Medieninhalten, die besser auf dem Benutzergerät gerendert 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, gerendert werden sollen.

In der Standardeinstellung sind keine Sites angegeben.

## Mobilerfahrung - Richtlinieneinstellungen

June 27, 2024

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.

### Touchoptimierten 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. Durch die Einstellung wird festgelegt, ob eine für Tablet-Geräte ausgelegte touchoptimierte Benutzeroberfläche zugelassen wird.

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 auf Mobilgeräten in Sitzungen 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 ist das Feature **Kombinationsfelder remoten** nicht zugelassen.

## 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

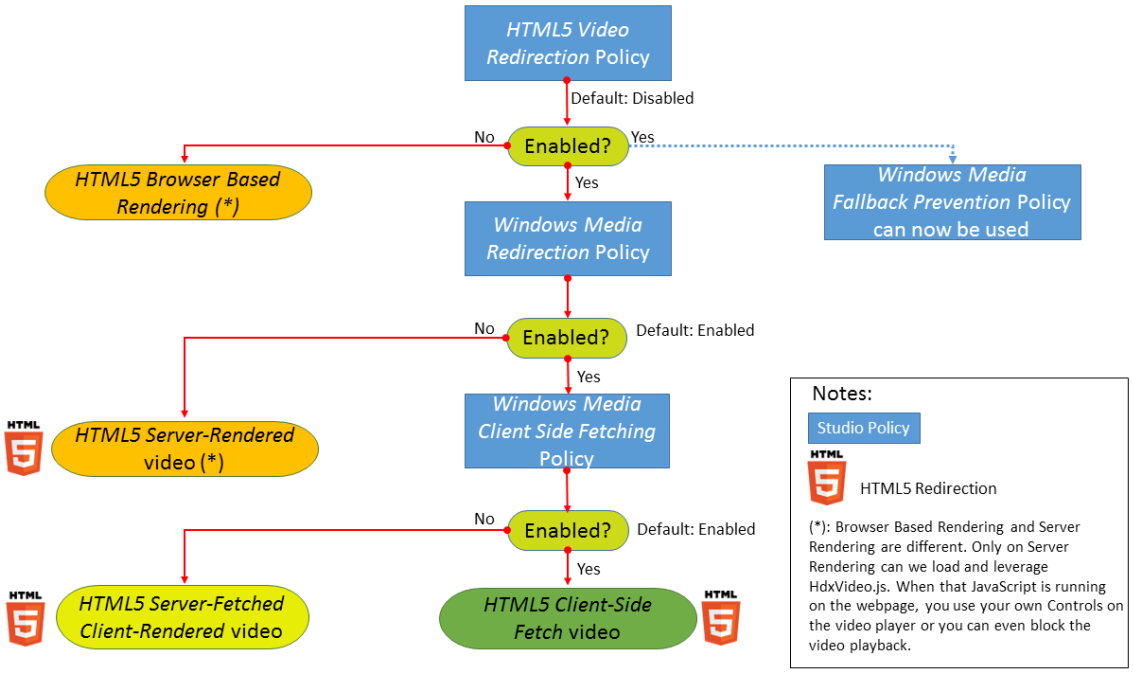
Zum Abfragen der ID der aktuellen Benutzersitzung geben Sie den Befehl **qwinsta** in der Windows-Eingabeaufforderung ein.

### 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 Webseiten 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.

Es kann sein, dass den von Ihnen kontrollierten Webseiten kein JavaScript hinzugefügt wurde und der Benutzer ein HTML5-Video wiedergibt. In diesem Fall wird in Citrix Virtual Apps and Desktops standardmäßig das serverseitige Rendering verwendet.

Lassen Sie ***Windows Media-Umleitung*** zu, damit die HTML5-Videoumleitung möglich ist. Diese Richtlinie ist für den serverseitigen Abruf und das clientseitige Rendering obligatorisch und für den clientseitigen Abruf notwendig. Beim clientseitigen Abruf muss *Clientseitiger Inhaltsabruf von Windows Media* zugelassen sein.

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

Sie können eine HTML5-Videoumleitungstestseite anzeigen.

#### TLS- und HTML5-Videoumleitung und Browserinhaltsumleitung

Sie können die HTML5-Videoumleitung für Folgendes verwenden:

- Umleitung von Videos von HTTPS-Websites
- Oder
- Umleitung von Browserinhalten zur Umleitung der gesamten Website

Das in diese Websites eingefügte JavaScript muss eine TLS-Verbindung zum Citrix HDX HTML5-Videoumleitungsdienst (WebSocketService.exe) herstellen, der auf dem VDA ausgeführt wird. Der Citrix HDX HTML5-Videoumleitungsdienst im Zertifikatsspeicher auf dem VDA generiert zwei benutzerdefinierte Zertifikate für Folgendes:

- Ausführen der Videoumleitung
- Gewährleistung der TLS-Integrität der Webseite

HdxVideo.js kommuniziert über Secure WebSockets mit dem auf dem VDA ausgeführten Dienst WebSocketService.exe. Dieser 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.
Der Registrierungsschlüssel muss nicht manuell festgelegt werden.

HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream

Name: MSTeamsRedirSupport

Wert: DWORD (1 - ein, 0 - aus)

> **Hinweis:**
>
> Es kann sein, dass Sie VDAs der Version 1906.2 oder höher mit älteren Controller-Versionen verwenden, für die die Richtlinie in Web Studio nicht verfügbar ist. Ein Beispiel für eine ältere Controller-Version ist Version 7.15. In diesem Fall ist die HDX-Optimierung auf dem VDA standardmäßig aktiviert. Ab Workspace-App-Version 1907 startet Microsoft Teams im optimierten Modus. Weitere Hinweise zur gemischten Verwendung von 7.15 LTSR-Controllern und CR-VDAs finden Sie im Knowledge Center-Artikel CTX205549.

> In diesem Fall können Sie die Registrierungseinstellung überschreiben, um das Feature für bestimmte Benutzer zu deaktivieren. Verwenden Sie eine Gruppenrichtlinie zur Anwendung eines Anmeldeskripts auf die Organisationseinheit des Benutzers, um die Registrierungseinstellung außer Kraft zu 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.

Bei Verwendung von **Multimediakonferenzen** müssen folgende Bedingungen erfüllt sein:

- Der Gerätetreiber des Herstellers für die in der Multimediakonferenz verwendete Webcam ist installiert.
- Die Webcam wird mit dem Benutzergerät verbunden, bevor eine Videokonferenzsitzung gestartet 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. Dieser Versuch wird fortgesetzt, 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. Die Einstellung aktiviert Folgendes:

- Transcodierung von Multimediainhalten in Echtzeit
- Zulassen von Audio- und Videostreaming für Mobilgeräte über problembehaftete Netzwerke
- Optimieren der Benutzererfahrung durch eine verbesserte Übermittlung von Windows Media-Inhalt über WAN

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 Transcodierung von Multimediainhalten in Echtzeit je nach Bedarf automatisch bereitgestellt, um das Medienstreaming zu aktivieren. Gleichzeitig wird eine nahtlose Benutzererfahrung auch bei schlechten Netzwerkbedingungen ermöglicht.

### 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, müssen die folgenden Einstellungen vorhanden und zugelassen sein:

- **Windows Media-Umleitung**
- **Einstellungen für Optimierung von Windows Media-Multimediaumleitung über WAN**

### Verhindern von Fallback auf Windows Media

Diese Einstellung gilt für die Browserinhaltsumleitung, HTML5 und Windows Media. Damit sie HTML5 unterstützt, 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**.

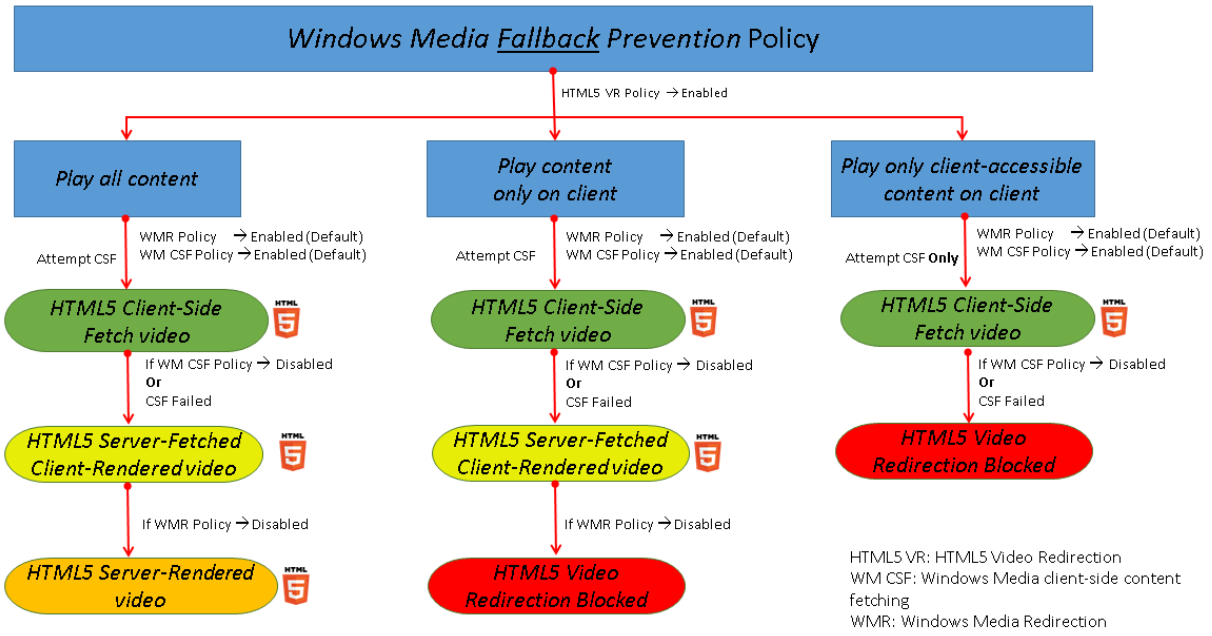
Wählen Sie für die Konfiguration dieser Einstellung eine der folgenden Optionen:

- **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, ist die folgende Fehlermeldung im Playerfenster zu sehen (Standardanzeigedauer: 5 Sekunden).

```
"Company has blocked video because of lack of resources"
```




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. Das Zulassen dieser Einstellung verbessert die Netzwerkauslastung und Serverskalierbarkeit. Die Verbesserung wird durch Verlagerung der gesamten Medienverarbeitung vom Hostserver auf das Benutzergerät erreicht. Dadurch wird auch das Erfordernis der Installation eines erweiterten Multimedia-Frameworks, z. B. von Microsoft DirectShow oder Media Foundation, auf Benutzergeräten hinfällig. Das Benutzergerät muss lediglich Dateien 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.

Wenn diese Einstellung aktiviert ist, erhöht sich die Ton- und Bildqualität von Medien, die auf dem Server gerendert werden, auf ein mit einer lokalen Wiedergabe auf dem Benutzergerät vergleichbares Niveau. 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. Diese Situation ist selten, kann aber mit geringer Bandbreite vorkommen, beispielsweise bei Medien, in denen die Schlüsselbilder (Keyframes) 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).

## Multistreamverbindungen - Richtlinieneinstellungen

June 27, 2024

Im Abschnitt **Multistreamverbindungen** finden Sie Richtlinieneinstellungen zum Verwalten der Quality-of-Service-Priorität für mehrere ICA-Verbindungen in einer Sitzung.

> **Hinweis:**
>
> Die MTU-Discovery wird nicht unterstützt, wenn die Multistream-Verbindungsrichtlinie aktiviert ist.

### 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) verwendet werden. Diese Spezifikation hilft beim

Austausch von Audiopaketdaten mit dem Benutzergerät. 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 Multistream aktiviert ist, wird die MTU-Discovery, ein Feature des adaptiven Transports, nicht unterstützt.

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

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:

- AppFlow: 2
- Audio: 0
- Browserinhaltsumleitung: 2
- Client-COM-Portzuordnung: 3
- Clientlaufwerkszuordnung: 2
- Clientdruckerzuordnung: 3
- Zwischenablage: 2
- CTXDND: 1 (**Hinweis:** Dies unterstützt das Ziehen und Ablegen von Dateien zwischen einer Citrix Sitzung und einem lokalen Endpunkt.)
- DVC-Plug-In (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.

# Portumleitung - Richtlinieneinstellungen

June 27, 2024

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. Diese Ports werden nicht von Legacyanwendungen verwendet, die Druckaufträge an die Druckobjekte auf dem Benutzergerät senden. Die meisten Anwendungen können heute Druckaufträge an 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)

## Drucken - Richtlinieneinstellungen

June 27, 2024

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 kann 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. Melden Sie sich bei Web Studio an, wählen Sie im linken Bereich **Richtlinien** und klicken Sie dann auf die Registerkarte **Richtlinien**.
2. Aktivieren Sie die Richtlinie **Sitzungsdrucker**.
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 ein Sitzungsdrucker einen nativen Druckertreiber benötigt und der native Druckertreiber nicht auf dem VDA installiert ist, wird der Sitzungsdrucker möglicherweise nicht in der Sitzung erstellt.

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.

### Abwarten der Druckererstellung vor Anwendungsstart

Verwenden Sie die Richtlinie auf dem Delivery Controller, um das Feature für Citrix Virtual Desktops zu aktivieren.

**Warten bis Drucker erstellt sind (Serverdesktop):**

Mit dieser Einstellung legen Sie fest, ob es eine Verzögerung bei der Sitzungsverbindung geben soll, sodass vom Client umgeleitete Drucker automatisch erstellt werden können.

Standardmäßig findet keine Verbindungsverzögerung statt.

**Warten bis Drucker erstellt sind (Citrix Virtual Apps):**

Das Ausführen des folgenden PowerShell-Cmdlets ermöglicht eine Verzögerung beim Herstellen der Verbindung zu auf Hosts mit mehreren Sitzungen ausgeführten virtuellen Apps, sodass vom Client umgeleitete Drucker automatisch erstellt werden können, bevor die App geöffnet wird.

```
Set-BrokerApplication -Name <VirtualAppName> -WaitForPrinterCreation
$true
```

Standardmäßig findet keine Verbindungsverzögerung statt.

# Clientdrucker - Richtlinieneinstellungen

June 27, 2024

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. Bei Auswahl dieser Option setzen die Remotedesktopdienste-Einstellungen für die automatische Erstellung von Clientdruckern diese Einstellung in Richtlinien mit niedrigerer Priorität außer Kraft.

## Generischen universellen Drucker automatisch erstellen

Mit dieser Einstellung aktivieren oder deaktivieren Sie die automatische Erstellung des generischen universellen Citrix Druckerobjekts für Sitzungen. Dies sind nur die 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

Mit dieser Einstellung aktivieren oder deaktivieren Sie die automatische Erstellung des Citrix PDF-Druckers für Sitzungen mit:

- Citrix Workspace-App für Windows (ab VDA 7.19)
- Citrix Workspace-App für HTML5
- 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** aus, um die Namen von Clientdruckern im alten Stil zu verwenden und die Abwärtskompatibilität mit den Namen älterer Drucker zu erhalten, wie sie in den XenDesktop-Versionen des Produkts vorliegen. Sie können diese Option mit den aktuellen Versionen von Citrix Virtual Apps and Desktops des Produkts verwenden. Ein Beispiel für einen Legacydruckernamen ist "Client/clientname#/HPLaserJet 4". Diese Option ist weniger sicher.

Wenn Sie den Citrix PDF-Drucker in einer Sitzung verwenden, die von der Citrix Workspace-App für HTML5 gestartet wurde, legen Sie die Einstellung **Clientdruckernamen** als Standard fest oder wählen Sie **Standarddruckernamen** aus. Wenn Sie **Legacydruckernamen** auswählen, unterstützt die Citrix Workspace-App für HTML5 die Option "Citrix PDF-Drucker"nicht.

### Direkte Verbindungen zu Druckservern

Mit dieser Einstellung aktivieren oder deaktivieren Sie direkte Verbindungen vom virtuellen Desktop oder von servergehosteten Anwendungen zu einem Druckserver für Clientdrucker. Hier werden die Clientdrucker in einer zugänglichen Netzwerkfreigabe gehostet.

Standardmäßig sind direkte Verbindungen aktiviert.

Aktivieren Sie direkte Verbindungen, wenn der Netzwerkdruckserver für virtuelle Desktops bzw. servergehostete Anwendungen nicht über ein WAN zugänglich ist. Direkte Verbindungen gestatten schnelleres Drucken, wenn sich der Netzwerkdruckserver und der virtuelle Desktop bzw. die servergehosteten Anwendungen 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. Mit diesen Regeln können Serveranwendungen auf Clientdrucker zugreifen, die denselben Treiber wie der Server, aber unterschiedliche Treibernamen verwenden.

Sie können die folgenden Aktionen ausführen:

- Treiberzuordnung hinzufügen
- Vorhandene Zuordnung bearbeiten
- Benutzerdefinierte Einstellungen für eine Zuordnung überschreiben
- Zuordnung entfernen
- Reihenfolge der Treibereinträge in der Liste ändern

Um eine Zuordnung hinzuzufügen, geben Sie den Clientdruckertreibernamen an und wählen dann den Servertreiber, den Sie ersetzen möchten.

### 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 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. Diese Option gilt nur, wenn ein Roamingprofil 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 das PDF-Format 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 einer 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.

## Treiber - Richtlinieneinstellungen

June 27, 2024

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 von:

- dem standardmäßigen Windows-Treibersatz
- 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 Option aus der folgenden Tabelle:

| Option | Beschreibung |
| --- | --- |
| **Nur druckermodellspezifische Treiber verwenden** | Der Clientdrucker verwendet 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** | Es werden keine modellspezifischen Standardtreiber verwendet. Nur universelle Druckertreiber werden zum Erstellen von Druckern verwendet. |
| **Universelles Drucken nur verwenden, wenn angeforderter Treiber nicht verfügbar ist** | Modellspezifische Standardtreiber werden 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. |
| **Druckermodellspezifische Treiber nur verwenden, wenn universelles Drucken nicht verfügbar ist** | Der universelle Druckertreiber wird verwendet, wenn er verfügbar ist. 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"

June 27, 2024

Der Abschnitt **Universeller Druckserver** enthält Richtlinieneinstellungen für die Behandlung des universellen Druckservers.

## SSL-Verschlüsselungssammlung

Diese Einstellung legt die SSL/TLS-Verschlüsselungssammlungen 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.

Folgende Verschlüsselungssammlungen entsprechen den einzelnen Werten:

**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: None.

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 SSL/TLS vom universellen Druckclient für Folgendes verwendet wird:

- Druckdatenstrom (CGP)-Verbindungen
- Webservice (HTTP/SOAP)-Verbindungen

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 Datenstromverbindungen (CGP) verwendete kryptografische SSL/TLS-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 Richtlinie aktiviert bzw. deaktiviert die Verwendung des universellen Citrix Druckservers. Wenden Sie die Richtlinieneinstellung auf Organisationseinheiten an, die den virtuellen Desktop oder servergehostete Anwendungen enthalten. Zu diesen Richtlinieneinstellungen gehören Fallback-Optionen, um Verbindungen zu Druckservern über den nativen Windows-Remotedruckdienst zuzulassen, falls die Citrix UPS-Komponente auf dem angeforderten Druckserver nicht installiert oder verfügbar ist. Änderungen an dieser Richtlinie treten erst nach dem Neustart des VDA in Kraft.

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 zwischen 1 und 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 Übertragungsrate wird für die Druckdaten berechnet, die von jedem Druckauftrag mit CGP an den universellen Druckserver geliefert werden. Wenden Sie die Richtlinie auf Organisationseinheiten an, die den virtuellen Desktop oder servergehostete Anwendungen enthalten.

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 zwischen 0 und 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. Außerdem werden Druckerverbindungen auf dem Server 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 warten muss, bevor der Server als offline gilt und die Last des Servers auf andere verfügbare Druckserver verteilt wird.

Der Standardschwellenwert ist 180 (Sekunden).

### Verbindungstimeout für den Webdienst des universellen Druckservers (HTTP/SOAP)

Diese Einstellung gibt die Anzahl von Sekunden an, die der universeller Druckclient warten muss, bis bei einer connect()-Operation des Webdiensts des universellen Druckservers das Zeitlimit überschritten wird. Diese Einstellung hat die folgenden Werte. Alle Werte sind numerisch und die Zeiteinheit ist Sekunden.

- Der Mindestwert ist 0.
- Der Höchstwert ist 60.
- Der Standardwert ist 10.

Wenn das Timeout zwischen 1 und 60 liegt, wartet der universelle Druckclient die angegebene Zeit, bis der Vorgang abgeschlossen ist. Dies ist ein Connect TCP Socket-Vorgang. Sockets sind eine Einrichtung von Windows, die die Kommunikation zwischen Prozessen über TCP/IP-Netzwerke ermöglicht.

Wenn das Timeout 0 ist, verwendet der universelle Druckclient das Standardtimeout des Betriebssystems. Diese Konfiguration war die in den vorherigen Versionen des universellen Druckclients vor dieser Änderung verfügbare Konfiguration.

Der universelle Druckclient ist die Komponente des Virtual Delivery Agent (VDA), die mit dem universellen Druckserver kommuniziert.

> **Hinweis:**
>
> Diese Richtlinieneinstellung gilt für VDA-Version 7.35 und höher.

### Empfangstimeout für den Webdienst des universellen Druckservers (HTTP/SOAP)

Diese Einstellung gibt die Anzahl von Sekunden an, die der universeller Druckclient warten muss, bis bei einer recv()-Operation des Webdiensts des universellen Druckservers das Zeitlimit überschritten wird. Diese Einstellung hat die folgenden Werte. Alle Werte sind numerisch und die Zeiteinheit ist Sekunden.

- Der Mindestwert ist 0.
- Der Höchstwert ist 60.
- Der Standardwert ist 10.

Wenn das Timeout zwischen 1 und 60 liegt, wartet der universelle Druckclient die angegebene Zeit, bis der Vorgang abgeschlossen ist. Dies ist ein Receive TCP Socket-Vorgang. Sockets sind eine Einrichtung von Windows, die die Kommunikation zwischen Prozessen über TCP/IP-Netzwerke ermöglicht.

Wenn das Timeout 0 ist, verwendet der universelle Druckclient das Standardtimeout des Betriebssystems. Diese Konfiguration war die in den vorherigen Versionen des universellen Druckclients vor dieser Änderung verfügbare Konfiguration.

Der universelle Druckclient ist die Komponente des Virtual Delivery Agent (VDA), die mit dem universellen Druckserver kommuniziert.

> **Hinweis:**
>
> Diese Richtlinieneinstellung gilt für VDA-Version 7.35 und höher.

### Sendetimeout für den Webdienst des universellen Druckservers (HTTP/SOAP)

Diese Einstellung gibt die Anzahl von Sekunden an, die der universeller Druckclient warten muss, bis bei einer send()-Operation des Webdiensts des universellen Druckservers das Zeitlimit überschritten wird. Diese Einstellung hat die folgenden Werte. Alle Werte sind numerisch und die Zeiteinheit ist Sekunden.

- Der Mindestwert ist 0.
- Der Höchstwert ist 60.
- Der Standardwert ist 10.

Wenn das Timeout zwischen 1 und 60 liegt, wartet der universelle Druckclient die angegebene Zeit, bis der Vorgang abgeschlossen ist. Dies ist ein Send TCP Socket-Vorgang. Sockets sind eine Einrichtung von Windows, die die Kommunikation zwischen Prozessen über TCP/IP-Netzwerke ermöglicht.

Wenn das Timeout 0 ist, verwendet der universelle Druckclient das Standardtimeout des Betriebssystems. Diese Konfiguration war die in den vorherigen Versionen des universellen Druckclients vor dieser Änderung verfügbare Konfiguration.

Der universelle Druckclient ist die Komponente des VDAs, die mit dem universellen Druckserver kommuniziert.

> **Hinweis:**
>
> Diese Richtlinieneinstellung gilt für VDA-Version 7.35 und höher.

## Universelles Drucken - Richtlinieneinstellungen

June 27, 2024

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 wird Folgendes festgelegt:

- verfügbare maximale Qualität für Bilder, die mit dem universellen Citrix Druckertreiber gedruckt werden
- verfügbare minimale Komprimierung für Bilder, 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
- Beste 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:

- Es kann vorkommen, dass die Komprimierung in der Einstellung **Universelles Drucken - Komprimierungslimit** niedriger ist als der Wert in der Einstellung **Universelles Drucken - Optimierungsstandards**. In diesem Fall 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. Diese Einstellung stellt sicher, dass jedes eindeutige Bild oder jede Schriftart nur einmal zum Drucker gesendet wird. Standardmäßig werden eingebettete Bilder und Schriftarten zwischengespeichert. 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 - Bildkomprimierungslimit** enthält, achten Sie auf Folgendes:

- Es kann vorkommen, dass die Komprimierung in der Einstellung **Universelles Drucken - Komprimierungslimit** niedriger ist als der Wert in der Einstellung **Universelles Drucken - Optimierungsstandards**. In diesem Fall 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 generische 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.

Wenn beispielsweise “Mittlere Auflösung (600 dpi)”konfiguriert ist, können Benutzer die Ausgabe nur mit einer maximalen Qualität von 600 dpi drucken. Außerdem enthält die Einstellung **Druckqualität** auf der Registerkarte **Erweitert** im Dialogfeld **Universeller Drucker** 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

# Sicherheit - Richtlinieneinstellungen

June 27, 2024

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. Es kann vorkommen, dass ein höherer Verschlüsselungsgrad auf dem Server oder Benutzergerät eingestellt ist. In diesem Fall können die 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 er-

forderlich 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 diese Einstellung 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. Diese Parameter werden bei der Installation des Virtual Delivery Agents in der Windows-Registrierung gespeichert. 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.

## Serverlimits - Richtlinieneinstellungen

June 27, 2024

Der Abschnitt **Serverlimits** enthält die Richtlinieneinstellung zum Steuern von Sitzungen im Leerlauf.

### Serverleerlauf-Zeitintervall

Mit dieser Einstellung geben Sie an, wie lange eine ununterbrochene Benutzersitzung erhalten bleibt, wenn keine Benutzereingaben stattfinden. Die Daten werden in Millisekunden berechnet.

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.

## Sitzungslimits - Richtlinieneinstellungen

June 27, 2024

Der Abschnitt **Sitzungslimits** enthält Richtlinieneinstellungen, die steuern, wie lange Sitzungen verbunden bleiben, bevor sie sich abmelden müssen.

### 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.

### Remote-PC-Zugriff –Timer für getrennte Sitzung

Diese Einstellung aktiviert oder deaktiviert einen Timer, der eine getrennte Benutzersitzung nach Ablauf des Timers abmeldet. Wenn Sie diese Einstellung aktivieren, können Sie mit der Einstellung **Getrennte Sitzungen - Timerintervall** festlegen, wie viele Minuten ein getrennter Desktop gesperrt bleibt, bevor die Benutzersitzung abgemeldet wird.

Diese Einstellung ist standardmäßig deaktiviert.

### 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).

### Sitzungstrennungstimer –Mehrere Sitzungen

Diese Einstellung aktiviert bzw. deaktiviert einen Timer, der angibt, wie lange eine getrennte RDS-Sitzung bestehen bleibt, bevor sie abgemeldet wird. Standardmäßig ist dieser Timer deaktiviert und getrennte Sitzungen werden nicht abgemeldet.

### Sitzungstrennungstimerintervall –Mehrere Sitzungen

Diese Einstellung legt fest, wie viele Minuten eine getrennte RDS-Sitzung bestehen bleibt, bevor sie 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).

### Sitzungsverbindungstimer –Mehrere Sitzungen

Mit dieser Einstellung aktivieren oder deaktivieren Sie einen Timer, mit dem die maximale Dauer einer ununterbrochenen Verbindung zwischen einem Benutzergerät und einem Terminalserver festgelegt wird. Standardmäßig ist dieser Timer aktiviert.

### Sitzungsverbindungstimerintervall –Mehrere Sitzungen

Diese Einstellung legt die Höchstdauer einer ununterbrochenen Verbindung zwischen einem Benutzergerät und einer RDS-Sitzung in Minuten fest. Standardmäßig ist die maximale Dauer 1440 Minuten (24 Stunden).

### Sitzungsleerlauftimer

Wenn keine Benutzereingaben stattfinden, wird diese Einstellung verwendet, um Folgendes zu aktivieren oder zu deaktivieren:

- Einen Timer, der angibt, wie lange eine ununterbrochene Benutzergeräteverbindung mit einem Desktop erhalten bleibt.

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

Wenn keine Benutzereingaben stattfinden, wird diese Einstellung verwendet, um Folgendes festzulegen:

- Die Anzahl der Minuten, für die eine ununterbrochene Benutzergeräteverbindung zu einem Desktop aufrechterhalten wird.

Standardmäßig bleiben Leerlaufsitzungen 1440 Minuten (24 Stunden) erhalten.

### Sitzungsleerlauftimer –Mehrere Sitzungen

Mit dieser Einstellung aktivieren oder deaktivieren Sie einen Timer, um die maximale Dauer einer Verbindung im Leerlauf zwischen einem Benutzergerät und einem Terminalserver zu bestimmen. Standardmäßig ist dieser Timer aktiviert.

### Sitzungsleerlauftimerintervall –Mehrere Sitzungen

Diese Einstellung legt die Dauer einer Verbindung im Leerlauf zwischen einem Benutzergerät und einer RDS-Sitzung in Minuten fest. Standardmäßig ist die maximale Dauer 1440 Minuten (24 Stunden).

> **Hinweis:**
>
> Es ist zu erwarten, dass Timereinstellungen für Multisitzungsmaschinen, die über Microsoft-Gruppenrichtlinien konfiguriert wurden, von Timereinstellungen, die mithilfe von Citrix Richtlinien konfiguriert wurden, überschrieben werden. Um unerwartetes Verhalten zu verhindern, wird empfohlen, Timereinstellungen mit einer der beiden Methoden zu konfigurieren.

# Sitzungszuverlässigkeit - Richtlinieneinstellungen

June 27, 2024

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.

Die Einstellungen in Web Studio werden auf dem Client für Folgendes durchgesetzt:

- Citrix Workspace-App 1808 und später
- Citrix Receiver für Windows 4.7 und höher.

Die Web Studio-Richtlinie überschreibt das Citrix Receiver-Gruppenrichtlinienobjekt auf den Clients. Bei Änderungen an diesen Richtlinien in Web 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: Legen Sie die Richtlinie in Web Studio fest.
> - Citrix Receivers für Windows vor 4.7 —Legen Sie die Richtlinie in Web Studio fest. Legen Sie außerdem die Citrix Receiver-Gruppenrichtlinienobjektvorlage auf dem Client fest, um ein konsistentes Verhalten zu erzielen.

Durch die Sitzungszuverlässigkeit bleiben Sitzungen aktiv und auf dem Bildschirm des Benutzers, wenn die Netzwerkverbindung unterbrochen wird. Die Benutzer sehen so lange weiterhin die Anwendung, die sie verwenden, bis die Netzwerkkonnektivität wiederhergestellt ist.

Verwenden Sie die Sitzungszuverlässigkeit, um die Sitzung auf dem Server aktiv zu halten. Als Hinweis darauf, dass die Verbindung unterbrochen wird, wird die Anzeige opak. Der Benutzer sieht während der Unterbrechung möglicherweise eine eingefrorene Sitzung. Der Benutzer kann die Interaktion mit der Anwendung fortsetzen, wenn die Netzwerkverbindung wiederhergestellt ist. Die Sitzungszuverlässigkeit verbindet Benutzer ohne Neuauthentifizierung wieder.

Wenn Sie sowohl Sitzungszuverlässigkeit als auch die Funktion zur automatischen Wiederverbindung verwenden, werden beide Funktionen nacheinander ausgeführt. Die Sitzungszuverlässigkeit beendet oder trennt die Benutzersitzung, nachdem der mit der Einstellung "Sitzungszuverlässigkeit - Timeout"festgelegte Zeitraum abgelaufen ist. Anschließend werden die Richtlinieneinstellungen für die automatische Wiederverbindung von Clients wirksam und es wird versucht, die Verbindung mit der unterbrochenen Sitzung wiederherzustellen.

Standardmäßig ist die Sitzungszuverlässigkeit zugelassen.

> **Hinweis:**
>
> Wenn Citrix ADC verwendet wird, müssen Sie **Sitzungszuverlässigkeit aktivieren** in Citrix StoreFront unter **Citrix Gateways verwalten**/**Secure Ticket Authority** auswählen, um es als Proxy für ICA-Verbindungen einzustellen.

### Sitzungszuverlässigkeit - Portnummer

Mit dieser Einstellung geben Sie die TCP-Portnummer für eingehende Sitzungszuverlässigkeitsverbindungen an.

Die Standardeinstellung der Portnummer ist "2598".

### Sitzungszuverlässigkeit - Timeout

Diese Einstellung legt die Zeitspanne in Sekunden fest. Zu diesem Zeitpunkt wartet der Sitzungszuverlässigkeitsproxy darauf, dass ein Benutzer die Verbindung wiederherstellt, bevor das Trennen der Sitzung zugelassen wird.

Sie können zwar eine Sitzung länger offen lassen, dies ist jedoch eine Komfortfunktion und der Benutzer wird nicht zu einer Neuauthentifizierung aufgefordert. Je länger eine Sitzung geöffnet bleibt, umso größer ist das Risiko, dass ein Benutzer sein Gerät unbeaufsichtigt lässt und unbefugte Benutzer Zugang erhalten.

Die Standardeinstellung des Timeouts ist 180 Sekunden (drei Minuten).

## Sitzungswasserzeichen - Richtlinieneinstellungen

June 27, 2024

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, das 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.

### Sitzungswasserzeichen aktivieren

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 ist das Sitzungswasserzeichen deaktiviert.

### Client-IP-Adresse einschließen

Wenn Sie diese Einstellung aktivieren, wird in der Sitzung die aktuelle Client-IP-Adresse als Wasserzeichen angezeigt.

Die Option Client-IP-Adresse einschließen ist standardmäßig deaktiviert.

### Verbindungszeit einschließen

Wenn Sie diese Einstellung aktivieren, wird im Sitzungswasserzeichen eine Verbindungszeit angezeigt. Das Format ist JJJJ/MM/TT hh:mm. Die angezeigte Zeit basiert auf der Systemuhr und der Zeitzone.

Die Option Verbindungszeit einschließen ist standardmäßig deaktiviert.

### Anmeldename einschließen

Wenn Sie diese Einstellung aktivieren, wird in der Sitzung der aktuelle Anmeldename als Wasserzeichen angezeigt. Das Anzeigeformat ist BENUTZERNAME@DOMÄNENNAME. Es wird empfohlen, Benutzernamen auf maximal 20 Zeichen zu beschränken. Wenn ein Benutzernamen mehr als 20 Zeichen hat, werden die Zeichen evtl. zu klein angezeigt oder abgeschnitten und die Wirksamkeit des Wasserzeichens verringert.

Die Option Anmeldename einschließen ist standardmäßig aktiviert.

### VDA-Hostname einschließen

Wenn Sie diese Einstellung aktivieren, wird in der Sitzung der VDA-Hostname der aktuellen ICA-Sitzung als Wasserzeichen angezeigt.

Die Option VDA-Hostname einschließen ist standardmäßig aktiviert.

### VDA-IP-Adresse einschließen

Wenn Sie diese Einstellung aktivieren, wird in der Sitzung die VDA-IP-Adresse der aktuellen ICA-Sitzung als Wasserzeichen angezeigt.

Die VDA-IP-Adresse ist standardmäßig deaktiviert.

### Sitzungswasserzeichenstil

Diese Einstellung steuert, ob eine einzelne oder mehrere Wasserzeichenbeschriftungen angezeigt werden sollen. Wählen Sie in dem Dropdownmenü **Wert** die Option **Einzeln** oder **Mehrere**.

Bei Auswahl von **Mehrere** werden fünf Wasserzeichenbeschriftungen in der Sitzung angezeigt: eine in der Mitte und vier in den Ecken.

Bei Auswahl von **Einzeln** wird nur eine Wasserzeichenbeschriftung in der Mitte angezeigt.

Standardmäßig ist für Sitzungswasserzeichenstil die Option Mehrere ausgewählt.

### Benutzerdefinierter Wasserzeichentext

Mit dieser Einstellung können Sie eine eigene Zeichenfolge (z. B. den Unternehmensnamen) zur Anzeige im Sitzungswasserzeichen anwenden. Wenn Sie eine Zeichenfolge angeben, wird dieser Text in einer neuen Zeile nach den anderen Informationen im Wasserzeichen angezeigt. Der benutzerdefinierte Text für Wasserzeichen ist auf 25 Unicode-Zeichen begrenzt. Wenn Sie eine längere Zeichenfolge konfigurieren, wird diese auf 25 Zeichen gekürzt.

Es gibt keinen Standardtext.

Ab Citrix Virtual Apps and Desktops 7 2206 können Sie den Text mithilfe von benutzerdefinierten Tags weiter anpassen. Die maximale Anzahl von Zeichen im benutzerdefinierten Text erhöht sich dadurch auf 1024.

Die verfügbaren Tags für Wasserzeicheneinstellungen sind in der folgenden Tabelle aufgeführt:

| Tag | Beschreibung | Beispiel |
|---|---|---|
| <font=value> | Hiermit können Sie die Schriftart des Wasserzeichentexts ändern. Der Wert ist der Name einer auf dem VDA verfügbaren Schriftart. | <font=Courier New> |
| <fontzoom=value> | Hiermit können Sie den Zoomfaktor für die Schriftart festlegen (in Prozent). Der Wert ist 200, wodurch der Wasserzeichentext auf 200 % vergrößert wird. | <fontzoom=200> |
| <position=value> | Hiermit können Sie die Position des Wasserzeichentexts ändern. Mögliche Werte sind center, topleft, topright, bottomleft und bottomright. Dieses Tag ist nur im Layoutstil "single style" anwendbar. | <position=topright> |
| <rotation=value> | Hiermit können Sie den Wasserzeichentext drehen. Der Wert wird in Grad angegeben und kann zwischen -360 und 360 liegen. | <rotation=45> |
| <style=value> | Hiermit können Sie den Anzeigestil ändern. Dieses Tag überschreibt die Richtlinie zum Sitzungswasserzeichenstil. | <style=single> |

Folgende Wasserzeichenstile sind verfügbar:

- Single style: Im Zentrum der Sitzung wird ein einzelnes Wasserzeichen mit Text angezeigt. Sie können die Position mit dem Positionstag ändern.
- xstyle oder multiple: In der Sitzung werden fünf Wasserzeichen angezeigt –eins in der Mitte und jeweils eins in jeder Ecke.
- Tile: In der Sitzung werden mehrere Textfelder angezeigt. Der Wasserzeichentext wird gleichmäßig über den gesamten Bildschirm verteilt.

Die verfügbaren Tags zum Ändern des Wasserzeichentexts sind in der folgenden Tabelle aufgeführt:

| Tag | Beschreibung |
|---|---|
| <clientip> | Die IP-Adresse des Endpunkts. |
| <date> | Das Datum, an dem die Sitzung eingerichtet wurde. |
| <domain> | Der Domänenname des angemeldeten Benutzerkontos. |
| <hostname> | Der Maschinenname des VDA. |
| <newline> | Hiermit wird eine zusätzliche Zeile erstellt. |
| <serverip> | Die IP-Adresse des VDA. |
| <time> | Die Uhrzeit, zu der die Sitzung eingerichtet wurde. |
| <username> | Der Name des Benutzers. |

> **Hinweis:**
>
> - Die Richtlinie **Benutzerdefinierter Wasserzeichentext** wird nur wirksam, wenn die Richtlinie **Sitzungswasserzeichen aktivieren** aktiviert ist. Der Standardwert ist *Deaktiviert*.
> - Wenn Sie die Tags zum Ändern des Wasserzeichentexts verwenden, werden alle anderen Richtlinien für Sitzungswasserzeichen mit Ausnahme von **Sitzungswasserzeichen aktivieren** ignoriert. Wenn Sie die Tags für Wasserzeichentexteinstellungen verwenden, können Sie alle anderen Wasserzeichenrichtlinien verwenden.

### Wasserzeichentransparenz

Sie können eine Wasserzeichendeckkraft von 0–100 angeben. Je größer der Wert, desto deckender ist das Wasserzeichen.

Der Standardwert ist 17.

## Zeitzonensteuerung - Richtlinieneinstellungen

June 27, 2024

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 Benutzergeräten. Dazu gehören Benutzergeräte, 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. Es kann vorkommen, dass diese Einstellung mit Citrix Receiver-Geräten verwendet wird, die detaillierte Zeitzoneninformationen an den Server senden. Dies könnten beispielsweise unterstützte Versionen von Citrix Receiver für Windows sein. In diesem Fall hat diese Einstellung keine Wirkung.

### Wiederherstellen der Zeitzone des Desktopbetriebssystems beim Trennen oder Abmelden der Sitzung

Es kann vorkommen, dass der Benutzer eine Sitzung trennt oder sich davon abmeldet. In diesem Fall legt diese Einstellung fest, ob die Zeitzoneneinstellung eines VDAs für Einzelsitzungs-OS auf die ursprüngliche Maschinenzeitzone zurückgesetzt wird. 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**.

Wenn Sie einen Einzelsitzungs-VDA (zuvor “Workstation VDA”) auf Maschinen mit einem Serverbetriebssystem verwenden, konfigurieren Sie das lokale Benutzerrecht **Zeitzone ändern** in **Alle**. 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, wenn der Server ein 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.

## TWAIN-Geräte - Richtlinieneinstellungen

June 27, 2024

Der Abschnitt **TWAIN-Geräte** enthält Richtlinieneinstellungen, die sich auf Folgendes beziehen:

- Zuordnung von TWAIN-Geräten, zum Beispiel Digitalkameras oder Scanner
- Optimieren der Bildübertragung vom Server zum Client

> **Hinweis:**
>
> TWAIN 2.0 wird mit Citrix Receiver für Windows 4.5 unterstützt.

### Client-TWAIN-Geräteumleitung

TWAIN-Geräte kommunizieren mit servergehosteten Bildverarbeitungsanwendungen unter Verwendung des TWAIN-Protokolls.

Diese Einstellung ermöglicht oder verhindert, dass Benutzer auf TWAIN-Geräte auf dem Benutzergerät zugreifen. 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.

## USB-Geräte - Richtlinieneinstellungen

June 27, 2024

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. Außerdem sind die USB-Benutzereinstellungen für eine automatische Verbindung der USB-Geräte konfiguriert.

> **Hinweis:**
>
> In Receiver für Windows 4.2 werden USB-Geräte auch automatisch umgeleitet, wenn das Gerät im Modus "Desktop Appliance"ist. Außerdem wird der Verbindungsbalken nicht angezeigt. In älteren Versionen von Citrix Receiver für Windows werden USB-Geräte auch automatisch umgeleitet, wenn sie wie folgt ausgeführt werden:

- im Modus "Desktop Appliance"
- mit von einer virtuellen Maschine (VM) gehosteten Anwendungen

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 entweder auf dem Clientendpunkt oder in der DDC-Richtlinie 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. Erstellen 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. Vergewissern Sie sich, 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. Außerdem 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.

Use this registry on client endpoint to configure whether plain audio devices are automatically redirected:

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.

Eine generische USB-Umleitung ist für Folgendes erforderlich:

- Nicht-Windows-Clients (z. B. Linux-Clients)
- Clients, bei denen der Benutzerzugriff vom Kunden auf lokale Clientfunktionen eingeschränkt wurde

Die generische USB-Umleitung kann jedes USB-Speichergerät ohne Hardwareverschlüsselung in VDA-Sitzungen mit Einzel- und Multisitzungs-OS umleiten.

Vor Citrix Virtual Apps and Desktops 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 Desktops 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. Es kann vorkommen, dass ein Gerät nicht konform ist oder nicht gemäß dem ursprünglichen Zweck verwendet werden soll. In diesem Fall 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 entspricht nicht in jedem Fall Ihren Wünschen. Beispiele für Citrix-optimierbare Geräte sind Drucker sowie Audio-, Video-, Speicher- und Standbildgeräte. 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.

### Zulassen, dass vorhandene USB-Geräte automatisch verbunden werden

Diese Einstellung ermöglicht oder verhindert die automatische Verbindung der zu Beginn einer Sitzung mit dem Endpunkt verbundenen USB-Geräte mit der Remotesitzung.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, wählen Sie eine der folgenden Optionen:

- Vor dem Umleiten von verfügbaren USB-Geräten fragen.
- Verfügbare USB-Geräte nicht automatisch umleiten.
- Verfügbare USB-Geräte automatisch umleiten.

Standardmäßig ist die Option **Vor dem Umleiten von verfügbaren USB-Geräten fragen** ausgewählt. Je nach der ausgewählten Richtlinie kann die Option, die im Bereich **Einstellungen** > **Geräte** des Clients ausgewählt wurde, außer Kraft gesetzt werden.

> **Hinweis:**
>
> Derzeit gilt die Richtlinie **Zulassen, dass vorhandene USB-Geräte automatisch verbunden werden** nur für die Citrix Workspace-App für Windows.

### Zulassen, dass neu angeschlossene USB-Geräte automatisch verbunden werden

Diese Einstellung ermöglicht oder verhindert die automatische Verbindung der USB-Geräte, die während einer Sitzung mit dem Endpunkt verbunden werden, mit der Remotesitzung.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, wählen Sie eine der folgenden Optionen:

- Vor dem Umleiten von verfügbaren USB-Geräten fragen.
- Verfügbare USB-Geräte nicht automatisch umleiten.

- Verfügbare USB-Geräte automatisch umleiten.

Standardmäßig ist die Option **Vor dem Umleiten von verfügbaren USB-Geräten fragen** ausgewählt. Je nach der ausgewählten Richtlinie kann die Option, die im Bereich **Einstellungen** > **Geräte** des Clients ausgewählt wurde, außer Kraft gesetzt werden.

> **Hinweis:**
>
> Derzeit gilt die Richtlinie **Zulassen, dass neu angeschlossene USB-Geräte automatisch verbunden werden** nur für die Citrix Workspace-App für Windows.

### Regeln für die Client-USB-Geräteumleitung (Version 2)

Diese Einstellung legt Regeln für das Filtern, Teilen und automatische Verbinden von USB-Geräten mit Remotesitzungen fest.

Wenn diese Einstellung ausgewählt ist, ersetzt der Host die Einstellung von *Regeln für die Client-USB-Geräteumleitung* durch die in dieser Einstellung konfigurierten Geräteregeln.

Weitere Informationen finden Sie unter Konfigurieren der Umleitung von USB-Verbundgeräten.

## Positivliste virtueller Kanäle - Richtlinieneinstellungen

June 27, 2024

Die Richtlinieneinstellung **Positivliste für virtuelle Kanäle** ermöglicht die Verwendung einer Positivliste, die angibt, welche virtuellen Kanäle in einer ICA-Sitzung geöffnet werden dürfen.

Wenn diese Option deaktiviert wird, sind alle virtuellen Kanäle zulässig.

Wenn die Option aktiviert wird, sind nur virtuelle Citrix Kanäle zulässig.

Um benutzerdefinierte virtuelle Kanäle oder solche von Drittanbietern zu verwenden, fügen Sie die virtuellen Kanäle der Liste hinzu. Eintragen eines virtuellen Kanals in die Liste:

1. Geben Sie den Namen des virtuellen Kanals gefolgt von einem Komma ein.
2. Geben Sie den Pfad zu dem Prozess ein, der auf den virtuellen Kanal zugreift.

Weitere Pfade können durch Kommas getrennt aufgelistet werden.

Beispiel:

```
CTXCVC1,C:\VC1\vchost.exe
```

```
CTXCVC2,C:\VC2\vchost.exe,C:\Program Files\Third Party\vcaccess.exe
```

Ab Citrix Virtual Apps and Desktops 7 2109 sind Positivlisten für virtuelle Kanäle standardmäßig aktiviert. Weitere Informationen zum Hinzufügen virtueller Kanäle zur Positivliste finden Sie unter Hinzufügen virtueller Kanäle zur Positivliste.

Wenn Sie HDX RealTime Optimization Pack für Skype for Business verwenden, fügen Sie den virtuellen Kanal der Positivliste hinzu. Weitere Informationen finden Sie in der Dokumentation zum HDX Real-Time Optimization Pack.

> **Wichtig:**
>
> Die VDA-Maschinen müssen neu gestartet werden, damit die Einstellung wirksam wird.

Weitere Informationen zu virtuellen Kanälen finden Sie unter Virtuelle ICA-Kanäle.

### Protokollierung –Positivliste virtueller Kanäle

Sie können diese Richtlinieneinstellung verwenden, um die Ebene für die Positivliste für die Protokollierung virtueller Kanäle zu konfigurieren.

Die folgenden Optionen sind verfügbar:

| Optionen | Beschreibung |
| --- | --- |
| Deaktiviert | Deaktiviert alle Protokollereignisse. |
| Nur Warnungen protokollieren | Ereignisse werden nur für benutzerdefinierte virtuelle Kanäle protokolliert, die versuchen zu öffnen und die nicht Teil der Zulassungsliste sind. |
| Alle Ereignisse protokollieren | Alle Ereignisse werden protokolliert |

### Protokolldrosselung für virtuelle Kanäle –Positivliste

Sie können diese Richtlinieneinstellung verwenden, um die Häufigkeit der Protokollierung von Ereignissen für eine aktive Sitzung zu konfigurieren.

Alle Ereignisse für jeden virtuellen Kanal werden bei ihrem ersten Auftreten protokolliert. Wiederholte Ereignisse werden für die Dauer der Drosselungsperiode unterdrückt, solange die Sitzung aktiv ist. Wenn eine Sitzung getrennt wird, wird die Drosselungsperiode zurückgesetzt.

## Visuelle Anzeige - Richtlinieneinstellungen

June 27, 2024

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 die Reaktion bei Verbindungen mit geringer Bandbreite. Diese Aktion kann jedoch eine geringfügige Verschlechterung der Bildqualität verursachen. 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.

## Bewegtbilder - Richtlinieneinstellungen

June 27, 2024

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.

> **Hinweis:**
>
> Die Mindestframeratesollwert ist veraltet und auf 10 Bilder pro Sekunde festgelegt. Dies kann von Endbenutzern mithilfe des Qualitätsreglers in der Grafikstatusanzeige geändert werden.

## Standbilder - Richtlinieneinstellungen

June 27, 2024

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 Röntgen-

bildern, wo kein Qualitätsverlust akzeptabel ist, sollten Sie die verlustreiche Komprimierung nicht einsetzen.

Verwandte Richtlinieneinstellung: Schwellenwert für verlustreiche Komprimierung

### Schwellenwert für verlustreiche Komprimierung

Hinweis: Bei Virtual Delivery Agent 7.x gilt diese Richtlinieneinstellung nur, wenn die Richtlinieneinstellung "Legacygrafikmodus"aktiviert ist.

Mit dieser Einstellung geben Sie die maximale Bandbreite in Kilobits pro Sekunde für eine Verbindung an, auf die die verlustreiche Komprimierung angewendet wird.

Der Standardschwellenwert ist 2147483647 Kilobits pro Sekunde.

Wenn Sie die Einstellung Grad der verlustreichen Komprimierung einer Richtlinie hinzufügen, ohne einen Schwellenwert anzugeben, kann sich dadurch die Anzeigegeschwindigkeit für detailreiche Bitmaps, wie Fotografien, über ein LAN verbessern.

Verwandte Richtlinieneinstellung: Grad der verlustreichen Komprimierung

## WebSockets - Richtlinieneinstellungen

June 27, 2024

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. Dabei werden nicht mehrere HTTP-Verbindungen geöffnet.

### 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>://:[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.*.*`).

## WIA-Geräte - Richtlinieneinstellungen

June 27, 2024

Der Abschnitt **WIA-Geräte** enthält Richtlinieneinstellungen für die Verwaltung der Scannerumleitung mithilfe der Windows-Bilderfassung (WIA).

### WIA-Umleitung

WIA-Geräte wie Digitalkameras und Scanner kommunizieren mithilfe des WIA-Frameworks mit servergehosteten Bildverarbeitungsanwendungen. Diese Einstellung ermöglicht oder verhindert, dass Benutzer auf WIA-Geräte auf dem Benutzergerät zugreifen. Standardmäßig ist die WIA-Umleitung nicht zugelassen.

Informationen zu WIA-kompatiblen Geräten finden Sie unter WIA-Geräte.

## Über die Registrierung verwaltete HDX-Features

June 27, 2024

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

Um den Registrierungs-Editor zu öffnen, führen Sie `regedit.exe` auf dem Server aus. Navigieren Sie dann zum Registrierungsschlüssel, um Einstellungen hinzuzufügen oder zu bearbeiten.

## Geräte

### Bloomberg-Tastaturen

Citrix Virtual Apps and Desktops unterstützt die Bloomberg-Tastatur (Starboard) der Modelle 4 und 3. Standardmäßig ist die Unterstützung für die erweiterte Bloomberg-Tastatur deaktiviert.

Um die Unterstützung für die Bloomberg-Tastatur zu aktivieren, legen Sie den folgenden Registrierungswert auf dem Client fest, bevor Sie eine Verbindung herstellen:

- **Schlüssel**:`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICAClient\GenericUSB`
- **Wertname**: `EnableBloombergHID`
- **Werttyp**: `DWORD`
- **Wertdaten**:
  - `0` - Deaktivieren
  - `1` - Aktivieren

Weitere Informationen finden Sie unter Konfigurieren von Bloomberg-Tastaturen.

### Zugeordnete Clientlaufwerke

Wenn sich ein Benutzer bei Citrix Virtual Apps and Desktops anmeldet, ordnet der Server aus Sicherheitsgründen standardmäßig Clientlaufwerke zu, ohne dass der Benutzer Ausführungsberechtigung hat. Sollen die Benutzer ausführbare Dateien auf zugeordneten Clientlaufwerken ausführen können, setzen Sie diese Standardeinstellung in der Registrierung auf dem Server außer Kraft.

Um den Zugriff zuzulassen, bearbeiten Sie den folgenden Registrierungswert (erstellen Sie **CDMSettings**, falls nicht vorhanden):

- **Schlüssel**:`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\CDMSettings`

- **Wertname**: `ExecuteFromMappedDrive`
- **Werttyp**: `DWORD`
- **Wertdaten**:
  - `1` - Berechtigung zulassen
  - `0` - Berechtigung für zugeordnete Laufwerke verweigern

Die Änderung wird für Sitzungen wirksam, die nach dem Bearbeiten der Registrierung verbunden werden.

Citrix Virtual Apps and Desktops 7 2006 ist die erste Version mit diesem Registrierungspfad. In früheren Versionen von Citrix Virtual Apps and Desktops wurde ein anderer Registrierungspfad verwendet.

Weitere Informationen finden Sie unter Clientlaufwerkzuordnung.

#### Microsoft Surface Pro und Surface Book-Stifte

Citrix Virtual Apps and Desktops unterstützt Standardstiftfunktionen bei Windows Ink-basierten Anwendungen. Standardmäßig ist dieses Feature aktiviert.

Um dieses Feature zu deaktivieren oder zu aktivieren, legen Sie folgenden Registrierungswert fest:

- **Schlüssel**:`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Citrix Virtual Desktop Agent\PenApi`
- **Wertname**: `DisablePen`
- **Werttyp**: `DWORD`
- **Wertdaten**:
  - `1` - Deaktivieren
  - `0` - Aktivieren

Weitere Informationen finden Sie unter Microsoft Surface Pro und Surface Book-Stifte.

#### Positivliste für WIA-Anwendungen

Mit dieser Einstellung können Sie festlegen, welche Anwendungen auf dem VDA Zugriff auf die WIA-Scannerumleitung erhalten.

Standardmäßig kann keine Anwendung auf die WIA-Schnittstelle zugreifen.

Um die Windows-Bilderfassung (WIA) für Anwendungen auf dem VDA anzupassen, erstellen Sie die folgende Registrierungseinstellung:

- **Schlüssel**:`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix`

- **Wertname**: `WIAAllowedProcesses`

  Wählen Sie **WIAAllowedProcesses** und klicken Sie mit der rechten Maustaste. Wählen Sie **Neu > Wert der mehrteiligen Zeichenfolge** und benennen Sie den neuen Wert in **AllowProcesses** um.

- Wertdaten: Geben Sie den vollständigen Pfad und den Prozessnamen für jede Anwendung ein, die auf die Windows-Bilderfassung (WIA) zugreifen darf. Jede Anwendung muss in einer neuen Zeile stehen.

Alle Änderungen an dieser Einstellung werden wirksam, wenn Sie das nächste Mal eine Sitzung auf dem VDA starten.

## Allgemein

### HDX Reducer

Sie können die Version des HDX-Komprimierungsalgorithmus (Reducer) konfigurieren, die Sie im Sitzungshost verwenden möchten.

Um Reducer V4 in einem Einzelsitzungs-VDA zu aktivieren, legen Sie den folgenden Registrierungswert fest:

**Schlüssel**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\GroupPolicy\Defaults\WDSettings`
**Wertname**: `ReducerOverrideMask`
**Werttyp**: `DWORD`
**Wertdaten**: 23 (Dezimal)

Um Reducer V4 in einem Multisitzungs-VDA zu aktivieren, legen Sie den folgenden Registrierungswert fest:

- **Schlüssel**:`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd`
- **Wertname**: `ReducerOverrideMask`
- **Werttyp**: `DWORD`
- **Wertdaten**: 23 (Dezimal)

### EDT-Timeout konfigurieren

Sie können das EDT-Timeout auf einen beliebigen Wert zwischen 5 und 25 Sekunden auf dem VDA konfigurieren. Der Standardwert für das EDT-Timeout beträgt 25 Sekunden.

- **Schlüssel**:HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd\Tds\udp\UDPStackParameters
- **Werttyp**: DWORD
- **Wertname**: edtConnectionTimeout
- **Wertdaten**: Zeit in Sekunden zwischen 5 und 25 (dezimal)

Sie können auch das Timeout für die Citrix Workspace-App für Windows konfigurieren:

- **Schlüssel**:HKLM\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\EDT
- **Werttyp**: String / REG_SZ
- **Wertname**: edtConnectionTimeout
- **Wertdaten**: Zeit in Sekunden zwischen 5 und 25 (dezimal)

#### Rendezvous-Version konfigurieren

Legen Sie den folgenden Registrierungswert fest, um die zu verwendende Version von Rendezvous zu konfigurieren:

- **Schlüssel**:HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent
- **Werttyp**: DWORD
- **Wertname**: GctRegistration
- **Wertdaten**:
  - 1 - Um V2 zu aktivieren
  - 0 - Um V1 zu aktivieren

#### Konfigurieren der automatischen Anmeldung am VDA

Mit dieser Einstellung können Sie die Microsoft-Richtlinieneinstellung **Kennwort immer anfordern** auf Windows 10-VDAs mit Einzel- bzw. Multisitzungs-OS aktivieren oder deaktivieren.

Wenn die Einstellung **Kennwort immer anfordern** aktiviert ist, müssen Benutzer bei jedem Start einer Remotesitzung ihre Anmeldeinformationen auf dem VDA eingeben. Wenn die Einstellung deaktiviert ist, stellen Benutzer automatisch eine Verbindung zur Remotesitzung her, ohne ihre Anmeldeinformationen auf dem VDA einzugeben.

Standardmäßig ist die Microsoft-Richtlinieneinstellung deaktiviert. Um die Einstellung **Kennwort immer anfordern** zu aktivieren bzw. deaktivieren, legen Sie den folgenden Registrierungswert auf dem VDA fest:

- **Schlüssel**:HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Portica

- **Wertname**: `AutoLogon`
- **Werttyp**: `DWORD`
- **Wertdaten**:
  - `1` –Deaktiviert die Microsoft-Richtlinieneinstellung und ermöglicht Benutzern die automatische Anmeldung bei einer Remotesitzung.
  - `0` —Aktiviert die Microsoft-Richtlinieneinstellung und fordert Benutzer auf, beim Start einer Remotesitzung ihre Anmeldeinformationen einzugeben.

#### Timeoutwarnung deaktivieren

Bei inaktiven Sitzungen erhalten Benutzer standardmäßig zwei Minuten vor der automatischen Trennung der Sitzung eine Warnmeldung.

Diese Einstellung deaktiviert und entfernt die Warnmeldung zur Trennung inaktiver Sitzungen auf:

- Windows Server 2004
- Windows 10 Multisitzungs-OS 2004 oder späteres Multisitzungs-OS

Um die Warnung zu entfernen, legen Sie den folgenden Registrierungswert auf dem VDA fest:

- **Schlüssel**:`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Winstations\ICA-CGP`
- **Wertname**: `fEnableTimeoutWarning`
- **Werttyp**: `DWORD`
- **Wertdaten**:
  - `1` – Deaktivieren der Warnmeldung
  - `0` – Aktivieren der Warnmeldung

Um die Warnmeldung anzuzeigen, löschen Sie den Registrierungswert oder legen ihn auf `0` fest.

#### 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.

Diese Einstellung ist standardmäßig aktiviert. Zum Deaktivieren der MTU-Discovery durch EDT konfigurieren Sie den folgenden Registrierungswert und starten Sie den VDA neu.

- **Schlüssel**:`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd`
- **Wertname**: `MtuDiscovery`

- **Werttyp**: DWORD
- **Wertdaten**: 0

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

#### Verlusttoleranzmodus aktivieren

Sie können auf adaptives Audio mit dem Verlusttoleranzmodus für den bidirektionalen Audiodienst für die Citrix Workspace-App für Windows, Mehrbenutzer-VDA und Desktop-VDA zugreifen. Diese Einstellung ist standardmäßig deaktiviert. Um den Verlusttoleranzmodus zu aktivieren, konfigurieren Sie je nach verwendeter Maschine den folgenden Registrierungswert und starten Sie die Maschine dann neu.

Client mit Citrix Workspace-App für Windows

- **Schlüssel**:HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio
- **Wertname**: EdtUnreliableAllowed
- **Werttyp**: REG_SZ
- **Wertdaten**: 1

TS-VDA

- **Schlüssel**:HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Audio
- **Wertname**: EdtUnreliableAllowed
- **Werttyp**: DWORD
- **Wertdaten**: 1

WS-VDA

- **Schlüssel**:HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Audio
- **Wertname**: EdtUnreliableAllowed
- **Werttyp**: DWORD
- **Wertdaten**: 1

### Allgemeine Inhaltsumleitung

#### Hinzufügen von URL-Typen für die Host-zu-Client-Umleitung

Standardmäßig unterstützen wir die Umleitung der folgenden URL-Typen: HTTP, HTTPS, RTSP, RTSPU, PNM und MMS. Sie können der Liste URL-Typen hinzufügen, indem Sie den folgenden Registrierungsschlüssel mit den folgenden Werten auf dem Windows-Client erstellen.

- **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 diese Registrierungseinstellung 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.

Weitere Informationen finden Sie unter Host-zu-Client-Umleitung.

#### Clientordner umleiten

Durch die Clientordnerumleitung ändert sich der Zugriff auf clientseitige Dateien bei der hostseitigen Sitzung. Berücksichtigen Sie, dass Sie die Clientordnerumleitung auf dem Server aktivieren und der Benutzer sie auf dem Benutzergerät konfiguriert. In diesem Fall wird der vom Benutzer angegebene Teil des lokalen Volumes umgeleitet.

Um die Clientordnerumleitung auf dem Server zu aktivieren, legen Sie den folgenden Registrierungswert fest:

- **Schlüssel**:HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Client Folder Redirection
- **Wertname**: CFROnlyModeAvailable
- **Werttyp**: DWORD
- **Wertdaten**: 1

Weitere Informationen finden Sie unter Clientordnerumleitung.

#### Host-zu-Client-Umleitung für spezifische Websites

Zum Aktivieren der Host-zu-Client-Umleitung für spezifische Websites legen Sie den folgenden Registrierungswert auf dem Server-VDA fest:

- **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.example.com`

`*.example.com`

Weitere Informationen finden Sie unter Host-zu-Client-Umleitung.

#### Verhalten lokaler Anwendungen beim Abmelden und Trennen

Standardmäßig werden lokale Anwendungen weiterhin 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. Um das Verhalten lokaler Anwendungen beim Abmelden und Trennen zu konfigurieren, legen Sie den folgenden Registrierungswert auf dem gehosteten Desktop fest:

- **Schlüssel**:`HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Citrix\Client Hosted Apps\Policies`
- **Wertname**: `Session State`
- **Werttyp**: `DWORD`
- **Wertdaten**:
  - `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.

Weitere Informationen finden Sie unter Lokaler App-Zugriff und URL-Umleitung.

#### Entfernen von URL-Typen aus der Standardliste für die Host-zu-Client-Umleitung

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: `http`, `https`, `rtsp`, `rtspu`, `pnm` oder `mms`. Geben Sie mehrere Werte auf separaten Zeilen an. Beispiel:

```
http
https
rtsp
```

Weitere Informationen finden Sie unter Host-zu-Client-Umleitung.

#### Standardbrowserkonfiguration auf dem Server-VDA

Sie können die Host-zu-Client-Umleitung aktivieren, um jede Standardbrowserkonfiguration auf dem Server-VDA zu ersetzen. 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.

- Internet Explorer (Standard)
  - **Schlüssel**:`HKEY_CLASSES_ROOT\http\shell\open\command_backup`
  - **Wertname**: `Default`
  - **Werttyp**: `REG_SZ`
  - **Wertdaten**: `"c:\program files\internet explorer\iexplore.exe""%1"`
  - **Schlüssel**:`HKEY_CLASSES_ROOT\https\shell\open\command_backup`
  - **Wertname**: `Default`
  - **Werttyp**: `REG_SZ`
  - **Wertdaten**: `"c:\program files\internet explorer\iexplore.exe""%1"`
- Google Chrome
  - **Schlüssel**:`HKEY_CLASSES_ROOT\http\shell\open\command_backup`
  - **Wertname**: `Default`
  - **Werttyp**: `REG_SZ`

  - **Wertdaten**: `"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe""%1"`
  - **Schlüssel**:`HKEY_CLASSES_ROOT\https\shell\open\command_backup`
  - **Wertname**: `Default`
  - **Werttyp**: `REG_SZ`
  - **Wertdaten**: `"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe""%1"`

- Microsoft Edge
  - **Schlüssel**:`HKEY_CLASSES_ROOT\http\shell\open\command_backup`
  - **Wertname**: `Default`
  - **Werttyp**: `REG_SZ`
  - **Wertdaten**: `"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe""%1"`
  - **Schlüssel**:`HKEY_CLASSES_ROOT\https\shell\open\command_backup`
  - **Wertname**: `Default`
  - **Werttyp**: `REG_SZ`
  - **Wertdaten**: `"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe""%1"`

#### Lokaler App-Zugriff für veröffentlichte Anwendungen

Durch lokalen App-Zugriff werden lokal installierte Windows-Anwendungen problemlos in eine gehostete Desktopumgebung integriert, ohne dass ein Wechsel zwischen Desktops nötig ist. Um den Zugriff auf veröffentlichte Anwendungen zu ermöglichen, legen Sie den folgenden Registrierungswert auf dem Server fest:

- **Schlüssel**:`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\DesktopStudio`
- **Wertname**: `ClientHostedAppsEnabled`
- **Werttyp**: `DWORD`
- **Wertdaten**:
  - `1` - Aktivieren
  - `0` - Deaktivieren

Weitere Informationen finden Sie unter Lokaler App-Zugriff und URL-Umleitung.

## Grafik

### 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 folgende Registrierungseinstellung, um die im Rahmen der Machbarkeitsstudie verfügbaren CUDA-Beschleunigungsfeatures zu verwenden:

- **Schlüssel**:`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper`
- **Wertname**: `CUDA`
- **Werttyp**: `DWORD`
- **Wertdaten**: `00000001`

Aktivieren Sie die folgende Registrierungseinstellung, um die im Rahmen der Machbarkeitsstudie verfügbaren OpenCL-Beschleunigungsfeatures zu verwenden:

- **Schlüssel**:`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper`
- **Wertname**: `OpenCL`
- **Werttyp**: `DWORD`
- **Wertdaten**: `00000001`

Weitere Informationen finden Sie unter GPU-Beschleunigung für Windows-Multisitzungs-OS.

### Progressiver Modus

Der progressive Modus ist standardmäßig deaktiviert. Sie können den Zustand des progressiven Modus über folgenden Registrierungswert ändern:

- **Schlüssel**:`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics`
- **Werttyp**: `REG_DWORD`
- **Wertname**: `ProgressiveDisplay`
- **Wertdaten**:
  - `0` – Immer aus (Progressiver Modus deaktiviert. Dies ist der Standardwert.)
  - `1` – Automatisch (Umschaltung basierend auf Netzwerkbedingungen)
  - 2 = Immer aktiviert

Weitere Informationen finden Sie unter Progressive Anzeige mit Thinwire.

> **Hinweis:**
>
> Der progressive Modus ist veraltet. Thinwire ist eine alternative Option, die die Bildübertragung optimiert, die Cache-Effizienz beibehält und gleichzeitig fast alle Vorteile des progressiven Modus bietet.

#### Rendering mit Windows Presentation Foundation (WPF)

Mit HDX 3D Pro können grafikintensive Anwendungen, die in Sitzungen mit Windows-Multisitzungs-OS ausgeführt werden, auf der GPU des Servers gerendert werden. Wenn Sie das Rendering mit Windows Presentation Foundation (WPF) auf die GPU des Servers verlagern, wird diese nicht durch das Grafikrendering verlangsamt.

Um das Rendering von WPF-Anwendungen mit der GPU des Servers zu aktivieren, erstellen Sie die folgende Einstellung in der Registrierung des Servers, der die Sitzungen mit Windows-Multisitzungs-OS ausführt:

1. Öffnen Sie auf dem VDA den Registrierungs-Editor und navigieren Sie zum folgenden Schlüssel:

   `HKLM\Software\Citrix\CtxHook\AppInit_DLLs\Graphics Helper`

2. Erstellen oder bearbeiten Sie die folgenden Registrierungswerte:

   - [REG_DWORD] AdapterHandle = 0x00000001
   - [REG_DWORD] DevicePath = 0x00000001
   - [REG_DWORD] Flag = 0x00000412
   - [REG_DWORD] WPF = 0x00000001

3. Erstellen Sie einen Unterschlüssel, der den Namen der ausführbaren Datei Ihrer WPF-App enthält. Wenn Ihre App beispielsweise “mywpfapp.exe”heißt, erstellen Sie folgenden Schlüssel:

   `HKLM\Software\Citrix\CtxHook\AppInit_DLLs\Graphics Helper\mywpfapp.exe`

4. Starten Sie den Server neu, damit die Einstellung wirksam wird.

Weitere Informationen finden Sie unter GPU-Beschleunigung für Windows-Multisitzungs-OS und im Blog Getting the best out of WPF apps on Windows multi-session OS.

### Multimedia

#### Echo in Multimediakonferenzen vermeiden

Citrix Virtual Apps and Desktops bietet eine Option zur Echounterdrückung, die jedes Echo minimiert. Dieses Feature ist standardmäßig aktiviert. Um die Echounterdrückung zu deaktivieren, können Sie eine der folgenden Registrierungseinstellungen ändern:

- **Schlüssel**:
  - 32 Bit: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio`
  - 64 Bit: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio`
- **Wertname**: `EchoCancellation`
- **Werttyp**: `String`/`REG_SZ`
- **Wertdaten**: `False`

Weitere Informationen finden Sie unter Audiofeatures.

#### Audio-Einschränkung

Nachdem Sie ein Audiogerät auf Ihrem Client installiert, die Audioumleitung aktiviert und eine RDS-Sitzung gestartet haben, schlägt die Wiedergabe von Audiodateien möglicherweise fehl. Fügen Sie als Workaround den folgenden Registrierungsschlüssel auf der RDS-Maschine hinzu und starten Sie diese anschließend neu:

- **Schlüssel**:`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SCMConfig`
- **Wertname**: `EnableSvchostMitigationPolicy`
- **Werttyp**: `DWORD`
- **Wertdaten**: `0`

Weitere Informationen finden Sie unter Audiofeatures.

#### Umleitung des Browserinhalts und DPI

Bei Verwendung der Browserinhaltsumleitung mit einer DPI-Skalierung von mehr als 100 % auf der Maschine des Benutzers wird der umgeleitete Browserinhalt fehlerhaft angezeigt. Um das Problem zu vermeiden, deaktivieren Sie die GPU-Beschleunigung der Browserinhaltsumleitung für Chrome, indem Sie den folgenden Registrierungswert auf der Maschine des Benutzers erstellen:

- **Schlüssel**:`HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\HdxMediaStream`
- **Wertname**: `GPU`
- **Werttyp**: `DWORD`
- **Wertdaten**: `0`

Weitere Informationen finden Sie unter Umleitung des Browserinhalts und DPI.

#### HD-Webcamauflösung

Wenn die Medientypaushandlung fehlschlägt, verwendet HDX die VGA-Standardauflösung (640 x 480 Pixel). Anhand der Registrierungsschlüssel auf dem Client können Sie die Standardauflösung konfigurieren. Stellen Sie vor dem Festlegen der folgenden Registrierungsschlüssel sicher, dass die Kamera die angegebene Auflösung unterstützt.

- **Schlüssel**:`HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXRealTime`
- Breite
  - **Wertname**: `DefaultWidth`
  - **Werttyp**: `DWORD`
  - **Wertdaten**: Gewünschte Breite als Dezimalzahl (zum Beispiel 1280)
- Höhe
  - **Wertname**: `DefaultHeight`
  - **Werttyp**: `DWORD`
  - **Wertdaten**: Gewünschte Höhe als Dezimalzahl (zum Beispiel 720)

#### Fallbackmodus für Microsoft Teams

Wenn Microsoft Teams nicht im optimierten VDI-Modus geladen werden kann (“Citrix HDX Not Connected”in Teams/Info/Version), fällt der VDA auf ältere HDX-Technologien wie Webcamumleitung und Clientaudio/-mikrofonumleitung zurück. Wenn Ihre Workspace-App- oder Plattform-OS-Version die Microsoft Teams-Optimierung nicht unterstützt, werden Fallback-Registrierungsschlüssel nicht angewendet.

Um den Fallbackmechanismus zu steuern, legen Sie einen der folgenden Registrierungswerte auf dem VDA fest:

- **Schlüssel** (nur ein Schlüssel erforderlich):
  - **Computereinstellung:** `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Teams`
  - **Benutzereinstellung:** `HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Teams`
- **Wertname**: `DisableFallback`
- **Werttyp**: `DWORD`
- Wertdaten:
  - 1 – Fallback-Modus deaktivieren
  - 2 – Nur Audio aktivieren

Wenn der Wert nicht vorhanden oder auf 0 gesetzt ist, wird der Fallbackmodus aktiviert. Für dieses Feature ist die Microsoft Teams-Version 1.3.0.13565 oder höher erforderlich. Weitere Informationen finden Sie unter Optimierung für Microsoft Teams.

#### Optimierung für Microsoft Teams mit Citrix App Layering

Wenn Sie Citrix App Layering zum Verwalten von VDA- und Microsoft Teams-Installationen auf verschiedenen Layern verwenden, müssen Sie einen neuen Registrierungsschlüssel **PortICA** in Windows erstellen, bevor Sie Microsoft Teams mit dem Flag `ALLUSER=1` über die Befehlszeile installieren. Behalten Sie den Standardwertnamen, den Typ und die Wert bei.

- Schlüssel für die 32-Bit-Version des Registrierungs-Editors: `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\PortICA`
- Schlüssel für die 64-Bit-Version des Registrierungs-Editors: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

Weitere Informationen finden Sie unter Optimierung für Microsoft Teams.

#### Single Sign-On mit integrierter Windows-Authentifizierung für die Browserinhaltsumleitung

Diese Einstellung bietet Single Sign-On bei einem Webserver, der mit der integrierten Windows-Authentifizierung (IWA) in derselben Domäne wie der VDA konfiguriert ist. Um Single Sign-On zu aktivieren, legen Sie den folgenden Registrierungswert auf 1 fest:

- **Schlüssel**:
  - `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediastream`

  oder
  - `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\HdxMediastream`
- **Wertname**: `WebBrowserRedirectionIwaSupport`
- **Werttyp**: `DWORD`
- **Wertdaten**: `1`

Weitere Informationen finden Sie unter Single Sign-On mit integrierter Windows-Authentifizierung.

#### User-Agent-Anforderungsheader

Der User-Agent-Header hilft bei der Identifizierung von HTTP-Anforderungen, die von der Browserinhaltsumleitung gesendet werden. Diese Einstellung kann beim Konfigurieren von Proxy- und Firewall-

regeln nützlich sein. Wenn der Server beispielsweise von der Browserinhaltsumleitung gesendete Anforderungen blockiert, können Sie eine Regel mit dem User-Agent-Header zum Umgehen bestimmter Anforderungen erstellen. Nur Windows-Geräte unterstützen den User-Agent-Anforderungsheader.

Standardmäßig ist die Zeichenfolge des User-Agent-Anforderungsheaders deaktiviert. Zum Aktivieren des User-Agent-Headers für vom Client gerenderte Inhalte verwenden Sie den Registrierungs-Editor.

Legen Sie auf jedem Client mit Citrix Workspace-App für Windows eine der folgenden Registrierungseinstellungen fest:

- **Schlüssel**:
  - 32 Bit: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStream`
  - 64 Bit: `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\HdxMediaStream`

- **Wertname**: `EnableCefUserAgentString`
- **Werttyp**: `DWORD`
- **Wertdaten**: 1

Nachdem Sie den Registrierungswert hinzugefügt haben, enthält der User-Agent-Header den Text CitrixBCR/2102.1, wobei 2102.1 die Version der Citrix Workspace-App für Windows ist.

#### Webcamsoftwarekomprimierung

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 die folgenden Werte auf dem Client hinzu:

- **Schlüssel**:`HKEY_CURRENT_USER\SOFTWARE\Citrix\HdxRealTime`
- **Wertname**: `DeepCompress_ForceSWEncode`
- **Werttyp**: `DWORD`
- **Wertdaten**: 1

Weitere Informationen finden Sie unter HDX-Webcamvideokomprimierung.

#### Webcamvideokomprimierung

Bei der HDX-Webcamvideokomprimierung wird das H.264-Video direkt an die Videokonferenzanwendung gesendet, die in der virtuellen Sitzung ausgeführt wird. Zum Optimieren von VDA-Ressourcen wird das Webcamvideo von der HDX-Webcamkomprimierung nicht codiert, transcodiert und decodiert. Dieses Feature ist standardmäßig aktiviert.

Um das direkte Videostreaming vom Server zur Videokonferenz-App zu deaktivieren, legen Sie den folgenden Registrierungswert im VDA fest.

- **Schlüssel**:`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxRealTime`
- **Wertname**: `OfferH264ToApp`
- **Werttyp**: `DWORD`
- **Wertdaten**: `0`

Weitere Informationen finden Sie unter HDX-Webcamvideokomprimierung.

#### Framerate der Webcamvideokomprimierung

Um die Framerate anzupassen, bearbeiten Sie den folgenden Registrierungswert auf dem Client:

- **Schlüssel**:`HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXRealTime`
- **Wertname**: `FramesPerSecond`
- **Werttyp**: `DWORD`
- **Wertdaten**: `15`

Wenn die Webcam die angegebene Framerate nicht unterstützt, verwendet die Anwendung standardmäßig 15 FPS.

Weitere Informationen finden Sie unter HDX-Webcamvideokomprimierung.

## Lastverwaltung - Richtlinieneinstellungen

June 27, 2024

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-Auslastung 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-Auslastung wird bei der Lastberechnung nicht berücksichtigt.

### CPU-Auslastung ausschließlich Prozesspriorität

> **Hinweis:**
>
> Wenn Maschinen von Workspace Environment Management verwaltet werden, kann die Verwendung dieser Einstellung zusammen mit den CPU Priority-Einstellungen unbeabsichtigte Ergebnisse liefern. Wir empfehlen, diese Einstellung zu deaktivieren, wenn Sie die CPU-Prioritätseinstellungen verwenden.

Mit dieser Einstellung geben Sie die Prioritätsstufe an, bei der die Prozess-CPU-Auslastung vom Lastindex der CPU-Auslastung 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

Diese Einstellung gibt die ungefähre Ausgangslast der Speichernutzung des Betriebssystems an. Sie definiert außerdem die Speichernutzung in MB, unterhalb derer für einen Server eine Nulllast gilt.

Standardmäßig sind dies 768 MB.

## Einstellungen der Richtlinie "Profilverwaltung"

June 27, 2024

Dieser Abschnitt enthält Richtlinieneinstellungen zum Aktivieren und Konfigurieren der Profilverwaltung.

Andere Informationen wie etwa die nachfolgend aufgeführten finden Sie unter Profilverwaltungsrichtlinien:

- Namen der entsprechenden INI-Dateieinstellung
- Für eine Richtlinieneinstellung erforderliche Version der Profilverwaltung

## Erweiterte Richtlinieneinstellungen

June 27, 2024

### 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 `Index.dat` gibt. Nach längerem Browsen im Internet können diese zusätzlichen Cookies das Profil aufblähen. Mit dieser Richtlinie können Sie die Verarbeitung von Index.dat durch die Profilverwaltung erzwingen und die zusätzlichen Cookies entfernen. Die Richtlinie verlangsamt die Abmeldung. 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.

Diese Richtlinie beschleunigt die Bereitstellung und vereinfacht die Optimierung. Sie müssen die Richtlinie nicht konfigurieren. Sie können die automatische Konfiguration jedoch deaktivieren, wenn Sie einen der folgenden Schritte ausführen:

- Upgrade zum Beibehalten der Einstellungen aus früheren Versionen
- Problembehandlung

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 | In folgenden Situationen *deaktiviert*: Personal vDisk wird verwendet, Citrix Virtual Desktops werden zugewiesen oder Citrix Virtual Desktops sind nicht installiert. 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**.

> **Wichtig:**
>
> Persönliche vDisk ist veraltet. Weitere Informationen finden Sie unter Entfernen von persön-

> lichen vDisks, AppDisks und nicht unterstützten Hosts.

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:

- Fügen Sie `Appdata\Local\Microsoft\Windows\Caches` und `Appdata\Local\Packages` unter **Zu spiegelnde Ordner** hinzu.
- Fügen Sie `Appdata\Local\Microsoft\Windows\UsrClass.Dat*` unter **Zu synchronisierende Dateien** hinzu.

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. In diesem Fall ändern sich möglicherweise die Einstellungen der Profilverwaltung, wenn sich die Umgebung ändert.

### Benutzer bei Problem abmelden

Hiermit können Sie festlegen, ob Benutzer abgemeldet werden, wenn ein Problem auftritt.

Wenn diese Richtlinie deaktiviert oder nicht konfiguriert ist, wird Benutzern von der Profilverwaltung ein temporäres Profil zugewiesen, wenn ein Problem auftritt. Beispielsweise ist der Benutzerspeicher 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 Nutzungsdaten gesammelt 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. Dieses Feature erfordert zusätzlichen Speicherplatz im Benutzerspeicher, um Suchindexe für Outlook zu speichern.

Melden Sie sich ab und wieder an, damit diese Richtlinie wirksam wird.

### Outlook-Suchindexdatenbank - Backup und Wiederherstellen

Hiermit können Sie festlegen, was bei der Anmeldung geschieht, wenn die Richtlinie "Suchindex-Roaming für Outlook aktivieren"aktiviert ist.

Wenn diese Richtlinie 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 die Suchindexdatenbank aufgrund einer Beschädigung nicht bereitgestellt werden kann, wird die Datenbank 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 den verfügbaren VHDX-Speicher.

#### Unterstützung gleichzeitiger Sitzungen für das Roaming des Outlook-Suchindex aktivieren

Ermöglicht der Profilverwaltung, native Outlook-Suche in gleichzeitigen Sitzungen desselben Benutzers zu bieten. Verwenden Sie diese Richtlinie zusammen mit der Richtlinie "Suchindex-Roaming für Outlook".

Wenn diese Richtlinie aktiviert ist, verwendet jede gleichzeitige Sitzung eine separate Outlook-OST-Datei.

Standardmäßig können nur zwei VHDX-Datenträger zum Speichern von Outlook-OST-Dateien verwendet werden (eine Datei pro Datenträger). Wenn der Benutzer mehrere Sitzungen startet, werden seine Outlook-OST-Dateien im lokalen Benutzerprofil gespeichert. Sie können die maximale Anzahl von VHDX-Datenträgern zum Speichern von Outlook-OST-Dateien angeben.

#### OneDrive-Container aktivieren

Ermöglicht Benutzern das Roaming von OneDrive-Ordnern.

Der OneDrive-Container ist eine VHDX-basierte Lösung für das Roaming von Ordnern. Die Profilverwaltung erstellt eine VHDX-Datei pro Benutzer in einer Dateifreigabe und speichert die OneDrive-Ordner

der Benutzer in den VHDX-Dateien. Die VHDX-Dateien werden angehängt, wenn sich Benutzer anmelden, und getrennt, wenn sich Benutzer abmelden.

### Roaming von UWP-Apps

Ermöglicht das Aktivieren des Roamings von Universal Windows Platform-Apps mit den Benutzern. Dadurch können die Benutzer von verschiedenen Geräten aus auf dieselben UWP-Apps zugreifen.

Wenn diese Richtlinie aktiviert ist, ermöglicht die Profilverwaltung das Roaming von UWP-Apps mit Benutzern durch die Speicherung der Apps auf separaten VHDX-Datenträgern. Diese Datenträger werden bei Benutzeranmeldungen angefügt und bei Benutzerabmeldungen getrennt.

Konfigurationsrangfolge:

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der .ini-Datei verwendet.
Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, wird das Feature deaktiviert.

#### Asynchrone Verarbeitung für Benutzergruppenrichtlinien bei Anmeldung aktivieren

Windows bietet zwei Verarbeitungsmodi für Benutzergruppenrichtlinien: synchron und asynchron. Windows verwendet einen Registrierungswert, um den Verarbeitungsmodus für die nächste Benutzeranmeldung zu bestimmen. Wenn der Registrierungswert nicht vorhanden ist, wird der synchrone Modus angewendet. Der Registrierungswert ist eine Einstellung auf Maschinenebene und es erfolgt kein Roaming mit Benutzern. Daher wird der asynchrone Modus in folgenden Fällen nicht wie erwartet angewendet:

- Wenn Benutzer sich an verschiedenen Maschinen anmelden.
- Wenn Benutzer sich an der Maschine anmelden, auf der die Richtlinie "Lokal zwischengespeicherte Profile nach Abmeldung löschen"aktiviert ist.

Wenn diese Richtlinie aktiviert ist, erfolgt das Roaming des Registrierungswerts mit Benutzern. Daher wird der Verarbeitungsmodus jedes Mal angewendet, wenn sich Benutzer anmelden.

#### Anteil freier Speicherplatz zum Auslösen der VHD-Datenträgerkomprimierung

Gilt, wenn VHD-Datenträgerkomprimierung aktivieren aktiviert ist. Hier können Sie den Anteil des freien Speicherplatzes zum Auslösen der VHD-Datenträgerkomprimierung angeben. Wenn die Quote des freien Speicherplatzes bei der Benutzerabmeldung den angegebenen Wert überschreitet, wird die Datenträgerkomprimierung ausgelöst.

Quote des freien Speicherplatzes = (aktuelle VHD-Dateigröße - Mindestgröße der VHD-Datei*) ÷ aktuelle VHD-Dateigröße

* Wird mit der GetSupportedSize-Methode der Klasse `MSFT_Partition` vom Microsoft Windows-Betriebssystem ermittelt.

#### Anzahl der Abmeldungen zum Auslösen der VHD-Datenträgerkomprimierung

Gilt, wenn VHD-Datenträgerkomprimierung aktivieren aktiviert ist. Sie können die Anzahl der Benutzerabmeldungen für das Auslösen der VHD-Datenträgerkomprimierung angeben.

Wenn die Anzahl der Abmeldungen seit der letzten Komprimierung den angegebenen Wert erreicht, wird die Datenträgerkomprimierung erneut ausgelöst.

#### Defragmentierung für VHD-Datenträgerkomprimierung deaktivieren

Gilt, wenn VHD-Datenträgerkomprimierung aktivieren aktiviert ist. Hier können Sie angeben, ob die Dateidefragmentierung für die VHD-Datenträgerkomprimierung deaktiviert werden soll.

Wenn die VHD-Datenträgerkomprimierung aktiviert ist, wird die VHD-Datenträgerdatei zuerst mit dem integrierten Windows-Tool `defrag` defragmentiert und anschließend komprimiert. Die Defragmentierung von VHD-Datenträgern führt zu einer besseren Komprimierung. Ihre Deaktivierung kann jedoch Systemressourcen einsparen.

### Multisitzungszurückschreiben für Profilcontainer aktivieren

Aktiviert das Zurückschreiben für Profilcontainer in Szenarios mit mehreren Sitzungen. Wenn diese Option aktiviert ist, werden Änderungen in allen Sitzungen in Profilcontainer zurückgeschrieben. Andernfalls werden nur Änderungen in der ersten Sitzung gespeichert, da nur die erste Sitzung im Lese-/Schreibmodus in Profilcontainern ist. Profilcontainer der Citrix Profilverwaltung werden ab Citrix Profilverwaltung 2103 unterstützt. FSLogix Profile Container wird ab Citrix Profilverwaltung 2003 unterstützt.

Um diese Richtlinie für den FSLogix-Profilcontainer zu verwenden, müssen folgende Voraussetzungen erfüllt sein:

- Das Feature “FSLogix Profile Container”ist installiert und aktiviert.
- In FSLogix ist der Profiltyp auf **Try for read-write profile and fallback to read-only** festgelegt.

### Benutzerspeicher replizieren

Hiermit können Sie den Remote-Benutzerprofilspeicher bei jeder An- und Abmeldung in mehrere Pfade replizieren. Dadurch kann die Profilverwaltung Profilredundanz für Benutzeranmeldungen bereitstellen.

Das Aktivieren der Richtlinie erhöht die System-E/A und verlängert u. U. das Abmelden.

> **Hinweis:**
>
> - Dieses Feature ist sowohl für den Benutzerspeicher als auch für den Container mit Gesamtprofil verfügbar.
> - Replizierte Profilcontainer bieten Profilredundanz für Benutzeranmeldungen, jedoch nicht für Failover während der Sitzung.

### Zugriff auf Benutzerspeicher mit Anmeldeinformationen aktivieren

Standardmäßig gibt sich die Citrix Profilverwaltung als aktueller Benutzer aus, um auf den Benutzerspeicher zuzugreifen. Aktivieren Sie dieses Feature, wenn sich die Profilverwaltung beim Zugriff auf den Benutzerspeicher nicht als aktueller Benutzer ausgeben soll. Sie können Benutzerspeicher in Speicherrepositorys (z. B. Azure Files) ablegen, auf die der aktuelle Benutzer keinen Zugriff hat.

Um sicherzustellen, dass die Profilverwaltung auf Benutzerspeicher zugreifen kann, speichern Sie die Anmeldeinformationen für den Profilspeicherserver in Workspace Environment Management (WEM) oder in der Windows-Anmeldeinformationsverwaltung. Es wird empfohlen, Workspace Environment Management zu verwenden, da Sie sonst für jede Maschine, auf der die Profilverwaltung ausgeführt wird, dieselben Anmeldeinformationen konfigurieren müssen. Wenn Sie die Windows-Anmeldeinformationsverwaltung verwenden, sollten Sie die Anmeldeinformationen im lokalen Systemkonto sicher speichern.

> **Hinweis:**
>
> Diese Richtlinie ist sowohl für dateibasierte als auch für VHDX-basierte Benutzerspeicher verfügbar. Für Profilverwaltungsversionen vor 2212 ist diese Richtlinie nur für VHDX-basierte Benutzerspeicher verfügbar.

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 sie standardmäßig deaktiviert.

### Speicherpfad für VHDX-Dateien anpassen

Die Profilverwaltung bietet die folgenden VHDX-basierten Richtlinien: Profilcontainer, Suchindex-Roaming für Outlook und Beschleunigtes Spiegeln von Ordnern. Standardmäßig werden VHDX-Dateien im Benutzerspeicher gespeichert. Mit dieser Richtlinie können Sie einen anderen Pfad zum Speichern angeben.

### Standardkapazität von VHD-Containern

Ermöglicht die Angabe der Standardspeicherkapazität (in GB) von VHD-Containern.

Konfigurationsrangfolge:

1. Wenn diese Richtlinie hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.
2. Wenn diese Richtlinie weder hier noch in der INI-Datei konfiguriert ist, wird der Standardwert (50 GB) verwendet.

### VHDX-Datenträger in Sitzungen automatisch wieder anfügen

Wenn diese Richtlinie aktiviert ist, bietet die Profilverwaltung ein hohes Maß an Stabilität der VHDX-basierten Richtlinien. Standardmäßig ist diese Richtlinie aktiviert.

Wenn diese Richtlinie aktiviert ist, überwacht die Profilverwaltung VHDX-Datenträger, die von VHDX-basierten Richtlinien verwendet werden. Wenn einer der Datenträger getrennt wird, bindet die Profilverwaltung den Datenträger automatisch wieder ein.

### Schwellenwert für die automatische Erweiterung von Profilcontainern

Ermöglicht die Angabe der Speicherbelegung, bei deren Erreichen die automatische Profilcontainererweiterung ausgelöst wird.

Konfigurationsrangfolge:

- 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 90 % verwendet.

### Inkrement für die automatische Erweiterung von Profilcontainern

Ermöglicht die Angabe der Speichermenge in GB, um die Profilcontainer automatisch erweitert werden.

Konfigurationsrangfolge:

- 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 (10 GB) verwendet.

### Grenzwert für die automatische Erweiterung von Profilcontainern

Ermöglicht die Angabe der maximalen Speicherkapazität in GB, bis zu der Profilcontainer automatisch erweitert werden können.

Konfigurationsrangfolge:

- 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 (80 GB) verwendet.

### Richtlinieneinstellungen auf Benutzerebene aktivieren

Wenn diese Richtlinie aktiviert ist, können Richtlinieneinstellungen auf Maschinenebene auf der Benutzerebene funktionieren und Einstellungen auf Benutzerebene setzen Einstellungen auf Maschinenebene außer Kraft.

Konfigurationsrangfolge:

1. Wenn diese Richtlinie hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.
2. Wenn diese Richtlinie weder hier noch in der INI-Datei konfiguriert ist, ist sie deaktiviert.

### Prioritätsreihenfolge für Benutzergruppen festlegen

Damit legen Sie die Prioritätsreihenfolge für Benutzergruppen fest. Die Reihenfolge bestimmt, welche Gruppe Vorrang hat, wenn ein Benutzer mehreren Gruppen mit unterschiedlichen Richtlinieneinstellungen angehört.

Wenn ein Benutzer mehreren Gruppen mit widersprüchlichen Richtlinieneinstellungen angehört, sollten Sie Folgendes beachten:

- Wenn der Benutzer einer oder mehreren in dieser Richtlinie definierten Gruppen angehört, hat die Gruppe mit der höchsten Priorität Vorrang.
- Wenn der Benutzer keiner der in dieser Richtlinie definierten Gruppen angehört, hat die Gruppe Vorrang, deren SID alphabetisch an erster Stelle steht.

### Auswahlmethode für den Benutzerspeicher

Wenn mehrere Benutzerspeicher verfügbar sind, kann damit die Methode für die Auswahl festgelegt werden. Die folgenden Optionen sind verfügbar:

- **Reihenfolge der Konfiguration.** Die Profilverwaltung wählt den frühesten konfigurierten Speicher aus.

- **Zugriffsleistung.** Die Profilverwaltung wählt den Speicher mit der besten Zugriffsleistung aus.

Konfigurationsrangfolge:

1. Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.
2. Wenn diese Einstellung weder hier noch in der .ini-Datei konfiguriert ist, wird die **Konfigurationsreihenfolge** verwendet.

## Grundlegende Richtlinieneinstellungen

June 27, 2024

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. Szenario: Die Richtlinie ist unter einem Multisitzungs-OS, etwa einer Citrix Virtual Apps-Umgebung, deaktiviert oder nicht konfiguriert. In diesem Fall 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 (in der Regel Benutzer von Citrix Virtual Desktops mit zugewiesenen virtuellen Desktops) Folgendes tun:

- Umgehen jeglicher Verarbeitung
- Anmelden
- Behandlung von Problemen mit der Desktop-Erfahrung per Profilverwaltung

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 nicht Anmeldungen lokaler Administratoren. 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.

Optionen für Pfade:

- Ein relativer Pfad. Dieser Pfad muss relativ zum Stammverzeichnis sein (normalerweise mit dem Attribut #homeDirectory# für einen Benutzer in Active Directory konfiguriert).
- Ein 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 Richtlinie 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.

### Benutzerspeicher migrieren

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 die folgenden Variablentypen verwenden:

- Systemumgebungsvariablen in Prozentzeichen
- Attribute des Active Directory-Benutzerobjekts in Rauten

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. Wenn mobile Benutzer arbeiten, werden ihre Profile lokal aktualisiert. Außerdem werden ihre Profile 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.

### Aktives Zurückschreiben bei Sitzungssperre und -trennung

Wenn diese Richtlinie und die Richtlinie **Aktiv zurückschreiben** aktiviert sind, werden Profildateien und -ordner nur dann zurückgeschrieben, wenn eine Sitzung gesperrt oder getrennt wird.

Wenn diese Richtlinie und die Richtlinien **Aktiv zurückschreiben** und **Aktives Zurückschreiben der Registrierung** aktiviert sind, werden Registrierungseinträge nur dann zurückgeschrieben, wenn eine Sitzung gesperrt oder getrennt wird.

## Unterstützung von Offlineprofilen

Aktiviert Offlineprofile. Dieses Feature ist für Computer gedacht, die häufig aus Netzwerken entfernt werden. Zum Beispiel Laptops oder mobile Geräte, keine 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

June 27, 2024

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. Szenario: Wenn der Speicher für plattformübergreifende Einstellungen eine Definitionsdatei ohne Daten enthält oder die zwischengespeicherten Daten eines Einzelplattformprofils neuer sind als die Definitionsdaten im Speicher. In diesem Fall migriert die Profilverwaltung die Daten vom Einzelplattformprofil in den Store, sofern Sie die 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.

## Dateisystem - Richtlinieneinstellungen

June 27, 2024

Dieser Abschnitt enthält Richtlinien, die Folgendes festlegen:

- Welche Dateien in einem Benutzerprofil, die zwischen dem System, auf dem das Profil installiert ist, und dem Benutzerspeicher synchronisiert werden
- Welche Verzeichnisse in einem Benutzerprofil, die zwischen dem System, auf dem das Profil installiert ist, und dem Benutzerspeicher synchronisiert werden

## Ausschlüsse - Richtlinieneinstellungen

June 27, 2024

Dieser Abschnitt enthält Informationen zu 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 werden in Dateinamen und Ordnernamen unterstützt, jedoch nur in Dateinamen rekursiv angewendet.

Beispiele:

- `Desktop\Desktop.ini` ignoriert die Datei `Desktop.ini` im Ordner `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.
- `Downloads\*\a.txt` ignoriert `a.txt` in jedem beliebigen unmittelbaren Unterordner des Ordners `Downloads`.

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%). Platzhalter in Ordnernamen werden unterstützt, aber nicht rekursiv angewendet.

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. Die möglichen Richtlinieneinstellungen und die entsprechenden Aktionen sind in der folgenden Tabelle aufgeführt:

| Richtlinieneinstellung | Aktion |
|---|---|
| Einstellung deaktiviert oder “Ausgeschlossene Dateien oder Ordner synchronisieren”auf Standard gesetzt | Die Profilverwaltung synchronisiert die ausgeschlossenen Dateien und Ordner aus dem Benutzerspeicher zu einem lokalen Profil, wenn sich ein Benutzer anmeldet. |
| Einstellung auf “Ausgeschlossene Dateien oder Ordner ignorieren”gesetzt | Die Profilverwaltung ignoriert die ausgeschlossenen Dateien und Ordner im Benutzerspeicher, wenn sich ein Benutzer anmeldet. |

| Richtlinieneinstellung | Aktion |
| --- | --- |
| Einstellung auf "Ausgeschlossene Dateien oder Ordner löschen"gesetzt | Die Profilverwaltung löscht die ausgeschlossenen Dateien und Ordner im Benutzerspeicher, wenn sich ein Benutzer anmeldet. |
| Einstellung in Web Studio nicht konfiguriert | Der Wert aus der INI-Datei wird verwendet. |
| Einstellung nicht in Web Studio oder in der INI-Datei konfiguriert | Die ausgeschlossenen Dateien und Ordner werden aus dem Benutzerspeicher zu einem lokalen Profil synchronisiert, wenn sich ein Benutzer anmeldet. |

### Verarbeitung von großen Dateien: Dateien werden als symbolische Verknüpfungen erstellt

Um die Anmeldeleistung zu verbessern und große Dateien zu verarbeiten, wird von der Profilverwaltung 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.

Auf diese Dateien kann nicht gleichzeitig in mehreren Sitzungen zugegriffen werden.

## Synchronisierung - Richtlinieneinstellungen

June 27, 2024

Der Abschnitt **Synchronisierung** enthält Informationen zu Richtlinieneinstellungen, um festzulegen, welche Dateien und Ordner in einem Benutzerprofil zwischen dem System, auf dem das Profil installiert ist, und dem Benutzerspeicher synchronisiert werden.

### Zu synchronisierende Verzeichnisse

Standardmäßig synchronisiert die Profilverwaltung das Benutzerprofil zwischen dem System, auf dem sie installiert ist, und dem Benutzerspeicher. Wenn Sie einen Ordner von der Synchronisierung

ausschließen, können Sie mit dieser Richtlinie die Unterordner des ausgeschlossenen Ordners in die Synchronisierung einbeziehen.

Pfade in dieser Liste müssen relativ zum Benutzerprofil sein. Platzhalter in Ordnernamen werden unterstützt, aber nicht rekursiv angewendet.

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

Standardmäßig synchronisiert die Profilverwaltung das Benutzerprofil zwischen dem System, auf dem sie installiert ist, und dem Benutzerspeicher. Wenn Sie einen Ordner von der Synchronisierung ausschließen, können Sie mit dieser Richtlinie die in dem ausgeschlossenen Ordner enthaltenen Dateien in die Synchronisierung einbeziehen.

Pfade in dieser Liste müssen relativ zum Benutzerprofil sein. Platzhalter werden in Dateinamen und Ordnernamen unterstützt, jedoch nur in Dateinamen rekursiv angewendet. Platzhalter können nicht geschachtelt werden.

Beispiele:

- `AppData\Local\Microsoft\Office\Access.qat` gibt eine Datei unter einem Ordner an, der in der Standardkonfiguration ausgeschlossen ist.
- `AppData\Local\MyApp\*.cfg` gibt alle Dateien mit der Erweiterung `.cfg` im Profilordner `AppData\Local\MyApp` 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 hilft bei der Lösung von Problemen mit Transaktionsordnern (auch “Referenzordner” ). Dieser Ordner enthält voneinander abhängige Dateien, wobei eine Datei auf die 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 Ordner **Internet Explorer-Cookies** 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.

In der folgenden Tabelle wird beispielsweise beschrieben, wie Index.dat auf Cookies verweist, wenn ein Benutzer im Internet unterwegs ist:

| Szenario | Wie Index.dat auf Cookies verweist |
|---|---|
| Ein Benutzer hat zwei Internet Explorer-Sitzungen (jede auf einem anderen Server) und besucht in jeder Sitzung verschiedene Websites.| Cookies von jeder Site werden auf dem entsprechenden Server hinzugefügt.|
|Der Benutzer meldet sich von der ersten Sitzung oder mitten in einer Sitzung ab (wenn die Funktion zum aktiven Zurückschreiben konfiguriert ist).| Die Cookies der zweiten Sitzung müssen die der ersten Sitzung ersetzen.|
|Die erste und die zweite Sitzung werden zusammengeführt und die Verweise auf die Cookies in Index.dat sind infolgedessen veraltet.| Weiteres Browsen in neuen Sitzungen führt zum wiederholten Zusammenführen und einem aufgeblähten Cookie-Ordner.|

Das Spiegeln des Cookie-Ordners behebt das Problem. In diesem Fall werden die Cookies jedes Mal, wenn sich Benutzer abmelden, mit den Cookies aus der letzten Sitzung überschrieben. 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.

### Beschleunigen der Ordnerspiegelung

Wenn sowohl diese Richtlinie als auch die Richtlinie **Zu spiegelnde Ordner** aktiviert sind, speichert die **Profilverwaltung gespiegelte Ordner** auf einem VHDX-basierten virtuellen Datenträger. Der virtuelle Datenträger wird während der Anmeldung angehängt und während der Abmeldung wieder entfernt. Durch Aktivieren dieser Richtlinie müssen die Ordner nicht mehr zwischen dem Benutzerspeicher und lokalen Profilen kopiert werden. Dies beschleunigt die Ordnerspiegelung.

## Ordnerumleitung - Richtlinieneinstellungen

June 27, 2024

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 UNC-Pfads. Dieser UNC-Pfad wird für umgeleitete Ordner angegeben.

Diese Einstellung ist standardmäßig deaktiviert. Und die Umgebungsvariable `%userdomain%` ist nicht Teil der UNC-Pfad-Angabe für umgeleitete Ordner.

## AppData(Roaming) - Richtlinieneinstellungen

June 27, 2024

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. Weitere Informationen finden Sie unter Pfad zum Benutzerspeicher.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

## Kontakte - Richtlinieneinstellungen

June 27, 2024

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.

## Desktop - Richtlinieneinstellungen

June 27, 2024

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.

## Dokumente - Richtlinieneinstellungen

June 27, 2024

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.

## Downloads - Richtlinieneinstellungen

June 27, 2024

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.

## Favoriten - Richtlinieneinstellungen

June 27, 2024

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.

## Links - Richtlinieneinstellungen

June 27, 2024

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.

## Musik - Richtlinieneinstellungen

June 27, 2024

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.

## Bilder - Richtlinieneinstellungen

June 27, 2024

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.

## Gespeicherte Spiele - Richtlinieneinstellungen

June 27, 2024

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.

## Startmenü - Richtlinieneinstellungen

June 27, 2024

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.

## Suchen - Richtlinieneinstellungen

June 27, 2024

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.

## Videos - Richtlinieneinstellungen

June 27, 2024

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.

## Protokollierung - Richtlinieneinstellungen

June 27, 2024

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 in Web Studio nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung nicht in Web Studio oder in der INI-Datei konfiguriert ist, wird Folgendes protokolliert:

- Fehler
- Allgemeine Informationen

### 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 nicht in Web Studio oder in der INI-Datei konfiguriert ist, wird Folgendes protokolliert:

- Fehler
- Allgemeine Informationen

### 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 nicht in Web Studio oder in der INI-Datei konfiguriert ist, wird Folgendes protokolliert:

- Fehler
- Allgemeine Informationen

### 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 nicht in Web Studio oder in der INI-Datei konfiguriert ist, wird Folgendes protokolliert:

- Fehler
- Allgemeine Informationen

### 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 nicht in Web Studio oder in der INI-Datei konfiguriert ist, wird Folgendes protokolliert:

- Fehler
- Allgemeine Informationen

### 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 nicht in Web Studio oder in der INI-Datei konfiguriert ist, wird Folgendes protokolliert:

- Fehler
- Allgemeine Informationen

### Anmeldung

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 nicht in Web Studio oder in der INI-Datei konfiguriert ist, wird Folgendes protokolliert:

- Fehler
- Allgemeine Informationen

### 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 geschieht Folgendes:

- Ein vorhandenes Backup der Datei (.bak) wird gelöscht.
- Die Protokolldatei wird in eine BAK-Datei umbenannt.
- 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 die Protokolldateien beim Neustart der Maschine beibehalten werden. Geben Sie für virtuelle Maschinen ohne eine persistente 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. So soll sichergestellt werden, 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 nicht in Web Studio oder in der INI-Datei konfiguriert ist, wird Folgendes protokolliert:

- Fehler
- Allgemeine Informationen

### 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 nicht in Web Studio oder in der INI-Datei konfiguriert ist, wird Folgendes protokolliert:

- Fehler
- Allgemeine Informationen

### 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 nicht in Web Studio oder in der INI-Datei konfiguriert ist, wird Folgendes protokolliert:

- Fehler
- Allgemeine Informationen

### 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 nicht in Web Studio oder in der INI-Datei konfiguriert ist, wird Folgendes protokolliert:

- Fehler
- Allgemeine Informationen

## Profilverarbeitung - Richtlinieneinstellungen

June 27, 2024

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. Daher stellt ein Wert von 60 sicher, dass Profile zwischen einer und zwei Minuten nach dem Abmelden der Benutzer gelöscht werden. Diese Aktion hängt davon ab, wann die letzte Überprüfung stattgefunden hat. 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 festgelegt, wie sich die Profilverwaltung verhält, wenn ein Benutzerprofil in beiden der folgenden Bereichen vorhanden ist:

- Benutzerspeicher

- Lokales Windows-Benutzerprofil (kein Citrix-Benutzerprofil)

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 Backup) 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. Danach wird das Benutzerspeicherprofil von der Profilverwaltung in folgenden beiden Bereichen verwendet:

- Aktuelle Sitzung
- Alle anderen mit dem Pfad zum gleichen Benutzerspeicher konfigurierten Sitzungen

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 vorhandener Anwendungsprofile

Diese Einstellung aktiviert oder deaktiviert die automatische Migration von Anwendungsprofilen über verschiedene Betriebssysteme. Die Anwendungsprofile umfassen die Anwendungsdaten im `AppData`-Ordner und die Registrierungseinträge unter `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 `AppData`-Ordner 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.

Szenario: Ein Benutzer hat kein Citrix Benutzerprofil, sondern ein lokales Windows-Benutzerprofil. In diesem Fall wird standardmäßig das lokale Profil verwendet und in den Benutzerspeicher migriert, sofern dieser Wert aktiviert 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.

Szenario: Ein Benutzer hat kein Citrix Benutzerprofil, sondern ein Windows-Roamingprofil. In diesem Fall wird standardmäßig das Roamingprofil verwendet und in den Benutzerspeicher migriert, sofern dieser Wert aktiviert 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 verbindliches 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.

## Registrierung - Richtlinieneinstellungen

June 27, 2024

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.

## Gestreamte Benutzerprofile - Richtlinieneinstellungen

June 27, 2024

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, wird 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, wird sie deaktiviert.

### Profilstreaming

Diese Einstellung aktiviert oder deaktiviert das Feature für gestreamte Citrix Benutzerprofile. Wenn diese Einstellung aktiviert ist, werden Dateien und Ordner nur dann aus dem Benutzerspeicher auf den lokalen Computer abgerufen, wenn die Benutzer nach der Anmeldung auf sie zugreifen. 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, wird 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 Benutzerprofile verarbeitet.

### Profilstreamingausschluss aktivieren

Wenn der Profilstreamingausschluss aktiviert ist:

- Die Profilverwaltung streamt die in der Ausschlussliste angegebenen Ordner nicht.
- Alle Ordner werden sofort vom Benutzerspeicher auf den lokalen Computer abgerufen, bei dem sich der Benutzer anmeldet.

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 Benutzerdateien aus dem Bereich für ausstehende Dateien in den Benutzerspeicher zurückgeschrieben werden, wenn ein Speicherserver nicht mehr reagiert und der Benutzerspeicher gesperrt bleibt. Dieses Verhalten verhindert ein Aufblähen des Bereichs für ausstehende Dateien und stellt sicher, dass der Benutzerspeicher 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.

#### Profilstreaming für ausstehenden Bereich aktivieren

Hiermit können Sie das Feature zum Profilstreaming für Dateien und Ordner im ausstehenden Bereich aktivieren.

Der ausstehende Bereich wird verwendet, um die Profilkonsistenz sicherzustellen, während Profilstreaming aktiviert ist. Profildateien und Ordner, die in gleichzeitigen Sitzungen geändert wurden, werden vorübergehend im ausstehenden Bereich gespeichert.

Diese Richtlinie ist standardmäßig deaktiviert, und alle Dateien und Ordner im ausstehenden Bereich werden bei der Anmeldung in das lokale Profil abgerufen. Wenn diese Richtlinie aktiviert ist, werden Dateien im ausstehenden Bereich nur dann in das lokale Profil abgerufen, wenn sie angefordert werden. Verwenden Sie die Richtlinie mit der Richtlinie "Profilstreaming", um eine optimale Anmeldeerfahrung bei mehreren gleichzeitigen Sitzungen zu gewährleisten.

Die Richtlinie gilt für Ordner im ausstehenden Bereich, wenn die Richtlinie "Profilstreaming für Ordner aktivieren"aktiviert ist.

## Richtlinieneinstellungen für Benutzerpersonalisierungslayer

June 27, 2024

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 des Benutzerlayers (GB): Die Standard-Benutzerlayergröße beträgt 10 GB (von Citrix empfohlenes Minimum). Ein Benutzerlayer ist ein Datenträger mit schlanker Speicherzuweisung, der auf die festgelegte Größe erweitert wird, wenn Speicherplatz verwendet wird. Benutzerlayer werden nie verkleinert.

> **Hinweis:**
>
> Das Vergrößern des Benutzerlayers wirkt sich auf neue Benutzerlayer aus und erweitert vorhandene Benutzerlayer. Das Verringern der Größe wirkt sich nur auf neue Benutzerlayer aus. Vorhandene Benutzerlayer werden nie verkleinert.

Weitere Informationen finden Sie unter Benutzerpersonalisierungslayer.

## Virtual Delivery Agent - Richtlinieneinstellungen

June 27, 2024

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. Diese Einstellung ist optional und kann mit der Einstellung **Controller-SIDs** verwendet werden.

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. Außerdem überprüft jeder Controller alle 90 Minuten die Sitedatenbank auf Controller-Informationen. Der Controller sendet aktualisierte Listen an seine registrierten VDAs, wenn eines der folgenden Ereignisse eintritt:

- Seit der letzten Prüfung wurde ein Controller hinzugefügt oder entfernt.
- Eine Richtlinienänderung ist eingetreten.

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.

## HDX 3D Pro - Richtlinieneinstellungen

June 27, 2024

Der Bereich "HDX 3D Pro"enthält Richtlinieneinstellungen, mit denen Sie das Tool zum Konfigurieren der Bildqualität für Benutzer aktivieren und konfigurieren können. Mit diesem Tool können Benutzer die Nutzung der verfügbaren Bandbreite optimieren. Für diese Optimierung wird das Gleichgewicht zwischen Bildqualität und Reaktion in Echtzeit angepasst.

### 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.

Szenario: Ein Benutzer aktiviert die verlustfreie Komprimierung. In diesem Fall 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, der den Benutzern im Tool zum Konfigurieren der Bildqualität zur Verfügung steht. Mithilfe dieser Werte können die Benutzer den Bereich der Bildqualitätsanpassung im Tool zur Konfiguration der Bildqualität definieren.

Geben Sie für die Bildqualität Werte zwischen 0 und 100 an. Der Höchstwert muss größer oder gleich dem Mindestwert sein.

## Überwachungsrichtlinie - Richtlinieneinstellungen

June 27, 2024

Der Abschnitt **Überwachung** enthält Richtlinieneinstellungen für die Prozess-, Ressourcen- und Anwendungsfehlerüberwachung.

Der Geltungsbereich dieser Richtlinien kann auf der Grundlage der folgenden Kriterien definiert werden:

- Site
- Bereitstellungsgruppe
- Art der Bereitstellungsgruppe
- Organisationseinheit
- Tags

## 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. Szenario: Sie möchten keine Ressourcen- und/oder Prozessdaten für einen bestimmten Bereich überwachen. Zum Beispiel für eine Bereitstellungsgruppe oder Organisationseinheit. In diesem Fall wird empfohlen, 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 jedem VDA in die Datenbank übertragen. Prozessdaten (falls aktiviert) werden alle 10 Minuten in die Datenbank übertragen. 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 Einstellungen für die Datenaufbewahrung werden zum Speichern der folgenden Elemente für einen VDA über einen Zeitraum von einem Jahr ca. 276 KB Speicherplatz benötigt:

- CPU
- Speicher
- IOPS
- Daten zur Datenträgerlatenz

| Anzahl an 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 an 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 variieren je nach Bereitstellung.

**Optionale Konfigurationen**

Sie können die Standardeinstellungen für die Datenaufbewahrung nach Bedarf ändern. Diese Konfiguration benötigt jedoch zusätzlichen Speicherplatz. 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.

## Richtlinie zum Sammeln von Daten für die Analyse

### VDA-Datenerfassung für die Analyse

Aktivieren oder deaktivieren Sie mithilfe der Richtlinie die Sammlung leistungs- und sicherheitsbezogener Metriken der VDAs für die Leistungs- und Sicherheitsanalyse durch den Überwachungsdienst.
Die Standardeinstellung ist **Zugelassen**. Setzen Sie die Richtlinie auf **Nicht zugelassen**, um die Erfassung von Daten von den VDAs zu beenden.

#### Zwischenablagen-Metadatensammlung für die Sicherheitsüberwachung

Verwenden Sie die Richtlinie, um die Zwischenablagen-Metadatensammlung durch den Brokerdienst zum Zweck der Sicherheitsüberwachung, von Audits und von Compliance zu aktivieren oder zu deaktivieren. Die Richtlinie ist standardmäßig **aktiviert**. Setzen Sie die Richtlinie auf **Deaktiviert**, um die Erfassung von Daten von den VDAs zu beenden.

#### Erfassung von Diagnosedaten zur Leistungsüberwachung

Verwenden Sie diese Richtlinie, damit der Überwachungsdienst Diagnosedaten wie Sitzungsinformationen, UPM/EUEM-Dienststatus, Microsoft Teams-Optimierung und Verbindungsprotokolle erfassen kann. Die Richtlinie ist standardmäßig **aktiviert**. Setzen Sie die Richtlinie auf **Deaktiviert**, um die Erfassung von Daten von den VDAs zu beenden.

### 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.

## Virtuelle IP - Richtlinieneinstellungen

June 27, 2024

> **Wichtig:**
>
> - Windows 10 Enterprise-Multisitzungs-OS unterstützt keine IP-Virtualisierung (virtuelle IP) für Remotedesktops und Citrix unterstützt weder Remotedesktop-IP-Virtualisierung noch virtuelles Loopback für Windows 10-Multisitzungs-OS.
> - Remotedesktop-IP-Virtualisierung (Virtual IP) wird auf in der Cloud gehosteten Maschinen nicht unterstützt. Informationen hierzu finden Sie in der Dokumentation von Microsoft.

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. Geben Sie beim Hinzufügen von Programmen zur Liste nur den Namen der ausführbaren Datei an. Sie müssen nicht den gesamten Pfad angeben.

In der Standardeinstellung sind keine ausführbaren Dateien angegeben.

## COM-Port- und LPT-Portumleitungseinstellungen in der Registrierung konfigurieren

June 27, 2024

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

| Registrierungsschlüssel | Beschreibung | Zulässige Werte |
|---|---|---|
| AllowComPortRedirection | Zulassen oder Verhindern der COM-Portumleitung | 1 (Zulassen) oder 0 (Verhindern) |
| LimitComBw | Bandbreitenlimit für COM-Portumleitungskanal | Numerischer Wert |
| LimitComBWPercent | Bandbreitenlimit für COM-Portumleitungskanal als Prozentsatz der Gesamtsitzungsbandbreite | Numerischer Wert zwischen 0 und 100 |
| AutoConnectClientComPorts | Automatische Verbindung von COM-Ports auf dem Benutzergerät | 1 (Zulassen) oder 0 (Verhindern) |
| AllowLptPortRedirection | Zulassen oder Verhindern der LPT-Portumleitung | 1 (Zulassen) oder 0 (Verhindern) |
| LimitLptBw | Bandbreitenlimit für LPT-Portumleitungskanal | Numerischer Wert |
| LimitLptBwPercent | Bandbreitenlimit für LPT-Portumleitungskanal als Prozentsatz der Gesamtsitzungsbandbreite | Numerischer Wert zwischen 0 und 100 |
| AutoConnectClientLptPorts | Automatische Verbindung von LPT-Ports auf dem Benutzergerät | 1 (Zulassen) oder 0 (Verhindern) |

Nach dem Konfigurieren dieser Einstellungen ändern Sie die Maschinenkataloge, damit sie das neue Masterimage oder die aktualisierte physische Maschine verwenden. Wenn sich die Benutzer das nächste Mal abmelden, werden die Desktops mit den neuen Einstellungen aktualisiert.

## Connector für Configuration Manager 2012 - Richtlinieneinstellungen

June 27, 2024

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 Web 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 Warnung

Diese Einstellung gibt das Intervall an, mit dem Benutzern Warnungen 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 Warnung

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} Save your work. The server goes offline for maintenance in {TIMELEFT}.

### Meldungsfeldtitel für Warnung

Diese Einstellung enthält den editierbaren Titel für die Titelleiste der Warnung, die Benutzer erhalten.

Der Standardtitel ist: Upcoming Maintenance

### Zeitraum für Warnung

Diese Einstellung definiert, wie lange vor Wartungsaufgaben die Warnung 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 Warnung 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} Save your work and log off. The server goes offline for maintenance in {TIMELEFT}.

### 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 Web 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

June 27, 2024

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 anderen Service gehostet werden, richten Sie die erste Verbindung mit dem Hypervisor bzw. Service beim Erstellen einer Site ein. Der Speicher und die Netzwerkdetails der Verbindung bilden die Ressourcen. Später können Sie die Verbindung und ihre Ressourcen ändern und weitere 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, so konfigurieren, dass sie eine eindeutige virtuelle Loopbackadresse im Bereich des lokalen Hosts verwenden.

### Delivery Controller

Dieser Artikel enthält Überlegungen und Verfahren für das Hinzufügen und Entfernen von Controllern zu/aus einer Site. 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

### Verwenden der 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 Profillösung verwenden, lesen Sie den vorliegenden Artikel mit allgemeinen Informationen. Weitere Informationen finden Sie in der Dokumentation zu Profilverwaltung.

#### Aufzeichnen einer Citrix Diagnostic Facility-Überwachung beim Systemstart

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.

### Citrix Insight Services

Citrix Insight Services (CIS) ist eine Plattform von Citrix für Instrumentierung, Telemetrie und Ablaufverfolgung.

#### Citrix Scout

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.

## Anwendungen

June 27, 2024

> **Hinweis:**
>
> Sie können Ihre Citrix Virtual Apps and Desktops-Bereitstellung mithilfe von zwei Verwaltungskonsolen verwalten: Web Studio (webbasiert) und Citrix Studio (Windows-basiert). Dieser Artikel behandelt nur Web Studio. Informationen zu Citrix Studio finden Sie im entsprechenden Artikel in Citrix Virtual Apps and Desktops 7 2212 oder früher.

## 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 stattdessen 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 Gruppen 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 (aber evtl. aus verschiedenen Gruppen) den gleichen Benutzern bereitstellen, ändern Sie in Web Studio die Eigenschaft `Application name (for user)`. Andernfalls 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:

- Bereitstellungsgruppen erstellen
- Anwendungsgruppen erstellen
- Tags

## Anwendungen hinzufügen

Sie können Anwendungen beim Erstellen von Bereitstellungsgruppen oder Anwendungsgruppen hinzufügen. Diese Verfahren werden unter Erstellen von Bereitstellungsgruppen und Erstellen von Anwendungsgruppenbeschrieben. 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 linken Bereich **Anwendungen** und dann in der Aktionsleiste **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 Seiten **Gruppen**, **Anwendungen** und **Zusammenfassung**. Wenn Sie eine Seite abgeschlossen haben, klicken Sie auf **Weiter**, bis Sie zur Seite **Zusammenfassung** gelangen.

Alternativen für Schritt 1, wenn Sie Anwendungen einer einzelnen Bereitstellungsgruppe oder Anwendungsgruppe hinzufügen möchten:

- **Hinzufügen von Anwendungen zu einer einzelnen Bereitstellungsgruppe:** Wählen Sie in zuerst in Web Studio im linken Bereich **Bereitstellungsgruppe**, dann im mittleren Bereich eine Bereitstellungsgruppe und zum Schluss in der Aktionsleiste **Anwendungen hinzufügen**. Der Assistent zeigt die Seite **Gruppen** nicht an.
- **Hinzufügen von Anwendungen zu einer einzelnen Anwendungsgruppe:** Wählen Sie zuerst in Web Studio im linken Bereich **Anwendungen**, dann im mittleren Bereich eine Anwendungsgruppe und zum Schluss in der Aktionsleiste unter dem Namen der Anwendungsgruppe den Eintrag **Anwendungen hinzufügen**. Der Assistent zeigt die Seite **Gruppen** nicht an.

#### Seite "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 sollten Sie Anwendungen Anwendungsgruppen (sofern verwendet) hinzufügen und nicht Bereitstellungsgruppen.

Beim Hinzufügen einer Anwendung aktivieren Sie das Kontrollkästchen mindestens einer Bereitstellungsgruppe (oder Anwendungsgruppe, falls verfügbar). Jede Anwendung muss immer mindestens einer Gruppe zugeordnet sein.

#### Anwendungsseite

Klicken Sie auf **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:** Anwendungen auf einem VDA in der Bereitstellungsgruppe oder an einem anderen Ort in Ihrem Netzwerk. Wenn Sie diese Quelle wählen, wird eine neue Seite geöffnet, auf der Sie mit folgenden Schritten eine Anwendung festlegen können, die Sie hinzufügen möchten:

  - Geben Sie den Pfad zur ausführbaren Datei, das Arbeitsverzeichnis, optionale Befehlszeilenargumente und Anzeigenamen für Administratoren und Benutzer ein.
  - Wählen Sie eine Anwendung von einem VDA in der Bereitstellungsgruppe aus. Klicken Sie dazu auf **Durchsuchen**, geben Sie Ihre Anmeldeinformationen für den VDA-Zugriff ein, warten Sie, bis Sie mit dem VDA verbunden sind, und wählen Sie eine Anwendung auf dem VDA aus. Die Eigenschaften der ausgewählten Anwendung werden automatisch in die Felder auf der Seite eingefügt.

- **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-Anwendungen bereitstellen.

  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 Liste **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 Liste angezeigt. Anwendungen, die den ausgewählten Gruppen bereits hinzugefügt wurden, können nicht ausgewählt werden.

Sie können die Eigenschaften einer Anwendung (Einstellungen) auf dieser Seite oder später ändern.

Standardmäßig werden hinzugefügte Anwendungen in einem Anwendungsordner mit dem Namen `Applications` abgelegt. Sie können die Anwendung auf dieser Seite oder später ändern. Wenn beim Hinzufügen einer Anwendung bereits eine gleichnamige Anwendung im Ordner vorliegt, werden Sie aufgefordert, die neue Anwendung umzubenennen. Übernehmen Sie den angebotenen neuen Namen oder lehnen Sie ihn ab und benennen Sie die Anwendung um oder wählen Sie einen anderen Ordner. Wenn beispielsweise `app` im Ordner **Applications** bereits vorhanden ist und Sie versuchen, dem Ordner eine andere Anwendung mit dem Namen `app` hinzuzufügen, wird der neue Name `app_1` angeboten.

#### Zusammenfassungsseite

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 **Fertigstellen**.

### Ändern der Gruppenzuordnung einer Anwendung

Nach dem Hinzufügen einer Anwendung können Sie die Bereitstellungsgruppen und Anwendungsgruppen ändern, denen die Anwendung zugeordnet ist.

Sie können eine Anwendung mit der Maus zu einer zusätzlichen Gruppe ziehen. Dies ist eine Alternative zum Verwenden der Befehle in der Aktionsleiste.

Wenn eine Anwendung mehreren Bereitstellungsgruppen oder Anwendungsgruppen 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 `Edit delivery group` haben. Der Bereitstellungsgruppentyp wird automatisch in `desktops and applications` konvertiert, wenn für das Eigenschaftendialogfeld ein Commit ausgeführt wird.

1. Melden Sie sich bei Web Studio an, wählen Sie im linken Bereich **Anwendungen** und wählen Sie dann die Anwendung.
2. Wählen Sie in der Aktionsleiste **Eigenschaften**.
3. Wählen Sie die Seite **Gruppen** aus.

    - Zum Hinzufügen einer Gruppe klicken Sie auf **Hinzufügen** und wählen Sie **Anwendungsgruppen** oder **Bereitstellungsgruppen**. (Wenn Sie keine Anwendungsgruppen erstellt haben, wird 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.
    - 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 Gruppe mehr zugeordnet ist, werden Sie vor dem Löschen der Anwendung gewarnt.
    - 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**.

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.

### 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 das Ziehen und Ablegen mit der Maus.)
- **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 linken Bereich **Anwendungen**.
2. Wählen Sie mindestens eine Anwendung im mittleren Bereich und dann die gewünschte Aufgabe in der Aktionsleiste.
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 die Anwendung dadurch 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 linken Bereich **Bereitstellungsgruppen**.
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 in der Aktionsleiste **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 Gruppe 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 linken Bereich **Anwendungen**.
2. Wählen Sie im mittleren Bereich die Anwendungsgruppe und wählen Sie dann mindestens eine Anwendung aus.
3. Wählen Sie in der Aktionsleiste **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 linken Bereich **Anwendungen**.
2. Wählen Sie die Anwendung und dann in der Aktionsleiste **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) | Standort |
| Bereitstellungsgruppen und Anwendungsgruppen, in denen die Anwendung verfügbar ist | Gruppen |
| Beschreibung | Identifizierung |
| Dateinamenerweiterungen und Dateitypzuordnung: die Erweiterungen, die von der Anwendung automatisch geöffnet werden | Dateitypzuordnung |
| Symbol | Bereitstellung |
| Schlüsselwörter für StoreFront | Identifizierung |
| Limits (siehe Konfigurieren von Anwendungslimits) | Bereitstellung |
| Name: Namen, die Benutzer und Administrator sehen | Identifizierung |
| Pfad zur ausführbaren Datei (siehe Übergeben von Parametern an veröffentlichte Anwendungen) | Standort |
| Verknüpfung auf dem Desktop des Benutzers: aktivieren oder deaktivieren | Bereitstellung |

| Eigenschaft | Seite |
| --- | --- |
| Sichtbarkeit: Legt fest, welche Benutzer die Anwendung in der Citrix Workspace-App sehen (eine unsichtbare Anwendung kann trotzdem gestartet werden). Soll sie nicht verfügbar und unsichtbar sein, fügen Sie sie einer anderen Gruppe hinzu. | Sichtbarkeit beschränken |
| Arbeitsverzeichnis | Standort |

Anwendungsänderungen werden evtl. für aktuelle Anwendungsbenutzer erst wirksam, wenn diese sich von ihrer 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. Das Limit kann zur Aufrechterhaltung der Serverleistung beitragen und eine Verschlechterung der Serviceleistung verhindern.

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 im Ausfallmodus ist.

Standardmäßig besteht kein Limit für die Anzahl gleichzeitig ausgeführter Anwendungsinstanzen. Es gibt mehrere Einstellungen für Anwendungslimits. Sie können eine beliebige Auswahl von Limits oder auch alle 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, `Delta` 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. Die Anforderungen bestimmen auch, 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)

  Zum Beschränken der Verwendung einer Anwendung auf bestimmte Maschinen innerhalb einer Bereitstellungsgruppe (zusätzlich zur Beschränkung der Instanzen auf allen Maschine der Site) gehen Sie folgendermaßen vor:

  - Verwenden Sie die Tagging-Funktionalität für diese Maschinen.
  - Konfigurieren Sie das Limit der Anzahl von Instanzen pro Maschine für diese Anwendung.

Werden Anwendungen 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. Instanzen, die das Limit überschreiten, werden nicht zwangsweise heruntergefahren. Sie können weiter ausgeführt werden, bis die Benutzer sie beenden.

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 unter Sitzungen.

Konfigurieren der maximalen Anzahl Instanzen pro Bereitstellungsgruppe und des Limits von einer Instanz pro Benutzer:

1. Wählen Sie im linken Bereich **Anwendungen** und dann eine Anwendung.
2. Wählen Sie in der Aktionsleiste **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 pro Maschine 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 Zeichen `"%*"`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 Zeichen %* Anführungszeichen. Zwischen dem Anführungszeichen nach dem Pfad und dem Anführungszeichen vor %* muss ein Leerzeichen stehen.

Die Befehlszeile für die veröffentlichte Anwendung Windows Media Player wäre beispielsweise:

```
"C:\Program Files\Windows Media Player\mplayer1.exe""%*"
```

> **Hinweis:**
>
> Die maximale Zeichenanzahl (einschließlich Argumenten) in der Befehlszeile zum Starten veröffentlichter Anwendungen beträgt 203.

### 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 zulässig.
- Ordner werden in Web 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 `View Applications` und die Berechtigung `Edit Application Properties`.
- Die meisten der folgenden Verfahren umfassen Aktionen aus der Aktionsleiste in Web 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 linken Bereich **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 in der Aktionsleiste **Ordner erstellen**. Geben Sie einen Namen ein.
- **Verschieben eines Ordners:** Wählen Sie den Ordner und dann in der Aktionsleiste **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 Ziehen mit der Maus.
- **Umbenennen eines Ordners:** Wählen Sie den Ordner und dann in der Aktionsleiste **Ordner umbenennen**. Geben Sie einen Namen ein.
- **Löschen eines Ordners:** Wählen Sie den Ordner und dann in der Aktionsleiste **Ordner löschen**. Beim Löschen eines Ordners, der Anwendungen und andere Ordner enthält, werden diese Objekte auch gelöscht. Beim Löschen einer Anwendung wird die Anwendungszuweisung aus der Bereitstellungsgruppe entfernt. Sie wird nicht von der Maschine entfernt.
- **Verschieben von Anwendungen in einen Ordner:** Wählen Sie eine oder mehrere Anwendungen. Wählen Sie dann in der Aktionsleiste **Anwendung verschieben**. Wählen Sie den Ordner aus.

Beim Erstellen von Bereitstellungsgruppen und Anwendungsgruppen können Sie Anwendungen, die Sie hinzufügen, auch auf der Seite **Anwendung** auch in einen 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 in der Anwendung `New-Broker` oder dem Cmdlet `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 Web Studio verfügbar.
- Die Option erfordert mindestens StoreFront 3.14, Citrix Receiver für Windows 4.11 und Delivery Controller 7.17.

## App-Pakete

June 27, 2024

> **Hinweis:**
>
> Sie können Ihre Citrix Virtual Apps and Desktops-Bereitstellung mithilfe von zwei Verwaltungskonsolen verwalten: Web Studio (webbasiert) und Citrix Studio (Windows-basiert). Dieser Artikel behandelt nur Web Studio. Informationen zu Citrix Studio finden Sie im entsprechenden Artikel in Citrix Virtual Apps and Desktops 7 2212 oder früher.

Microsoft bietet drei Verpackungstechnologien zur Bereitstellung von Anwendungen für Benutzer: App-V, MSIX und das MSIX-Feature zum Anfügen von Apps. In diesem Artikel wird die Bereitstellung solcher Anwendungspakete mit **Web Studio > App-Pakete** erläutert:

- App-V-Anwendungen bereitstellen
- MSIX- und MSIX App Attach-Anwendungen bereitstellen

## App-V-Anwendungen bereitstellen

In diesem Abschnitt wird Folgendes behandelt:

- Überblick. Beschreibung der zum Bereitstellen und Verwalten der App-V-Pakete verwendeten Verwaltungsmethoden.
- Verfahren. Verfahren zum Bereitstellen der Pakete.

### Übersicht

Dieser Abschnitt erläutert die zum Bereitstellen und Verwalten der App-V-Pakete verwendeten Verwaltungsmethoden. Weitere Informationen zu den Komponenten und Konzepten für die Bereitstellung von App-V-Paketanwendungen finden Sie in der Microsoft-Dokumentation: https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-for-windows.

Sie können die folgenden Methoden verwenden, um App-V-Pakete bereitzustellen und zu verwalten:

- **Duale Verwaltung**. Anwendungspakete werden auf App-V-Servern konfiguriert und verwaltet. Citrix Virtual Apps and Desktops- und App-V-Server arbeiten bei der Bereitstellung und Verwaltung von Paketen zusammen.

  Bei dieser Methode muss Citrix Virtual Apps and Desktops die Snapshot-Ansicht zum Status des App-V-Servers regelmäßig aktualisieren. Dies ist mit Hardware-, Infrastruktur- und Verwaltungsaufwand verbunden. Citrix Virtual Apps and Desktops- und App-V-Server müssen insbesondere für die Benutzerberechtigungen immer synchronisiert bleiben.

  Duale Verwaltung funktioniert am besten in Bereitstellungen, in denen App-V und Ihre Umgebung eng gekoppelt sind:

  - **App-V-Verwaltungsserver**. Veröffentlicht und verwaltet den Lebenszyklus von App-V-Paketen und dynamischen Konfigurationsdateien.
  - **Citrix Personalisierungskomponente**, die auf VDA-Maschinen installiert ist. Verwalten die Registrierung des entsprechenden App-V-Veröffentlichungsservers, der für Anwendungsstarts erforderlich ist.

  Dadurch wird sichergestellt, dass der App-V-Veröffentlichungsserver zum entsprechenden Zeitpunkt für den Benutzer synchronisiert ist. Der Veröffentlichungsserver verwaltet andere Aspekte des Paketlebenszyklus, z. B. Aktualisieren bei Anmeldung und Verbindungsgruppen.

- **Einzelverwaltung**. Anwendungspakete werden in Netzwerkfreigaben gespeichert. Citrix Virtual Apps and Desktops stellt Pakete unabhängig bereit und verwaltet sie unabhängig.

  Diese Methode reduziert den Mehraufwand, da die App-V-Server und die Datenbankinfrastruktur in der Bereitstellung nicht benötigt werden.

  Bei dieser Methode speichern Sie App-V-Pakete in einer Netzwerkfreigabe und laden ihre Metadaten von diesem Speicherort in Ihre Umgebung hoch. Die auf VDA-Maschinen installierte Komponente Citrix Personalisierung verwaltet und stellt Anwendungen wie folgt bereit:

  - Verarbeiten die Bereitstellungskonfigurationsdateien und Benutzerkonfigurationsdateien, wenn eine Anwendung gestartet wird.
  - Verwalten alle Aspekte der Lebenszyklen für Pakete auf der Hostmaschine.

Sie können beide Verwaltungsmethoden parallel verwenden. Das heißt, die einer Bereitstellungsgruppe hinzugefügten Anwendungen dürfen aus App-V-Paketen stammen, die auf App-V-Servern oder in Netzwerkfreigaben vorhanden 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.

#### Verfahren

Zur Unterstützung der Bereitstellung von App-V-Anwendungen müssen Sie die Citrix Personalisierungskomponente auf VDA-Maschinen installieren. Weitere Informationen finden Sie unter Citrix Personalisierungskomponente auf VDA-Maschinen installieren.

Führen Sie die folgenden Schritte aus, um mit App-V verpackte Anwendungen für die Benutzer bereitzustellen:

1. Speichern Sie die Anwendungspakete in Netzwerkfreigaben.
2. Laden Sie Anwendungspakete in Ihre Umgebung hoch.
3. Fügen Sie die Anwendungen zu Bereitstellungsgruppen hinzu.
4. Erstellen Sie Isolationsgruppen, um die automatische Bereitstellung voneinander abhängiger App-V-Pakete zu aktivieren.

Informationen dazu, wie Sie das Erkennen und Anwenden dynamischer App-V-Konfigurationsdateien im Einzelverwaltungsmodus in Citrix Virtual Apps and Desktops konfigurieren, finden Sie in diesem Citrix Blog.

## MSIX- und MSIX App Attach-Anwendungen bereitstellen

In diesem Abschnitt wird Folgendes behandelt:

- Überblick. Beschreibung der Verwaltung und Bereitstellung von MSIX- und MSIX App Attach-Paketen.
- Verfahren. Verfahren zum Bereitstellen der Pakete.

### Übersicht

Citrix Virtual Apps and Desktops stellt MSIX- und MSIX App Attach-Anwendungen über die auf VDA-Maschinen installierte Citrix Personalisierungskomponente bereit. Diese Komponente verwaltet alle Lebenszyklusaspekte der Pakete auf der Hostmaschine.

Weitere Informationen zu MSIX und zum MSIX-Feature zum Anfügen von Apps finden Sie in der Microsoft-Dokumentation unter https://docs.microsoft.com/en-us/windows/msix/ bzw. https://docs.microsoft.com/en-us/azure/virtual-desktop/what-is-app-attach.

### Verfahren

Zur Unterstützung der Bereitstellung von MSIX-Paketen und von mit dem MSIX-Feature zum Anfügen von Apps erstellten Paketen müssen Sie die Citrix Personalisierungskomponente auf VDA-Maschinen installieren. Weitere Informationen finden Sie unter Citrix Personalisierungskomponente auf VDA-Maschinen installieren.

Führen Sie folgende Schritte aus, um MSIX-Pakete und mit dem MSIX-Feature zum Anfügen von Apps verpackte Anwendungen für Benutzer bereitzustellen:

1. Speichern Sie die Anwendungspakete in Netzwerkfreigaben.
2. Laden Sie Anwendungspakete in Ihre Umgebung hoch.
3. Fügen Sie die Anwendungen zu Bereitstellungsgruppen hinzu.

## Citrix Personalisierungskomponente auf VDA-Maschinen installieren

Die Citrix Personalisierungskomponente verwaltet die Veröffentlichung von Anwendungspaketen im App-V- und MSIX-Format sowie von mit dem MSIX-Feature zum Anfügen von Apps erstellen Paketen. Die Komponente wird bei der Installation eines VDA nicht standardmäßig installiert. Sie können die Komponente während oder nach der VDA-Installation installieren.

Verwenden Sie eine der folgenden Methoden, um die Komponente während der VDA-Installation zu installieren:

- Wechseln Sie im Installationsassistenten zur Seite **Zusätzliche Komponenten**, und aktivieren Sie dann das Kontrollkästchen **Citrix Personalisierung für App-V - VDA**.
- Verwenden Sie in der Befehlszeilenschnittstelle die Option **/includeadditional "Citrix Personalisierung für App-V - VDA"**.

Gehen Sie folgendermaßen vor, um die Komponente nach der VDA-Installation zu installieren:

1. Wechseln Sie auf der VDA-Maschine zu **Systemsteuerung > Programme > Programme und Funktionen**, klicken Sie mit der rechten Maustaste auf **Citrix Virtual Delivery Agent**, und wählen Sie dann **Ändern** aus.
2. Wechseln Sie im angezeigten Assistenten zur Seite **Zusätzliche Komponenten**, und aktivieren Sie dann das Kontrollkästchen **Citrix Personalisierung für App-V - VDA**.

> **Hinweis:**
>
> Microsoft App-V Desktop Client ist die Komponente, die virtuelle Anwendungen aus App-V-Paketen auf Benutzergeräten ausführt. Windows 10 (1607 oder höher), Windows Server 2016 und Windows Server 2019 enthalten diese App-V-Clientsoftware bereits. Sie müssen sie nur auf VDA-Maschinen aktivieren. Weitere Informationen finden Sie in folgendem Artikel der Microsoft-Dokumentation: https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-enable-the-app-v-desktop-client.

### Anwendungspakete in Netzwerkfreigaben speichern

Nach dem Einrichten der Infrastruktur generieren Sie die Anwendungspakete und speichern sie an einem Netzwerkspeicherort, z. B. in einer UNC- oder SMB-Netzwerkfreigabe oder einer Azure-Dateifreigabe.

Verfahren:

1. Generieren Sie Anwendungspakete. Weitere Informationen hierzu finden Sie in der Microsoft Dokumentation.
2. Speichern Sie Anwendungspakete an einem Netzwerkspeicherort:
    - **App-V-Einzelverwaltung:** Speichern Sie die Pakete und die dazugehörigen dynamischen Konfigurationsdateien (App-V) in einer UNC- oder SMB-Netzwerkfreigabe oder einer Azure-Dateifreigabe.
    - **App-V-Dualverwaltung:** Veröffentlichen Sie die Pakete auf dem App-V-Verwaltungsserver über einen UNC-Pfad. (Die Veröffentlichung über HTTP-URLs wird nicht unterstützt.)
    - **MSIX-Pakete und mit dem MSIX-Feature zum Anfügen von Apps erstellte Pakete:** Speichern Sie die Pakete in einer UNC- oder SMB-Netzwerkfreigabe oder in einer Azure-Dateifreigabe.

3. Stellen Sie sicher, dass der VDA über Leseberechtigung für den Paketspeicherpfad verfügt:

    - Wenn Sie Pakete in einer UNC- oder SMB-Netzwerkfreigabe in Ihrer AD-Domäne speichern, erteilen Sie der VDA-Maschine die Leseberechtigung für den Speicherpfad. Dazu können Sie dem AD-Konto der Maschine explizit die Leseberechtigung für die Freigabe erteilen oder das Konto einer AD-Gruppe hinzufügen, die über diese Berechtigung verfügt.
    - Wenn Sie Pakete in einer Azure-Dateifreigabe speichern, erteilen Sie zunächst einem Benutzerkonto die Leseberechtigung für den Speicherpfad in Azure. Konfigurieren Sie als Nächstes `ctxAppVService` auf der VDA-Maschine so, dass es dieses Benutzerkonto für den Zugriff auf den Paketspeicherpfad verwendet. Die dafür erforderliche Schrittfolge ist im folgenden Abschnitt beschrieben.

#### Ändern des Benutzeranmeldekontos

Der VDA ruft `ctxAppVService` auf, um auf Paketspeicherpfade zuzugreifen. Standardmäßig greift `ctxAppVService` mit dem **lokalen Systemkonto** der Maschine auf Paketspeicherpfade zu. Diese Art der Maschinenauthentifizierung funktioniert in AD-Domänen. Sie funktioniert jedoch nicht in Szenarios mit AD- und Azure AD-Integration, die eine auf Benutzerkonten basierende Authentifizierung erfordern.

Wenn Sie Pakete in einer Azure-Dateifreigabe speichern, ändern Sie das Anmeldekonto für `ctxAppVService` in ein Benutzerkonto, das über Leseberechtigung für den Paketspeicherpfad verfügt. Verfahren:

1. Starten Sie **Dienste**, klicken Sie mit der rechten Maustaste auf **ctxAppVService**, und wählen Sie dann **Eigenschaften** aus.
2. Wählen Sie auf der Registerkarte **Anmelden** die Option **Dieses Konto** aus, geben Sie ein Benutzerkonto mit Leseberechtigung für den Paketspeicherpfad ein, und geben Sie dann das Kennwort des Benutzers zweimal ein.
3. Klicken Sie auf **OK**.

### Upload von Anwendungspaketen in Ihre Umgebung

Laden Sie die Anwendungspakete nach dem Speichern an einem Netzwerkspeicherort in Ihre Umgebung hoch, um sie bereitzustellen. Verwenden Sie nach Bedarf eine der folgenden Methoden:

- Massenupload
- Upload nacheinander

### Vorbereitungen

Citrix Virtual Apps and Desktops verwendet eine VDA-Maschine, um die Verbindung zum Netzwerkspeicherort für die Paketdiscovery einzurichten. Erstellen Sie daher vorher eine Bereitstellungsgruppe und stellen Sie sicher, dass mindestens ein VDA in der Gruppe die folgenden Anforderungen erfüllt:

- VDA-Version:
  - Ermitteln von App-V-Paketen: 2203 oder später
  - Ermitteln von MSIX-Paketen und von Paketen, die mit dem MSIX-Feature zum Anfügen von Apps erstellt wurden: 2209 oder später
- Citrix Personalisierung für App-V: installiert
- Berechtigung für den Paketspeicherort: Lesen (weitere Informationen siehe Schritt 2: Anwendungspakete in Netzwerkfreigaben speichern).
- Eingeschaltet: ja
- Zustand: registriert

### Massenupload von Anwendungspaketen

Laden Sie die Pakete vom Netzwerkspeicherort in Ihre Umgebung hoch. Stellen Sie vor dem Upload sicher, dass die folgenden Elemente bereit sind:

- Eine Bereitstellungsgruppe, die die Anforderungen an die Vorbereitung erfüllt
- Der Netzwerkstandortpfad

Gehen Sie beim Massenupload von Paketen folgendermaßen vor:

1. Wählen Sie im linken Bereich **App-Pakete** aus.
2. Klicken Sie auf der Registerkarte **Quellen** auf die Schaltfläche **Quelle hinzufügen**. Die Seite **Quelle hinzufügen** wird angezeigt.
3. Geben Sie im Feld **Name** einen aussagekräftigen Namen für die Quelle des Pakets ein.
4. Klicken Sie im Feld **Bereitstellungsgruppe** auf **Bereitstellungsgruppe wählen**. Wählen Sie als Nächstes eine Bereitstellungsgruppe aus, die die unter Vorbereitung angegebenen Anforderungen erfüllt, und klicken Sie dann auf **OK**.
5. Wählen Sie im Feld **Standorttyp** die Option **Microsoft App-V-Server** oder **Netzwerkfreigabe** aus, je nachdem, wo Sie die Pakete speichern, und legen Sie dann die entsprechenden Einstellungen fest:
   - Geben Sie bei Auswahl von **Microsoft App-V-Server** die folgenden Informationen ein:
     - URL des Verwaltungsservers. Beispiel:`http://appv-server.example.com`

  - Anmeldeinformationen des Verwaltungsserveradministrators.
  - URL und Portnummer des Veröffentlichungsservers. Beispiel:`http://appv-server.example.com:3330`
- Wenn Sie **Netzwerkfreigabe** ausgewählt haben, geben Sie die folgenden Informationen an:
  - Geben Sie den UNC-Pfad der Netzwerkfreigabe ein. Beispiel:`\\Package-Server\apps\`
  - Wählen Sie die Typen der Pakete aus, die Sie hochladen möchten. Es stehen die Optionen App-V, MSIX und MSIX App Attach zur Verfügung.
  - Geben Sie an, ob Unterordner nach Paketen durchsucht werden sollen.

6. Klicken Sie auf **Quelle hinzufügen**.

   Die Seite "Quelle hinzufügen"wird geschlossen und die neu hinzugefügte Quelle wird in der Liste der Quellen angezeigt. Citrix Virtual Apps and Desktops lädt die Pakete über einen VDA in der Bereitstellungsgruppe in Ihre Umgebung hoch. Nach Abschluss des Uploads wird im Statusfeld *Import war erfolgreich* angezeigt. Die entsprechenden Pakete werden auf der Registerkarte **Pakete** angezeigt.

   > **Hinweis:**
   >
   > Um an einem Quellspeicherort nach Paketupdates zu suchen und diese in Ihre Umgebung zu importieren, wählen Sie den Speicherort in der Quellliste aus, und klicken Sie auf **Nach Paketupdates suchen**.

#### Upload von Anwendungspaketen nacheinander

Laden Sie ein Anwendungspaket aus einer Netzwerkfreigabe in Ihre Umgebung hoch. Stellen Sie vor dem Upload sicher, dass die folgenden Elemente bereit sind:

- Eine Bereitstellungsgruppe, die die unter Vorbereitung angegebenen Anforderungen erfüllt
- Der Netzwerkstandortpfad

Gehen Sie folgendermaßen vor, um ein Paket in Ihre Umgebung hochzuladen:

1. Wählen Sie im linken Bereich **App-Pakete** aus.
2. Klicken Sie auf der Registerkarte **Pakete** auf die Schaltfläche **Paket hinzufügen**. Die Seite **Paket hinzufügen** wird angezeigt.
3. Klicken Sie im Feld **Bereitstellungsgruppe** auf **Bereitstellungsgruppe wählen**. Wählen Sie als Nächstes eine Bereitstellungsgruppe aus, die die unter Vorbereitung angegebenen Anforderungen erfüllt, und klicken Sie dann auf **OK**.
4. Geben Sie im Feld **Vollständiger Paketpfad** einen Pfad nach Bedarf ein:

- Um mehrere Pakete gleichzeitig hochzuladen, geben Sie deren vollständigen Pfad durch Semikolons (;) getrennt ein. Beispiel:`\\Package-Server\apps\office365.appv;\\Package-Server\apps\skype.msix;\\Package-Server\apps\slack.vhd`
- Um alle in einer Netzwerkfreigabe vorhandenen Pakete hochzuladen, geben Sie den Speicherpfad ein. Beispiel: \package-Server\apps\

5. Klicken Sie auf **Paket hinzufügen**.

   Das Anwendungspaket wird auf der Registerkarte **Pakete** angezeigt.

### Anwendungen zu Bereitstellungsgruppen hinzufügen

Fügen Sie die Anwendungen nach dem vollständigen Upload eines Anwendungspakets nach Bedarf einer oder mehreren Bereitstellungsgruppen hinzu. Benutzer, die diesen Bereitstellungsgruppen zugeordnet sind, können dann auf die Anwendungen zugreifen.

Gehen Sie folgendermaßen vor, um eine oder mehrere Anwendungen in einem Paket mehreren Bereitstellungsgruppen hinzuzufügen:

1. Wählen Sie im linken Bereich **App-Pakete** aus.
2. Wählen Sie auf der Registerkarte **Pakete** nach Bedarf ein Paket aus.
3. Klicken Sie in der Aktionsleiste auf **Bereitstellungsgruppen hinzufügen**. Die Seite “Bereitstellungsgruppen hinzufügen”wird angezeigt.
4. Wählen Sie nach Bedarf eine oder mehrere Anwendungen im Paket aus, und klicken Sie dann auf **Weiter**. Bereitstellungsgruppen mit dem Bereitstellungstyp *Anwendungen* werden angezeigt.
5. Wählen Sie in der Liste der Bereitstellungsgruppen die Gruppen aus, denen Sie die Anwendungen zuweisen möchten, und klicken Sie dann auf **Weiter**.
   **Hinweis:** Wenn Sie ein MSIX-Paket oder ein mit dem MSIX-Feature zum Anfügen von Apps erstelltes Paket ausgewählt haben, werden nur Bereitstellungsgruppen mit einer Funktionsebene ab 2106 in der Liste angezeigt.
6. Klicken Sie auf **Fertigstellen**.

Sie können einer Bereitstellungsgruppe auch in folgenden Situationen Anwendungspakete hinzufügen:

- Beim Erstellen einer Bereitstellungsgruppe. Weitere Informationen finden Sie unter Bereitstellungsgruppen erstellen.
- Beim Bearbeiten vorhandener Bereitstellungsgruppen oder Anwendungsgruppen. Weitere Informationen finden Sie unter Hinzufügen von Anwendungen.

### Isolationsgruppen für App-V-Pakete erstellen (optional)

Sie können Isolationsgruppen erstellen, um die automatische Bereitstellung voneinander abhängiger App-V-Pakete zu aktivieren.

> **Hinweis:**
>
> Isolationsgruppen werden für die App-V-Einzelverwaltungsmethode unterstützt. Wenn Sie die duale Verwaltung für App-V verwenden, können Sie dasselbe Ziel erreichen, indem Sie *Verbindungsgruppen* in der Microsoft App-V-Infrastruktur erstellen. Weitere Informationen finden Sie in folgendem Artikel der Microsoft-Dokumentation: https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-connection-group-file.

#### Info zu Isolationsgruppen

Eine Isolationsgruppe ist eine Sammlung voneinander abhängiger Anwendungspakete, die in derselben Windows Sandbox ausgeführt werden müssen, damit eine virtuelle Umgebung erstellt werden kann. Citrix App-V-Isolationsgruppen ähneln App-V-Verbindungsgruppen, sind jedoch nicht mit ihnen identisch. Eine Isolationsgruppe umfasst zwei Typen von Paketen:

- **Explizite** Anwendungspakete. Anwendungen mit spezifischen Lizenzanforderungen. Sie können diese Anwendungen auf einen bestimmten Kreis von Benutzern beschränken, indem Sie sie Bereitstellungsgruppen hinzufügen.
- **Automatische** Anwendungspakete. Anwendungen, die immer für alle Benutzer verfügbar sind, unabhängig davon, ob sie Bereitstellungsgruppen hinzugefügt wurden.

Beispiel: Anwendung app−a erfordert zur Ausführung JRE 1.7. Sie können eine Isolationsgruppe erstellen, die app-a (als *Explizit* gekennzeichnet) und JRE 1.7 (als *Automatisch* gekennzeichnet) enthält. Fügen Sie als Nächstes das App-V-Paket für app−a einer oder mehreren Bereitstellungsgruppen hinzu. Wenn ein Benutzer app-a startet, wird auch JRE 1.7 automatisch bereitgestellt.

Wenn ein Benutzer eine App-V-Anwendung startet, die in einer Isolationsgruppe als *Explizit* gekennzeichnet ist, überprüft Citrix Virtual Apps and Desktops die Zugriffsberechtigung des Benutzers auf die Anwendung in Bereitstellungsgruppen. Wenn der Benutzer über die Berechtigung zum Zugriff auf die Anwendung verfügt, werden dem Benutzer alle als *Automatisch* gekennzeichneten Anwendungspakete in derselben Isolationsgruppe zur Verfügung gestellt.

Die als *Automatisch* gekennzeichneten Pakete müssen Sie keiner Bereitstellungsgruppe hinzufügen. Wenn die Isolationsgruppe ein anderes *explizites* Anwendungspaket enthält, wird dieses Paket dem Benutzer nur dann zur Verfügung gestellt, wenn es sich in derselben Bereitstellungsgruppe befindet.

Weitere Informationen zu Isolationsgruppen finden Sie in diesem Citrix Blog.

**Erstellen von App-V-Isolationsgruppen** Erstellen Sie eine Isolationsgruppe und fügen Sie ihr voneinander abhängige Anwendungspakete hinzu. Verfahren:

1. Klicken Sie auf der Registerkarte **Isolationsgruppen** auf **Isolationsgruppe hinzufügen**.
2. Geben Sie einen Namen und eine Beschreibung für die Isolationsgruppe ein. Alle Anwendungspakete in Ihrer Umgebung werden in der Liste **Verfügbare Pakete** angezeigt.
3. Wählen Sie in der Liste **Verfügbare Pakete** nach Bedarf eine Anwendung aus, und klicken Sie dann auf den Pfeil nach rechts. Die ausgewählte Anwendung wird in der Liste **Pakete in Isolationsgruppe** angezeigt.
4. Wählen Sie im Feld **Bereitstellung** die Option **Explizit** oder **Automatisch** für die Anwendung aus.
5. Wiederholen Sie die Schritte 2—3, um weitere Pakete hinzuzufügen.
6. Um die Reihenfolge der Pakete in der Liste anzupassen, klicken Sie auf den Pfeil nach oben oder den Pfeil nach unten.
7. Klicken Sie auf **Speichern**.

> **Hinweis:**
>
> Isolationsgruppenkonfigurationen führen zur Erstellung einer App-V-Verbindungsgruppe auf dem VDA. Bereitstellungsszenarien können komplex sein, und der App-V-Client unterstützt Pakete, die sich jeweils nur in einer aktiven Verbindungsgruppe befinden. Es wird empfohlen, dasselbe Paket nicht zwei verschiedenen Isolationsgruppen hinzuzufügen, die derselben Bereitstellungsgruppe hinzugefügt werden.

## Anwendungspakete auf Einzelsitzungs- oder gemeinsam genutzten Desktop-VDAs veröffentlichen

Sie können App-V-, MSIX- und MSIX-Pakete zum Anfügen von Apps jetzt direkt über Bereitstellungsgruppen an Ihre Einzelsitzungen oder gemeinsam genutzten Desktop-VDA-Sitzungen bereitstellen. Sie können bei der Anmeldung je nach den Zugriffsberechtigungen, die für die Anwendungen festgelegt wurden, auf die Anwendungspakete auf Ihrem Desktop-VDA zugreifen.

### Vorteile

- Anwendungen sind bei der Anmeldung auf dem VDA verfügbar und werden nicht bei Bedarf über Workspace oder StoreFront bereitgestellt.
- Startzeit ist beim Zugriff auf die Anwendungspakete verkürzt.
- Die unabhängige Wartung der Anwendungspakete wird getrennt vom Basisimage des VDA erleichtert.

### Überlegungen

- Diese Option ist für Einzelsitzungs-VDAs nur über das entsprechende PowerShell-SDK verfügbar. Derzeit ist sie im Web Studio-Workflow nicht verfügbar. Das Veröffentlichen auf gemeinsam genutzten Desktops kann mit dem PowerShell SDK oder auf die bestehende Weise über den Web Studio-Workflow erfolgen. Weitere Informationen zum bestehenden Verfahren finden Sie unter Anwendungen zu Bereitstellungsgruppen hinzufügen.
- Anwendungen müssen Teil einer Bereitstellungsgruppe sein.

### Voraussetzungen

- Achten Sie darauf, dass die Anwendungspakete signiert und am Fileshare- oder UNC-Speicherort verfügbar sind. Weitere Informationen finden Sie unter Anwendungspakete auf Netzwerkfreigaben speichern.
- Installieren Sie die Komponenten von Citrix Personalization auf VDA-Maschinen.

### Verfahren

Gehen Sie folgendermaßen vor, um Anwendungspakete auf Desktop-VDAs bereitzustellen:

1. Importieren Sie Anwendungspakete in Web Studio.
2. Veröffentlichen Sie das BrokerApplication-Paket.
3. Beschränken Sie die Sichtbarkeit von Anwendungen in Web Studio.

### Anwendungspakete in Web Studio importieren

1. Öffnen Sie einen Webbrowser. Geben Sie `https://<address of the server hosting Web Studio>/Citrix/Studio` ein.
2. Erstellen Sie eine Bereitstellungsgruppe. Weitere Informationen finden Sie unter Bereitstellungsgruppen erstellen.
3. Importieren Sie die Anwendungspakete in Web Studio. Weitere Informationen finden Sie unter Massenupload von Anwendungspaketen.

### Anwendungspaket auf BrokerApplication veröffentlichen

Wenn Sie auf einem Mehrsitzungs-VDA (gemeinsam genutzt) oder auf einem Einzelsitzungs-Anwendungs-VDA veröffentlichen, bleibt das Veröffentlichungsverfahren unverändert. Weitere Informationen finden Sie unter Anwendungen zu Bereitstellungsgruppen hinzufügen.
Wenn Sie auf einem Einzelsitzung-Desktop-VDA veröffentlichen:

Führen Sie die folgenden PowerShell-Befehle auf dem Delivery Controller aus:

1. Gehen Sie wie folgt vor, um die im Paket enthaltenen Befehle abzurufen:

   ```
   Import-Module "D:\Support\Tools\Scripts\Citrix.Cloud.AppLibrary.
   Admin.v1.psm1"
   ```

   > **Hinweis:**
   >
   > Die Version von App-V **package** discovery module, die diese Funktion unterstützt, finden Sie in der Citrix Virtual Apps and Desktops-ISO (2311 oder höhere Versionen) im obigen Pfad.

2. Gehen Sie wie folgt vor, um die relevanten Bereitstellungsgruppen-IDs und die IDs der Anwendungspakete abzurufen:

   ```
   Get-BrokerDesktopGroup | Format-Table Uid, Name
   Get-AppLibAppVApplication | Format-Table Uid, Name
   ```

3. Gehen Sie wie folgt vor, um die Pakete zu veröffentlichen und die entsprechenden BrokerMachineConfigurations zu erstellen:

   ```
   Publish-PackagedApplication -AppLibararyApplicationUid <AppLibararyApplica
   .Uid > -DesktopGroupUid <DesktopGroup.Uid>
   ```

4. Gehen Sie wie folgt vor, um die Brokerkonfigurationen zu synchronisieren, die später an den Broker Agent auf dem VDA gesendet werden:

   ```
   Update-DesktopGroupMachineConfigurations -DesktopGroupUid <
   DesktopGroup.Uid>
   ```

   > **Hinweis:**
   >
   > Achten Sie darauf, dass Sie den PowerShell-Befehl `Update-DesktopGroupMachineConfiguratio` ausführen, nachdem Sie Anwendungspakete auf einem VDA veröffentlicht oder entfernt haben.

### Sichtbarkeit von Anwendungen in Web Studio beschränken

Standardmäßig stehen alle Anwendungspakete, die der Bereitstellungsgruppe Ihres VDAs zugewiesen sind, den Benutzern in ihrer Desktopsitzung zur Verfügung. Sie können die Sichtbarkeit von Anwendungspaketen auf den Desktop-VDAs steuern, indem Sie sie für bestimmte Benutzer oder Gruppen in Web Studio festlegen. Informationen zum Verwalten der Sichtbarkeit von Anwendungspaketen finden Sie unter Anwendungseigenschaften ändern.

# Apps für die Universelle Windows-Plattform

June 27, 2024

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.

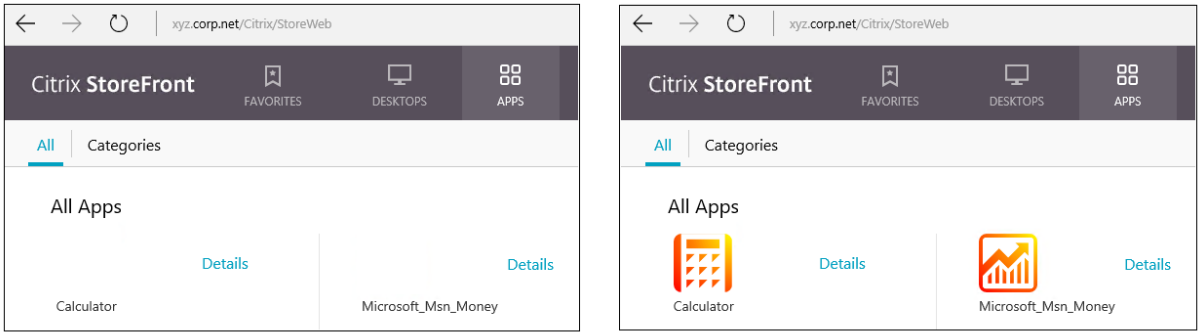
 

Eine ordnungsgemäße Abmeldung von einer veröffentlichten UWP-App, die in einem festen oder Seamlessfenster gestartet wurde, verhindert möglicherweise, dass die VDA-Sitzung geschlossen und der Benutzer zwangsweise abgemeldet wird. In diesem Fall verhindern mehrere in der VDA-Sitzung verbleibende Prozesse, 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 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 UWP-App möglicherweise auch der Server-Manager gestartet. Um dies zu verhindern, können Sie den automatischen Start des Server-Managers über den Registrierungsschlüssel `HKLM\Software\Microsoft\ServerManager\DoNotOpenServerManagerAtLogon` deaktivieren. Einzelheiten finden Sie unter `https://blogs.technet.microsoft.com/rmilne/2014/05/30/how-to-hide-server-manager-at-logon/`.

### 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.

Um die Verwendung universeller Apps auf einem VDA zu deaktivieren, fügen Sie die Registrierungseinstellung **EnableUWASeamlessSupport** in `HKLM\Software\Citrix\VirtualDesktopAgent\FeatureToggle` hinzu und legen Sie sie auf **0** fest.

### 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, führen Sie den Befehl zum Deinstallieren auf der jeweiligen Maschine aus. Sie können das AppX-Paket nicht mit einem Befehl von allen Maschinen der Benutzer deinstallieren.

## Autoscale

June 27, 2024

Autoscale ist ein Feature zur konsistenten und proaktiven Energieverwaltung Ihrer Maschinen. Es zielt auf eine Balance zwischen Kosten und Benutzererfahrung ab.

Autoscale ermöglicht die proaktive Energieverwaltung aller registrierten Maschinen mit Einzelsitzungs- und Multisitzungs-OS in einer Bereitstellungsgruppe.

Zu den Autoscalefeatures gehören folgende:

- Zeitplan- und Lasteinstellungen
- Dynamische Sitzungstimeouts
- Autoscale getaggte Maschinen (Cloudburst)
- Abmeldebenachrichtigungen für Benutzer

### Unterstützte VDA-Hostingplattformen

Autoscale unterstützt alle Plattformen, die Citrix Virtual Apps and Desktops unterstützt. Dazu gehören diverse Infrastrukturplattformen wie XenServer, Amazon Web Services, Google Cloud Platform, Microsoft Azure Resource Manager, VMware vSphere und viele mehr. Eine vollständige Liste der unterstützten Plattformen finden Sie unter Systemanforderungen für Citrix Virtual Apps and Desktops.

> **Hinweis:**
>
> Wenn Sie Verbindungen mit Hosts öffentlicher Clouds zu Ihrer Bereitstellung hinzufügen, benötigen Sie eine Hybrid Rights-Lizenz. Informationen zur Hybrid Rights-Lizenz finden Sie unter Transition und Trade-Up (TTU) mit Hybrid Rights. Informationen zum Hinzufügen einer Lizenz finden Sie unter Erstellen einer Site.

### Unterstützte Workloads

Autoscale unterstützt Multisitzungs-OS- und Einzelsitzungs-OS-Bereitstellungsgruppen. Es gibt drei relevante Benutzeroberflächen:

- Autoscale-Benutzeroberfläche für Multisitzungs-OS-Bereitstellungsgruppen:
- Autoscale-Benutzeroberfläche für zufällige (gepoolte) Einzelsitzungs-OS-Bereitstellungsgruppen (früher “gepoolte VDI-Bereitstellungsgruppen”)
- Autoscale-Benutzeroberfläche für statische Einzelsitzungs-OS-Bereitstellungsgruppen (bisher “statische VDI-Bereitstellungsgruppen”)

Weitere Hinweise zu den Benutzeroberflächen für verschiedene Bereitstellungsgruppen finden Sie unter Autoscale-Benutzeroberflächen.

### Vorteile

Das Autoscale-Feature bietet folgende Vorteile:

- Konsistenter Einzelmechanismus zur Verwaltung von Maschinen in einer Bereitstellungsgruppe
- Gewährleistung der Verfügbarkeit und Kostenkontrolle durch Energieverwaltung auf der Basis der Last, eines Zeitplans oder von beidem

- Zur Überwachung von Kennzahlen wie Kosteneinsparungen und Kapazitätsauslastung und Aktivierung von Benachrichtigungen verwenden Sie Director.

### Sehen Sie sich das 2-minütige Video an

Das folgende Video bietet einen kurzen Überblick über Autoscale.

Dies ist ein eingebettetes Video. Klicken Sie auf den Link, um das Video anzusehen

## Erste Schritte mit Autoscale

June 27, 2024

Autoscale funktioniert auf Bereitstellungsgruppenebene. Es ermöglicht die proaktive Energieverwaltung von Maschinen in einer Bereitstellungsgruppe nach von Ihnen festgelegten Zeitplänen.

Autoscale gilt für alle Typen von Bereitstellungsgruppen:

- Einzelsitzungs-OS (statisch)
- Einzelsitzungs-OS (zufällig)
- Multisitzungs-OS (zufällig)

In diesem Artikel werden die Grundkonzepte für Autoscale beschrieben und das Aktivieren und Konfigurieren von Autoscale für eine Bereitstellungsgruppe erläutert.

### Grundkonzepte

Betrachten Sie vor dem Start die folgenden Grundkonzepte in Autoscale:

- Zeitpläne
- Kapazitätspuffer
- Lastindex

#### Zeitpläne

Autoscale schaltet Maschinen in einer Bereitstellungsgruppe gemäß einem von Ihnen festgelegten Zeitplan ein und aus.

Ein Zeitplan enthält die Anzahl der aktiven Maschinen für jedes Zeitfenster, mit definierten Spitzen- und Nebenzeiten.

Zeitplaneinstellungen variieren je nach Typ der Bereitstellungsgruppe. Weitere Informationen:

- Multisitzungs-OS-Bereitstellungsgruppen
- Zufällige Einzelsitzungs-OS-Bereitstellungsgruppen
- Statische Einzelsitzungs-OS-Bereitstellungsgruppen

#### Kapazitätspuffer

Der Kapazitätspuffer dient zum Vorhalten freier Kapazität zur Berücksichtigung dynamischer Laststeigerungen. Es sind zwei Szenarien zu beachten:

- Bei Multisitzungs-OS-Bereitstellungsgruppen wird der Kapazitätspuffer als Prozentsatz der Gesamtkapazität der Bereitstellungsgruppe in Bezug auf den Lastindex definiert.
- Bei Bereitstellungsgruppen mit Einzelsitzungs-OS wird der Kapazitätspuffer als Prozentsatz der Gesamtanzahl von Maschinen in der Bereitstellungsgruppe definiert.

#### Lastindex

> **WICHTIG:**
>
> Der Lastindex gilt nur für Multisitzungs-OS-Bereitstellungsgruppen.

Der Lastindexwert legt fest, mit welcher Wahrscheinlichkeit eine Maschine Anmeldeanfragen von Benutzern empfängt. Er wird anhand der in der **Citrix Lastverwaltungsrichtlinie** konfigurierten Einstellungen für gleichzeitige Anmeldungen, Sitzungen, CPU, Datenträger und Speichernutzung berechnet.

Der Lastindex liegt zwischen 0 und 10.000. Standardmäßig gilt eine Maschine als voll ausgelastet, wenn sie 250 Sitzungen hostet.

- Die Ziffer “0”bedeutet, dass eine Maschine ohne Last ist. Eine Maschine mit einem Lastindexwert von 0 befindet sich bei einer Basislast.
- Die Ziffer “10.000”bedeutet, dass eine Maschine vollständig ausgelastet ist und keine weiteren Sitzungen ausführen kann.

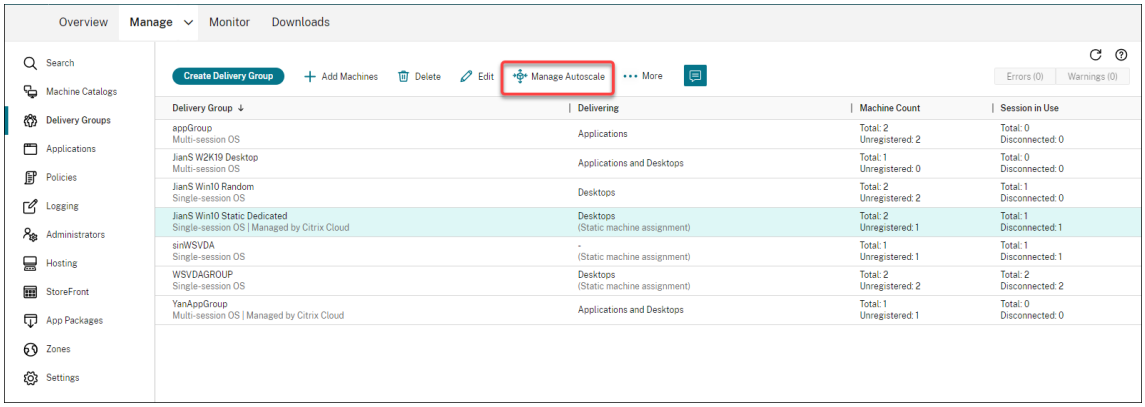
### Autoscale für eine Bereitstellungsgruppe aktivieren

Autoscale ist standardmäßig deaktiviert, wenn Sie eine Bereitstellungsgruppe erstellen. Führen Sie folgende Schritte aus, um Autoscale in Web Studio für eine Bereitstellungsgruppe zu aktivieren und zu konfigurieren:

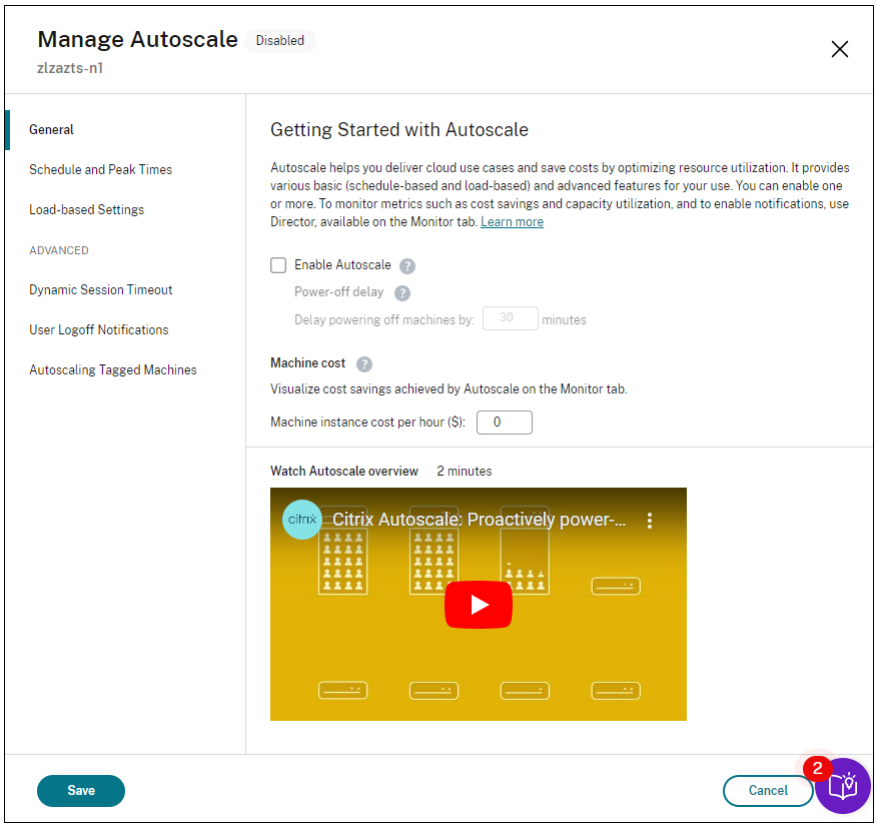
Sie können Autoscale auch mit PowerShell-Befehlen für eine Bereitstellungsgruppe aktivieren und konfigurieren. Weitere Informationen finden Sie unter Broker PowerShell SDK-Befehle.

1. Wählen Sie im linken Bereich **Bereitstellungsgruppen**.
2. Wählen Sie die Bereitstellungsgruppe aus, die Sie verwalten möchten, und klicken Sie auf **Autoscale verwalten**.




3. Aktivieren Sie auf der Seite **Autoscale verwalten** das Kontrollkästchen **Autoscale aktivieren**, um das Feature zu aktivieren. Nachdem Sie Autoscale aktiviert haben, werden die Optionen auf der Seite verfügbar.




4. Um die Standardeinstellungen an die Anforderungen Ihres Unternehmens anzupassen, führen Sie die folgenden Einstellungen aus:

   - Zeitpläne festlegen

- Um inaktive Maschinen effektiver auszuschalten, verwenden Sie Dynamisches Sitzungstimeout und Benachrichtigungen zur Benutzerabmeldung.
- Um die Energieverwaltung nur für einen Teil der Maschinen in der Bereitstellungsgruppe durchzuführen, verwenden Sie Autoscale getaggte Maschinen.

Zum Deaktivieren des Features deaktivieren Sie das Kontrollkästchen **Autoscale**. Die Optionen auf der Seite werden grau angezeigt, sodass zu sehen ist, dass Autoscale für die ausgewählte Bereitstellungsgruppe deaktiviert ist.

> **Wichtig:**
>
> - Wenn Sie Autoscale deaktivieren, verbleiben alle über Autoscale verwalteten Maschinen in dem zum Zeitpunkt der Deaktivierung aktiven Zustand.
> - Nachdem Sie Autoscale deaktiviert haben, werden Maschinen im Drainingzustand aus diesem genommen. Weitere Hinweise zum Drainingzustand finden Sie unter Drainingzustand.

### Metriken überwachen

Nachdem Sie Autoscale für eine Bereitstellungsgruppe aktiviert haben, können Sie für die mit Autoscale verwalteten Maschinen folgende Kennzahlen aus Director erfassen.

- Maschinennutzung
- Geschätzte Einsparungen
- Warnmeldungsbenachrichtigungen für Maschinen und Sitzungen
- Maschinenstatus
- Lastauswertungstrends

> **Hinweis:**
>
> Wenn Sie die automatische Skalierung für eine Bereitstellungsgruppe anfänglich aktivieren, kann es einige Minuten dauern, bis Überwachungsdaten für diese Bereitstellungsgruppe angezeigt werden.
> Wird Autoscale anschließend wieder deaktiviert, sind die Überwachungsdaten weiterhin verfügbar. Autoscale erfasst Überwachungsdaten in Intervallen von 5 Minuten.

Weitere Informationen zu Metriken finden Sie unter Überwachen von mit Autoscale verwalteten Maschinen.

## Nützliche Info

Autoscale funktioniert auf Bereitstellungsgruppenebene. Es wird für einzelne Bereitstellungsgruppen konfiguriert. Autoscale verwaltet nur die Maschinen in der ausgewählten Bereitstellungsgruppe.

### Kapazität und Maschinenregistrierung

Autoscale enthält nur Maschinen, die beim Bestimmen der Kapazität in einer Site registriert sind. Eingeschaltete Maschinen, die nicht registriert sind, können keine Sitzungsanfragen annehmen. Daher werden sie nicht in die Gesamtkapazität der Bereitstellungsgruppe einbezogen.

### Einsatz mehrerer Maschinenkataloge

Bei manchen Sites sind einer Bereitstellungsgruppe mehrere Maschinenkataloge zugeordnet. Autoscale schaltet Maschinen aus jedem Katalog nach dem Zufallsprinzip ein, um die Zeitplan- bzw. die Sitzungsanforderungen zu erfüllen.

Beispiel: Eine Bereitstellungsgruppe hat zwei Maschinenkataloge, Katalog A mit drei eingeschalteten Maschinen und Katalog B mit einer eingeschalteten Maschine. Wenn Autoscale eine weitere Maschine einschalten muss, kann es eine aus Katalog A oder Katalog B einschalten.

### Maschinenbereitstellung und Sitzungsbedarf

Der einer Bereitstellungsgruppe zugeordnete Maschinenkatalog muss über genügend Maschinen zum Ein- und Ausschalten bei steigendem und sinkendem Bedarf verfügen. Überschreitet der Sitzungsbedarf die Gesamtzahl der registrierten Maschinen in einer Bereitstellungsgruppe stellt Autoscale sicher, dass alle registrierten Maschinen eingeschaltet werden. **Autoscale stellt jedoch keine zusätzlichen Maschinen bereit.**

### Instanzgröße

Sie können Ihre Kosten optimieren, wenn Sie die Größe Ihrer Instanzen in öffentlichen Clouds passend festlegen. Wir empfehlen die Bereitstellung kleinerer Instanzen, sofern diese Ihren Workload-, Leistungs- und Kapazitätsanforderungen entsprechen.

Kleinere Instanzen hosten weniger Benutzersitzungen als größere. Daher versetzt Autoscale Maschinen viel schneller in den Drainingzustand , da die Abmeldung der letzten Benutzersitzung schneller erfolgt. Kleinere Instanzen werden somit schneller ausgeschaltet, wodurch die Kosten gesenkt werden.

**Drainingzustand**

Autoscale versucht, die Anzahl der eingeschalteten Maschinen in einer Bereitstellungsgruppe auf die konfigurierte Poolgröße und den Kapazitätspuffer zu beschränken.

Um dies zu erreichen, versetzt Autoscale die überzähligen Maschinen mit den wenigsten Sitzungen in den "Drainingzustand"und schaltet sie aus, sobald alle Sitzungen abgemeldet sind. Dies ist der Fall, wenn der Sitzungsbedarf sinkt und laut Zeitplan weniger Maschinen benötigt werden, als eingeschaltet sind.

Autoscale versetzt überzählige Maschinen nacheinander in den Drainingzustand .

- Sind auf mehren Maschinen gleich viele Sitzungen aktiv, wird die Maschine in den Drainingzustand versetzt, die für die als Ausschaltverzögerung vorgegebene Zeitdauer eingeschaltet war.

  Dadurch wird vermieden, dass kürzlich eingeschaltete Maschinen in den Drainingzustand versetzt werden, da auf ihnen am ehesten weniger Sitzungen aktiv sind.
- Waren mehre Maschinen für die als Ausschaltverzögerung vorgegebene Zeitdauer eingeschaltet, werden sie von Autoscale nach dem Zufallsprinzip einzeln in den Drainingzustand versetzt.

Maschinen im Drainingzustand nehmen keine neuen Sitzungen an und warten auf die Abmeldung bestehender Sitzungen. Es werden nur Maschinen zum Abschalten in Betracht gezogen, wenn alle Sitzungen abgemeldet sind. Stehen keine Maschinen sofort für Sitzungsstarts zur Verfügung, werden Sitzungsstarts von Autoscale bevorzugt an Maschinen im Drainingzustand weitergeleitet, anstatt neue Maschinen einzuschalten.

Eine Maschine wird aus dem Drainingzustand genommen, wenn eine der folgenden Bedingungen erfüllt ist:

- Die Maschine ist ausgeschaltet.
- Autoscale ist für die Bereitstellungsgruppe deaktiviert, zu der die Maschine gehört.
- Autoscale verwendet die Maschine, um die Anforderungen an den Zeitplan oder den Lastbedarf zu erfüllen. Dieser Fall tritt auf, wenn der Zeitplan (planbasierte Skalierung) oder der aktuelle Bedarf (lastbasierte Skalierung) mehr Maschinen benötigt, als derzeit eingeschaltet sind.

> **Wichtig:**
>
> Stehen keine Maschinen sofort für Sitzungsstarts zur Verfügung, werden Sitzungsstarts von Autoscale bevorzugt an Maschinen im Drainingzustand weitergeleitet, anstatt neue Maschinen einzuschalten. Eine Maschine im Drainingzustand, die einen Sitzungsstart hostet, bleibt im Drainingzustand.

Mit dem PowerShell-Befehl `Get-BrokerMachine` können Sie herausfinden, welche Maschinen im Drainingzustand sind. Beispiel: `Get-BrokerMachine -DrainingUntilShutdown $true`.

Alternativ können Sie die Verwaltungskonsole verwenden. Siehe Anzeigen von Maschinen im Drainingzustand.

### Anzeigen von Maschinen im Drainingzustand

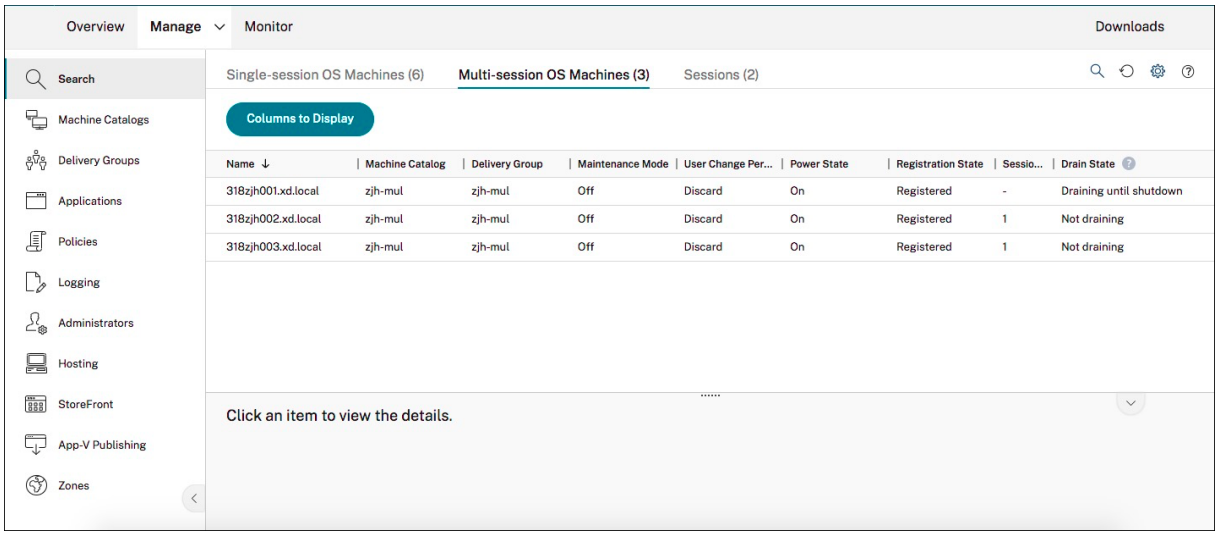
> **Hinweis:**
>
> Dieses Feature gilt nur für Multisitzungsmaschinen.

In Web Studio können Sie Maschinen im Drainingzustand anzeigen und sehen, welche Maschinen vor dem Herunterfahren stehen. Führen Sie hierzu die folgenden Schritte aus:

1. Navigieren Sie zum Knoten **Suchen** und klicken Sie auf **Anzuzeigende Spalten**.
2. Wählen Sie im Fenster **Anzuzeigende Spalten** das Kontrollkästchen neben **Drainingzustand**.
3. Klicken Sie auf **Speichern**, um das Fenster **Anzuzeigende Spalten** zu schließen.

Die Spalte **Drainingzustand** kann die folgenden Informationen enthalten:

- **Draining bis zum Herunterfahren:** Diese Meldung erscheint für Maschinen im Drainingzustand, bis sie heruntergefahren werden.
- **Nicht Draining:** Diese Meldung erscheint für Maschinen, die noch nicht im Draining sind.




## Weitere Informationen

Weitere Hinweise zu Autoscale finden Sie unter Citrix Autoscale auf Tech Zone.

# Zeitplan- und Lasteinstellungen

June 27, 2024

## Energieverwaltung von Maschinen durch Autoscale

Autoscale schaltet Maschinen basierend auf dem ausgewählten Zeitplan ein und aus. Über Autoscale können Sie mehrere Zeitpläne, z. B. für bestimmte Wochentage, festlegen und die Anzahl der während dieser Zeiten verfügbaren Maschinen vorgeben. Benutzergruppen, die Maschinenressourcen zu einem bestimmten Zeitpunkt an bestimmten Tagen nutzen kann mit Autoscale so eine optimales Benutzererfahrung geboten werden. Maschinen bleiben während des Zeitplans eingeschaltet, unabhängig davon, ob auf ihnen Sitzungen ausgeführt werden.

> **Hinweis:**
>
> AutoScale unterstützt jede energieverwaltete Maschine.

Der Zeitplan basiert auf der **Zeitzone** der Bereitstellungsgruppe. Zum Ändern der Zeitzone können Sie Benutzereinstellungen in einer Bereitstellungsgruppe ändern. Weitere Informationen finden Sie unter Bereitstellungsgruppen verwalten.

Autoscale hat zwei Standardzeitpläne: *Werktage* (Montag bis Freitag) und *Wochenende* (Samstag und Sonntag). Beim Zeitplan **Werktage** ist zu Spitzenzeiten eine Maschine von 7:00 Uhr bis 18:30 Uhr und zu Nebenzeiten keine Maschine eingeschaltet. Der Standardwert für den Kapazitätspuffer ist 10 % in Spitzen- und Nebenzeiten. Beim Zeitplan **Wochenende** ist standardmäßig keine Maschine eingeschaltet.

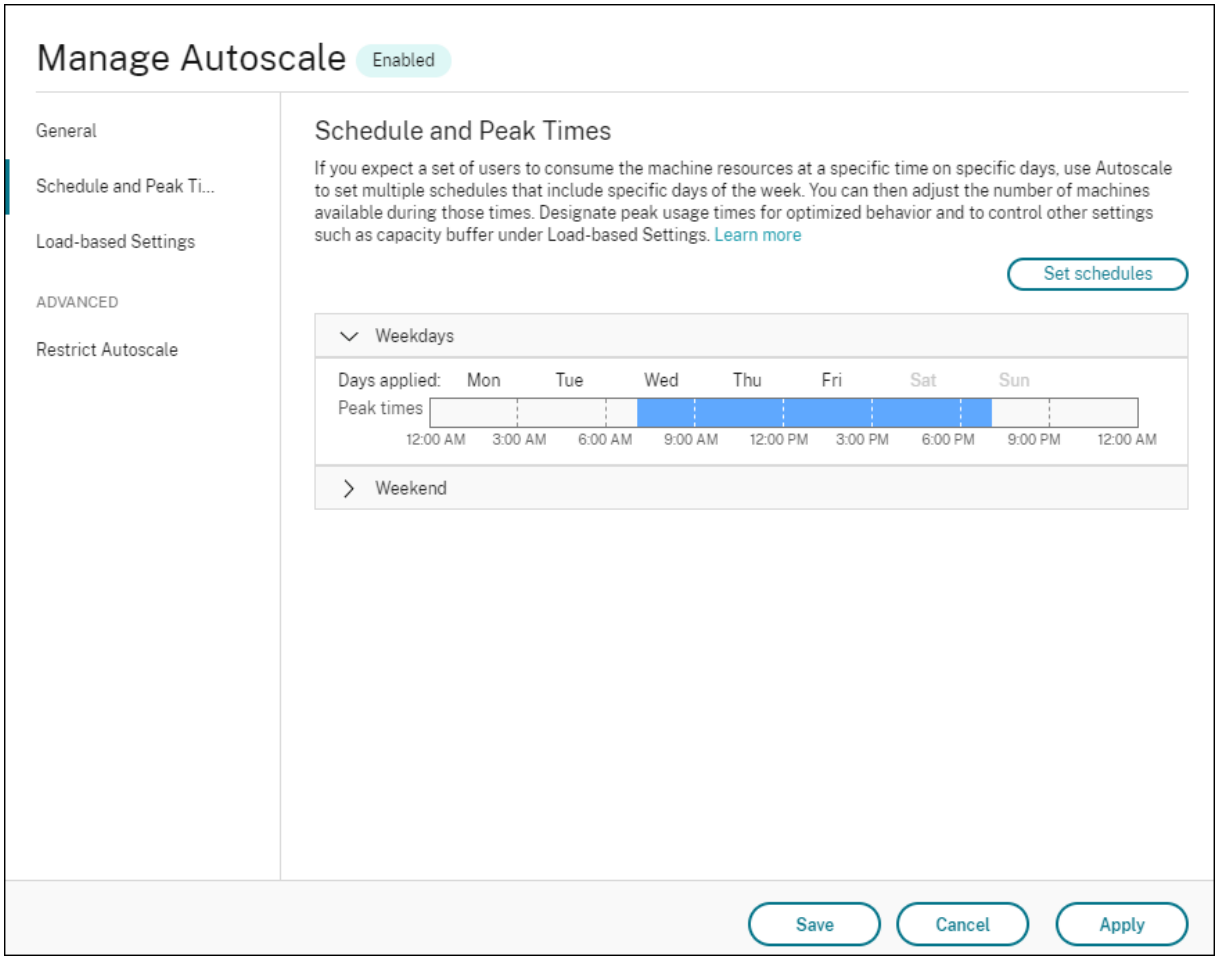
> **Hinweis:**
>
> Autoscale behandelt in seiner Kalkulation nur in der Site registrierte Maschinen als Teil der verfügbaren Kapazität. "Registriert"bedeutet, dass eine Maschine einsatzbereit oder bereits im Einsatz ist. Dadurch wird sichergestellt, dass nur Maschinen, die Benutzersitzungen annehmen können, zur Kapazität für die Bereitstellungsgruppe gezählt werden.

## Benutzeroberflächen

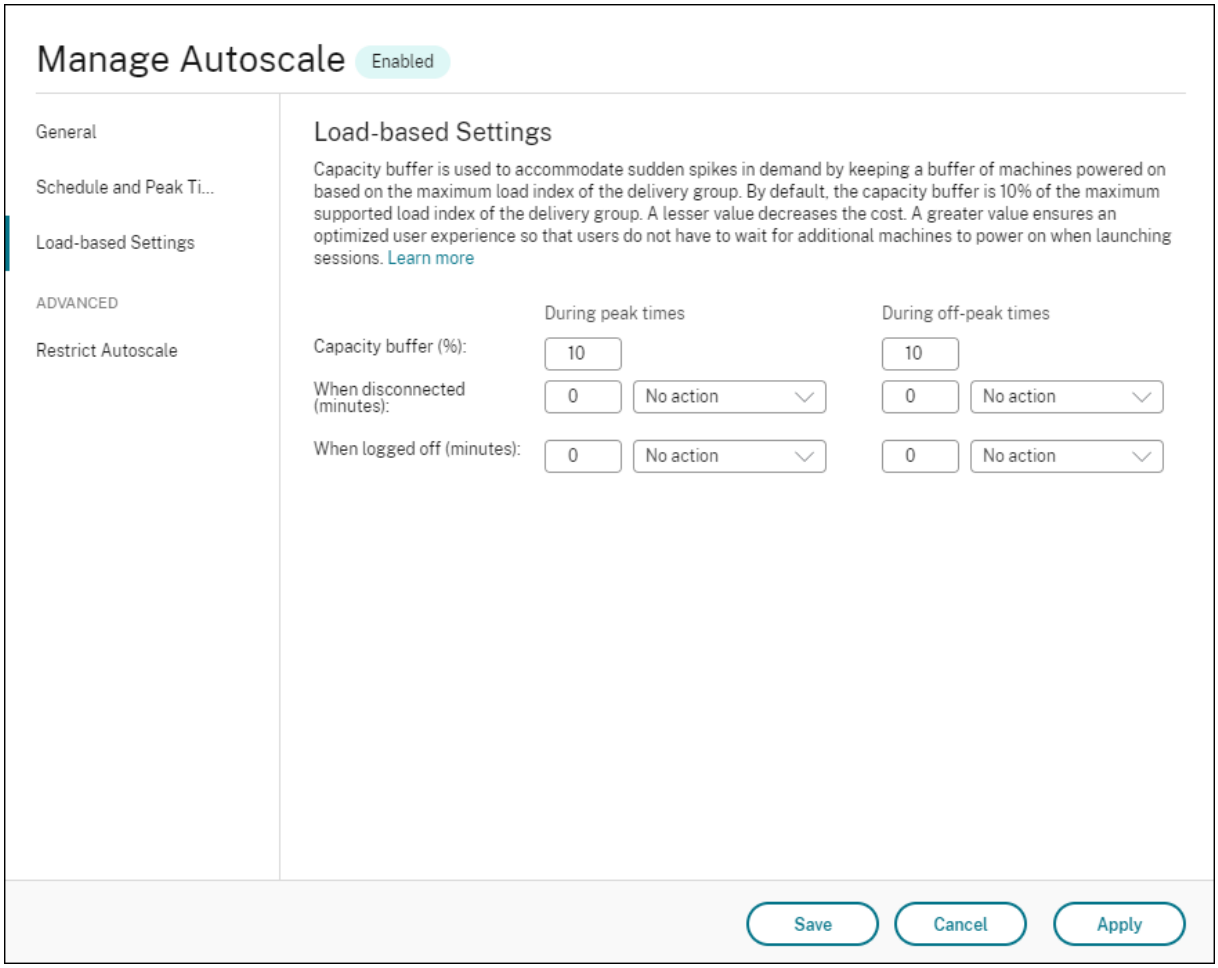
Es gibt drei Benutzeroberflächen.

Benutzeroberfläche für *statische* Einzelsitzungs-OS-Bereitstellungsgruppen:

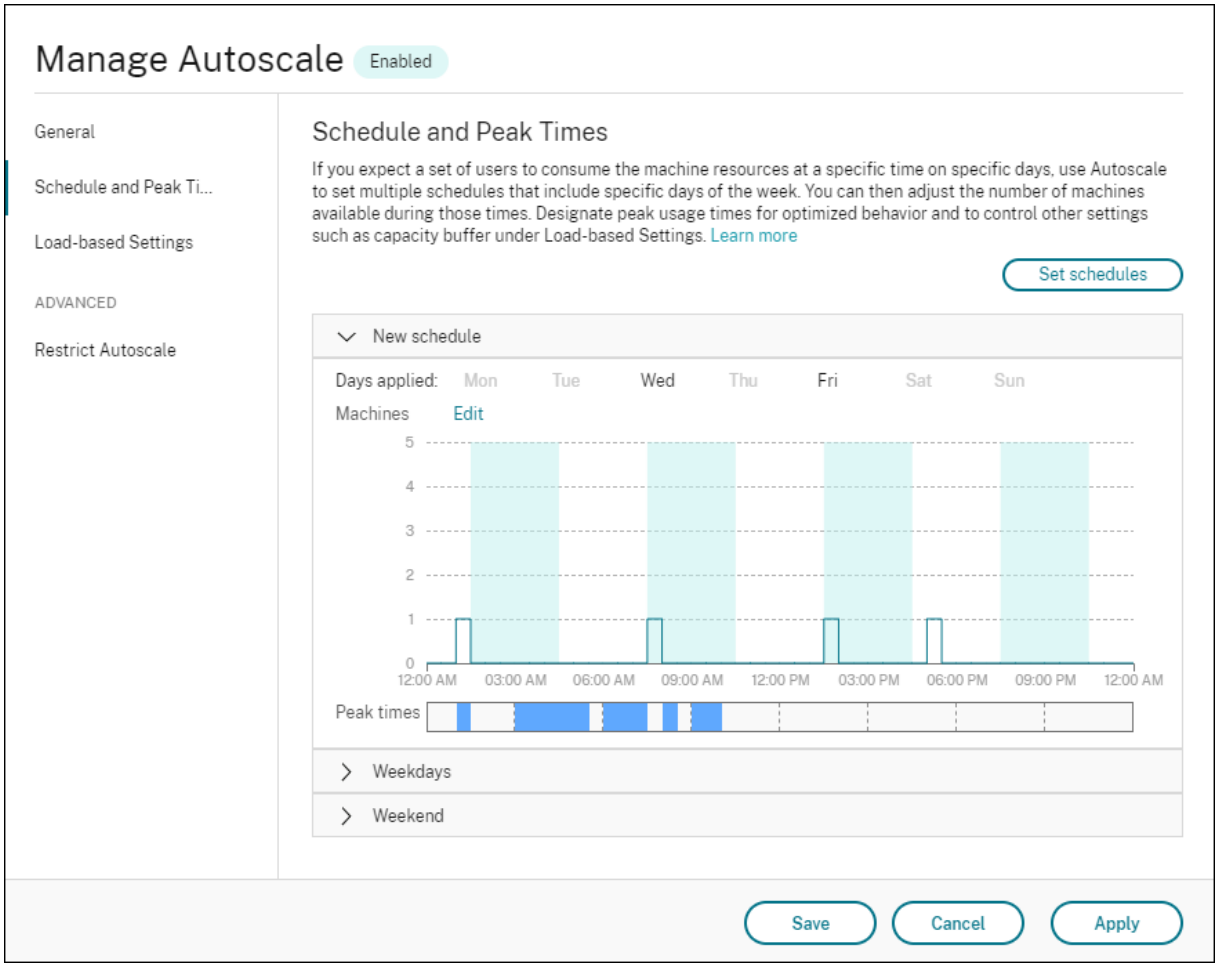


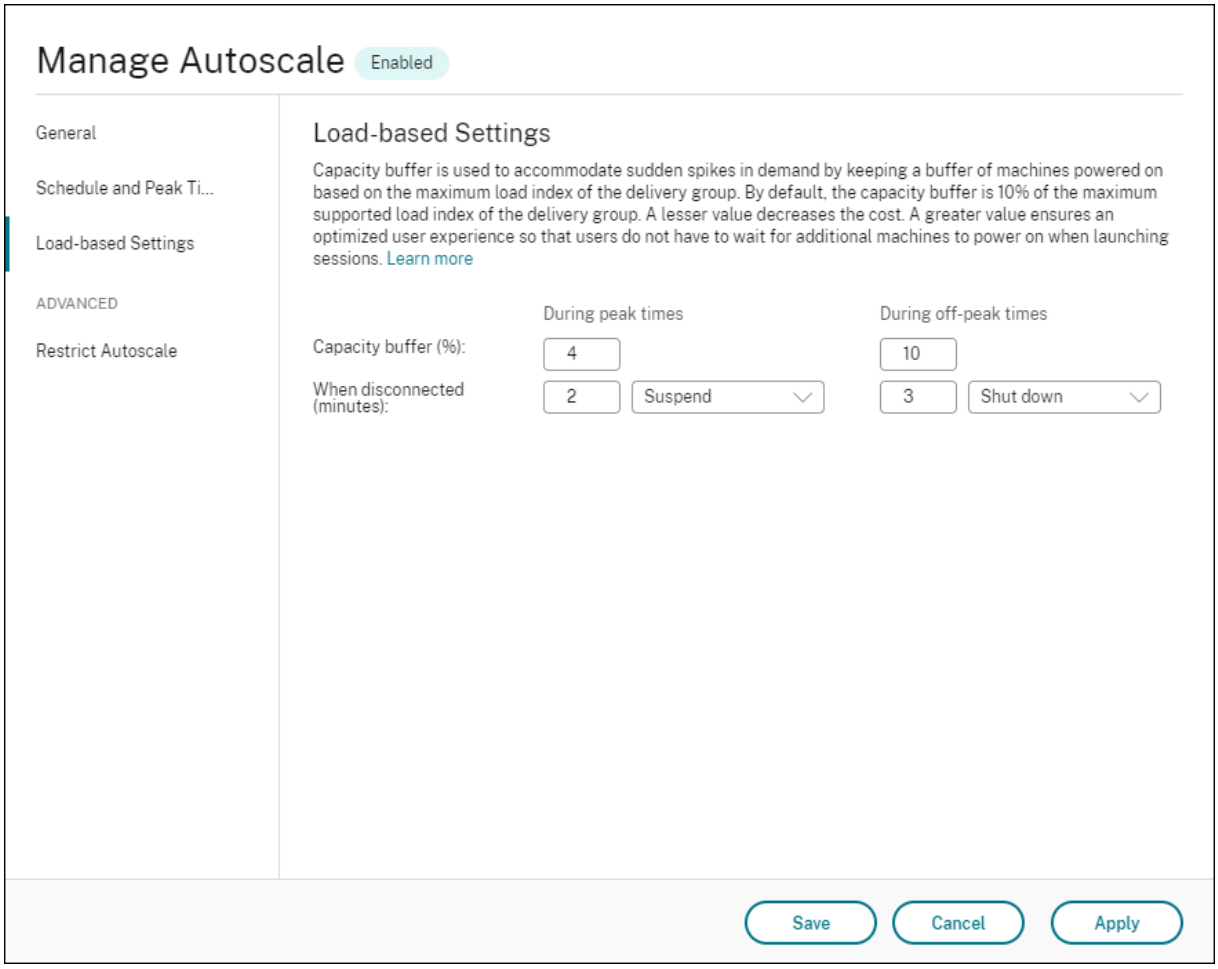



Autoscale-Benutzeroberfläche für *zufällige Einzelsitzungs-OS-Bereitstellungsgruppen*:

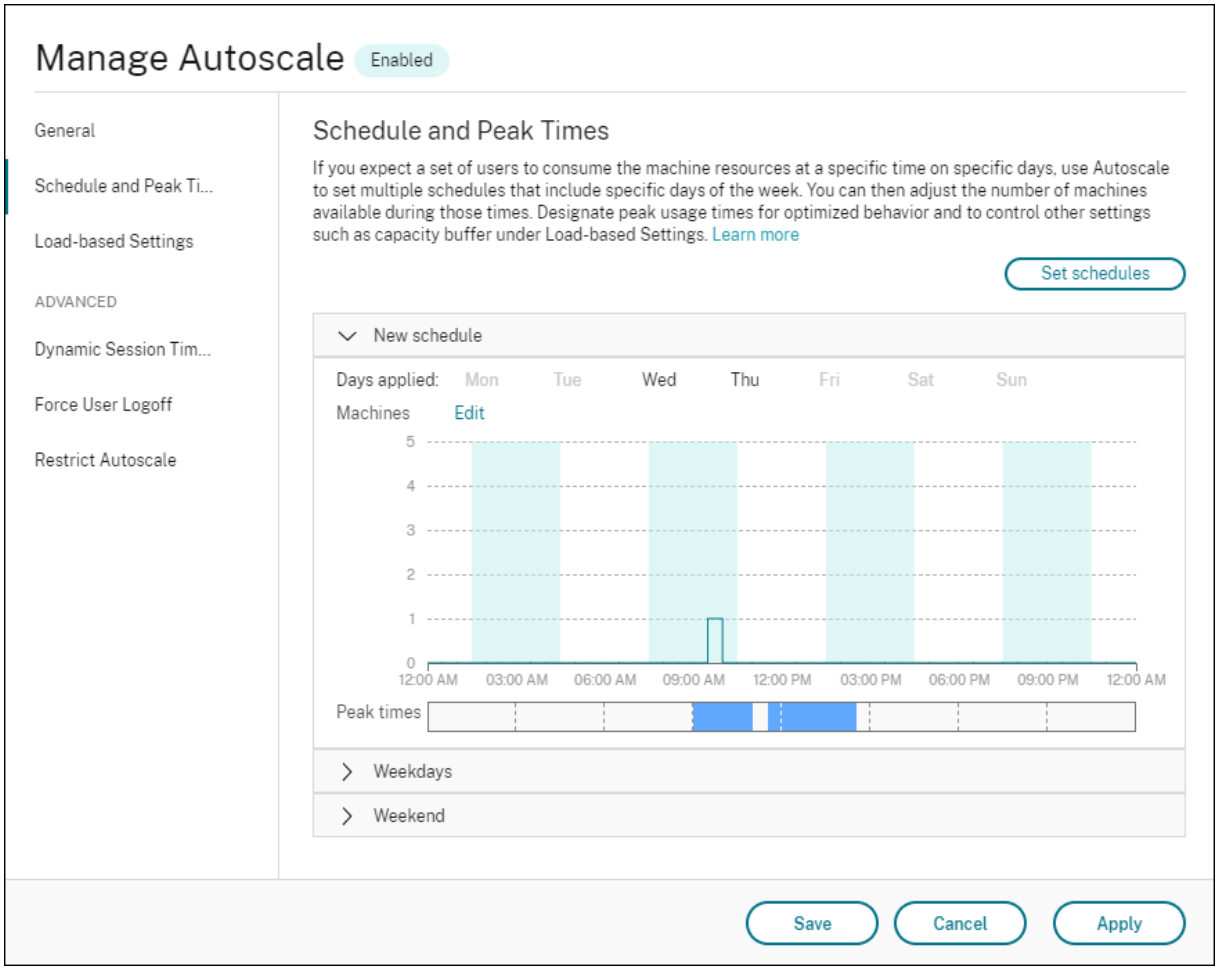


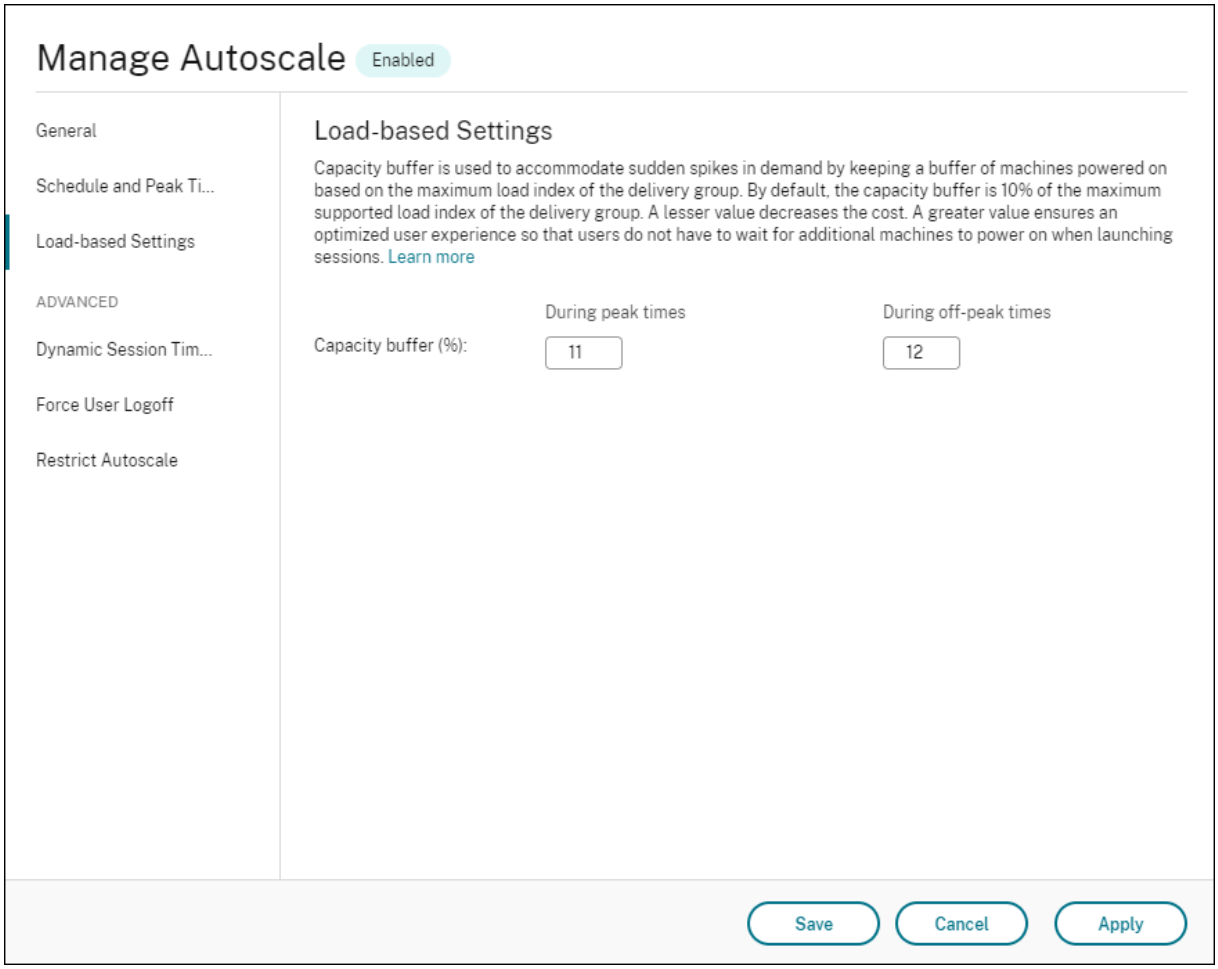



Autoscale-Benutzeroberfläche für *Multisitzungs-OS-Bereitstellungsgruppen*:






### Zeitplanbasierte Einstellungen

**Autoscale-Zeitplan:** Ermöglicht das Hinzufügen, Bearbeiten, Auswählen und Löschen von Zeitplänen.

**Angewendete Tage:** Zur Auswahl der Tage, auf die der ausgewählten Zeitplan angewendet wird. Die restlichen Tage sind ausgegraut.

**Bearbeiten:** Ermöglicht die Zuweisung der Maschinen für jede Stunde oder jede halbe Stunde. Sie können Maschinen nach Zahl oder Prozentsatz zuordnen.

> **Hinweis:**
>
> - Diese Option ist nur in den Autoscale-Benutzeroberflächen für Multisitzungs-OS-Bereitstellungsgruppen und für zufällige Einzelsitzungs-OS-Bereitstellungsgruppen verfügbar.
> - Das Histogramm neben **Bearbeiten** stellt die Anzahl oder den Prozentsatz der Maschinen dar, die in verschiedenen Zeitfenstern ausgeführt werden.

- Sie können **Maschinen jedem Zeitfenster zuweisen**, indem Sie oberhalb von **Spitzenzeiten** auf **Bearbeiten** klicken. Abhängig von der Option, die Sie aus dem Menü im Fenster **Zu startende Maschinen** ausgewählt haben, können Sie Maschinen nach Zahl oder Prozentsatz zuweisen.
- Für Multisitzungs-OS-Bereitstellungsgruppen können Sie die Mindestanzahl ausgeführter Maschinen für alle 30 Minuten separat festlegen. Für Einzelsitzungs-OS-Bereitstellungsgruppen können Sie die Mindestanzahl ausgeführter Maschinen für alle 60 Minuten separat festlegen.

Um eigene Zeitpläne zu definieren, führen Sie die folgenden Schritte aus:

1. Klicken Sie auf der Seite **Zeitplan und Spitzenzeiten** des Fensters **Autoscale verwalten** auf **Zeitpläne festlegen**.
2. Wählen Sie im Fenster **Autoscale-Zeitpläne bearbeiten** die Tage aus, die Sie jedem Plan zuordnen möchten. Sie können bei Bedarf auch Zeitpläne löschen.
3. Klicken Sie auf **Fertig stellen**, um die Zeitpläne zu speichern und zur Seite **Zeitplan und Spitzenzeiten** zurückzukehren.
4. Wählen Sie den gewünschten Zeitplan aus und konfigurieren Sie ihn.
5. Klicken Sie auf **Anwenden**, um das Fenster **Autoscale verwalten** zu schließen oder konfigurieren Sie Einstellungen auf anderen Seiten.

**Wichtig:**

- Eine Überlappung von Zeitplänen am selben Tag ist nicht zulässig. Wenn Sie beispielsweise Montag in Zeitplan2 auswählen, nachdem Sie Montag in Zeitplan1 ausgewählt haben, wird Montag in Zeitplan1 automatisch gelöscht.
- Bei Zeitplannamen spielt die Groß- und Kleinschreibung keine Rolle.
- Ein Zeitplanname darf nicht leer sein oder nur Leerzeichen enthalten.
- Leerzeichen zwischen den Zeichen sind zulässig.
- Ein Zeitplanname darf die folgenden Zeichen nicht enthalten: \ / ; : # . * ? = < > | [ ] ( ) { } ‘“‘.
- Autoscale unterstützt keine mehrfach vorkommenden Zeitplannamen. Geben Sie für jeden Zeitplan einen anderen Namen ein.
- Leere Zeitpläne werden nicht unterstützt. Das bedeutet, dass Zeitpläne ohne ausgewählte Tage nicht gespeichert werden.

**Hinweis:**

Die im ausgewählten Zeitplan enthaltenen Tage hervorgehoben und die nicht enthaltenen Tage ausgegraut dargestellt.

### Lastbasierte Einstellungen

**Spitzenzeiten:** Hier können Sie die Spitzenzeiten für die Tage im ausgewählten Zeitplan definieren. Klicken Sie hierzu mit der rechten Maustaste auf das horizontale Balkendiagramm. Nachdem Sie die Spitzenzeiten gewählt haben, werden die verbleibenden, nicht gewählten Zeiten standardmäßig als Nebenzeiten behandelt. **Standardmäßig** gilt der Zeitraum von 7:00 bis 19:00 Uhr als Spitzenzeit für die Tage im ausgewählten Zeitplan.

> **Wichtig:**
>
> - Bei Multisitzungs-OS-Bereitstellungsgruppen wird das Balkendiagramm der Spitzenzeiten für den Kapazitätspuffer verwendet.
> - Bei Einzelsitzungs-OS-Bereitstellungsgruppen wird das Balkendiagramm der Spitzenzeiten für den Kapazitätspuffer verwendet und steuert die Aktionen, die nach Abmeldung und/oder Trennung ausgelöst werden sollen.
> - Sie können für Multisitzungs-OS- und Einzelsitzungs-OS-Bereitstellungsgruppen die Spitzenzeiten für die Tage in einem Zeitplan auf einer Detailebene von 30 Minuten definieren. Alternativ können Sie stattdessen den Befehl `New-BrokerPowerTimeScheme` `PowerShell` verwenden. Weitere Informationen finden Sie unter Broker PowerShell SDK-Befehle.

**Kapazitätspuffer:** Ermöglicht den Betrieb eines Puffers eingeschalteter Maschinen. Ein geringerer Wert senkt die Kosten. Ein höherer Wert sorgt für eine optimale Benutzererfahrung, da die Benutzer beim Starten von Sitzungen nicht auf das Einschalten zusätzlicher Maschinen warten müssen. Standardmäßig beträgt der Kapazitätspuffer 10 % in Spitzen- und Nebenzeiten. Wenn Sie den Kapazitätspuffer auf 0 setzen, müssen die Benutzer beim Starten von Sitzungen evtl. warten, bis zusätzliche Maschinen hochgefahren sind. In Autoscale können Sie den Kapazitätspuffer für Spitzen- und Nebenzeiten separat festlegen.

### Sonstige Einstellungen

> **Tipp:**
>
> - Sie können die sonstigen Einstellungen mit dem Broker PowerShell SDK konfigurieren. Weitere Informationen finden Sie unter Broker PowerShell SDK-Befehle.
> - Informationen zu den SDK-Befehlen, die mit den Einstellungen "Wenn getrennt"und "Wenn abgemeldet"verknüpft sind, finden Sie unter https://citrix.github.io/delivery-controller-sdk/Broker/about_Broker_PowerManagement/#power-policy.

**Wenn getrennt:** Hier können Sie festlegen, wie lange eine getrennte, gesperrte Maschine nach dem Trennen der Sitzung eingeschaltet bleibt, bevor sie angehalten oder heruntergefahren wird. Wenn ein

Zeitwert angegeben wird, wird die Maschine nach Verstreichen dieser Zeit abhängig von der von Ihnen konfigurierten Aktion angehalten oder heruntergefahren. Standardmäßig ist getrennten Maschinen keine Aktion zugewiesen. Sie können für Spitzen- und Nebenzeiten separate Aktionen definieren. Klicken Sie dazu auf den Abwärtspfeil und wählen Sie eine der folgenden Optionen:

- **Keine Aktion**. Die Maschine bleibt nach der Sitzungstrennung eingeschaltet. Es erfolgt keine Aktion durch Autoscale.
- **Anhalten.** Die Maschine wird nach Ablauf der vorgegebenen Zeit automatisch angehalten, jedoch nicht abgeschaltet. Die folgende Option wird verfügbar, nachdem Sie **Anhalten**ausgewählt haben.
  - **Wenn keine erneute Verbindung in (Minuten)**. Angehaltene Maschinen stehen zur Wiederverbindung durch getrennte Benutzer zur Verfügung, jedoch nicht für neue Benutzer. Um Maschinen für alle Workloads wieder verfügbar zu machen, fahren Sie sie herunter. Geben Sie das Timeout in Minuten an, nach dessen Ablauf Autoscale sie herunterfährt.
- **Herunterfahren**. Die Maschine wird nach Ablauf der vorgegebenen Zeit heruntergefahren.

> **Hinweis:**
>
> Diese Option ist nur in den Autoscale-Benutzeroberflächen für Multisitzungs-OS-Bereitstellungsgruppen und für zufällige Einzelsitzungs-OS-Bereitstellungsgruppen verfügbar.

**Wenn abgemeldet:** Hier können Sie festlegen, wie lange eine Maschine nach der Abmeldung der Sitzung eingeschaltet bleibt, bevor sie angehalten oder heruntergefahren wird. Wenn ein Zeitwert angegeben wird, wird die Maschine nach Verstreichen dieser Zeit abhängig von der von Ihnen konfigurierten Aktion angehalten oder heruntergefahren. Standardmäßig ist abgemeldeten Maschinen keine Aktion zugewiesen. Sie können für Spitzen- und Nebenzeiten separate Aktionen definieren. Klicken Sie dazu auf den Abwärtspfeil und wählen Sie eine der folgenden Optionen:

- **Keine Aktion**. Die Maschine bleibt nach der Sitzungsabmeldung eingeschaltet. Es erfolgt keine Aktion durch Autoscale.
- **Anhalten.** Die Maschine wird nach Ablauf der vorgegebenen Zeit automatisch angehalten, jedoch nicht abgeschaltet.
- **Herunterfahren**. Die Maschine wird nach Ablauf der vorgegebenen Zeit heruntergefahren.

> **Hinweis:**
>
> Diese Option ist nur in der Autoscale-Benutzeroberfläche für statische Einzelsitzungs-OS-Bereitstellungsgruppen verfügbar.

**Energieverwaltung von Einzelsitzungs-OS-Maschinen beim Übergang in einen anderen Zeitraum mit getrennten Sitzungen**

> **Wichtig:**
>
> - Diese Erweiterung gilt nur für Einzelsitzungs-OS-Maschinen mit getrennten Sitzungen. Sie gilt nicht für Einzelsitzungs-OS-Maschinen mit abgemeldeten Sitzungen.
> - Damit die Erweiterung wirksam wird, müssen Sie Autoscale für die entsprechende Bereitstellungsgruppe aktivieren. Andernfalls werden beim Übergang die Trennaktionen der Energierichtlinie nicht ausgelöst.

In früheren Versionen blieben Einzelsitzungs-OS-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 diesem Release wird die Maschine nach Ablauf der festgelegten Trennzeit von Autoscale angehalten oder ausgeschaltet (je nach der für den Zielzeitraum konfigurierten Trennaktion).

Beispielsweise konfigurieren Sie die folgenden Energierichtlinien für eine Einzelsitzungs-OS-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 Einzelsitzungs-OS-Maschinen, bei denen während der Spitzenzeit eine Sitzung getrennt wurde, beim Übergang von der Spitzen- in die Nebenzeit eingeschaltet. Ab diesem Release werden die Richtlinienaktionen `OffPeakDisconnectAction` und `OffPeakDisconnectTimeout` beim Übergang zu einem neuen Zeitraum auf Einzelsitzungs-OS-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 fest (wahr, d. h. aktiviert das vorherige Verhalten). 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 Einzelsitzungs-OS-Bereitstellungsgruppe, 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.

### Funktionsweise des Kapazitätspuffers

Der Kapazitätspuffer dient zum Vorhalten freier Kapazität zur Berücksichtigung dynamischer Laststeigerungen. Es sind zwei Szenarien zu beachten:

- Bei Multisitzungs-OS-Bereitstellungsgruppen wird der Kapazitätspuffer als Prozentsatz der Gesamtkapazität der Bereitstellungsgruppe in Bezug auf den Lastindex definiert. Weitere Hinweise zum Lastindex finden Sie unter Lastindex.
- Bei Einzelsitzungs-OS-Bereitstellungsgruppen wird der Kapazitätspuffer als Prozentsatz der Gesamtkapazität der Bereitstellungsgruppe in Bezug auf die Anzahl der Maschinen definiert.

> **Hinweis:**
>
> Wenn Sie Autoscale auf Maschinen mit Tag beschränken, wird der Kapazitätspuffer als Prozentsatz der Gesamtkapazität der Maschinen mit Tag in der Bereitstellungsgruppe in Bezug auf den Lastindex definiert.

In Autoscale können Sie den Kapazitätspuffer für Spitzen- und Nebenzeiten separat festlegen. Ein niedrigerer Wert im Feld "Kapazitätspuffer"senkt die Kosten, da Autoscale weniger freie Kapazität einschaltet. Ein höherer Wert sorgt für eine optimale Benutzererfahrung, da die Benutzer beim Starten von Sitzungen nicht auf das Einschalten zusätzlicher Maschinen warten müssen. Standardmäßig beträgt der Kapazitätspuffer 10 %.

> **Wichtig:**
>
> Der Kapazitätspuffer bewirkt das Einschalten von Maschinen, sobald die Reservekapazität unter x Prozent der Gesamtkapazität der Bereitstellungsgruppe sinkt. Dadurch wird der erforderliche Prozentsatz an Kapazitätsreserven beibehalten.

## Multisitzungs-OS-Bereitstellungsgruppen

### Wann werden Maschinen eingeschaltet?

> **Wichtig:**
>
> Wenn ein Zeitplan ausgewählt ist, schaltet Autoscale alle im Zeitplan zum Einschalten konfigurierten Maschinen ein. Diese Maschinen bleiben während des Zeitplans lastunabhängig eingeschaltet.

Wenn die Anzahl eingeschalteter Maschinen in der Bereitstellungsgruppe die Pufferkapazität gemäß Lastindex nicht mehr erfüllen kann, schaltet Autoscale weitere Maschinen ein. Angenommen, Ihre Bereitstellungsgruppe hat 20 Maschinen und 3 Maschinen werden im Rahmen der planbasierten Skalierung mit einem Kapazitätspuffer von 20% eingeschaltet. Schließlich werden 4 Maschinen eingeschaltet, wenn keine Last vorhanden ist. Dies liegt daran, dass ein 4 x 10.000 Lastindex als Puffer benötigt wird; daher müssen mindestens 4 Maschinen eingeschaltet werden. Dies kann zu Spitzenzeiten, bei einer höheren Maschinenauslastung, neuen Sitzungsstarts und beim Hinzufügen neuer Maschinen zur Bereitstellungsgruppe eintreten. Autoscale schaltet nur Maschinen ein, die die folgenden Kriterien erfüllen:

- Die Maschinen sind nicht im Wartungsmodus.
- Der Hypervisor, auf dem die Maschinen ausgeführt werden, ist nicht im Wartungsmodus.
- Die Maschinen sind derzeit ausgeschaltet.
- Die Maschinen haben keine ausstehenden Energieaktionen.

### Wann werden Maschinen ausgeschaltet?

> **Wichtig:**
>
> - Wenn ein Zeitplan ausgewählt ist, schaltet Autoscale die Maschinen gemäß diesem Zeitplan aus.
> - Autoscale schaltet keine Maschinen aus, die im Zeitplan als eingeschaltet konfiguriert sind.

Sind mehr als genügend Maschinen (laut Zeitplan und einschließlich Puffer) für eine Bereitstellungsgruppe eingeschaltet, schaltet Autoscale überzählige Maschinen aus. Dies kann zu Nebenzeiten, bei einer gesunkenen Maschinenauslastung, bei Sitzungsabmeldungen und beim Entfernen von Maschinen aus einer Bereitstellungsgruppe eintreten. Autoscale schaltet nur Maschinen aus, die die folgenden Kriterien erfüllen:

- Die Maschinen und der Hypervisor, auf dem sie ausgeführt werden, sind nicht im Wartungsmodus.
- Die Maschinen sind derzeit eingeschaltet.
- Die Maschinen sind als verfügbar registriert oder warten auf die Registrierung nach dem Start.
- Die Maschinen haben keine aktiven Sitzungen.
- Die Maschinen haben keine ausstehenden Energieaktionen.
- Die Maschinen erfüllen die angegebene Ausschaltverzögerung. Dies bedeutet, dass die Maschinen mindestens x Minuten eingeschaltet waren, wobei x die für die Bereitstellungsgruppe festgelegte Ausschaltverzögerung ist.

#### Beispielszenario

Angenommen, Sie haben das folgende Szenario:

- **Bereitstellungsgruppenkonfiguration**. Die Bereitstellungsgruppe, die von Autoscale verwaltet werden soll, enthält 10 Maschinen (M1 bis M10).
- **Autoscale-Konfiguration**
  - Der Kapazitätspuffer ist auf 10 % eingestellt.
  - Im ausgewählten Zeitplan ist keine Maschine enthalten.

Das Szenario hat folgenden Ablauf:

1. Kein Benutzer meldet sich an.
2. Die Anzahl der Benutzersitzungen erhöht sich.
3. Weitere Benutzersitzungen beginnen.
4. Die Benutzersitzungslast nimmt aufgrund von Sitzungsbeendigungen ab.

5. Die Benutzersitzungslast nimmt weiter ab, bis sie nur von lokalen Ressourcen getragen wird.

Informationen zur Funktionsweise von Autoscale in diesem Szenario finden Sie nachfolgend.

- Keine Benutzerlast (Anfangszustand)
  - Eine Maschine (z. B. M1) wird eingeschaltet. Die Maschine wird wegen des konfigurierten Kapazitätspuffers eingeschaltet. In diesem Fall gilt 10 (Anzahl der Maschinen) x 10.000 (Lastindex) x 10 % (konfigurierter Kapazitätspuffer) = 10.000. Daher wird eine Maschine eingeschaltet.
  - Der Lastindexwert der eingeschalteten Maschine (M1) liegt bei einer Basislast (Lastindex = 0).
- Der erste Benutzer meldet sich an.
  - Die Sitzung wird an Maschine M1 zum Hosten geleitet.
  - Der Lastindex der eingeschalteten Maschine M1 erhöht sich und liegt nicht mehr bei der Basislast.
  - Autoscale schaltet eine zusätzliche Maschine (M2) ein, um den Bedarf gemäß dem konfigurierten Kapazitätspuffer zu decken.
  - Der Lastindexwert der Maschine M2 liegt bei einer Basislast.
- Die Benutzerlast steigt.
  - Die Sitzungen werden auf die Maschinen M1 und M2 verteilt. Dadurch steigt der Lastindex der eingeschalteten Maschinen (M1 und M2).
  - Die Kapazitätsreserven liegen nach wie vor auf einem Niveau über 10.000 gemäß Lastindex.
  - Der Lastindexwert der Maschine M2 liegt nicht mehr bei einer Basislast.
- Weitere Benutzersitzungen beginnen.
  - Die Sitzungen werden auf die Maschinen M1 und M2 verteilt. Dadurch steigt der Lastindex der eingeschalteten Maschinen (M1 und M2) weiter.
  - Wenn die gesamte freie Kapazität in Bezug auf den Lastindex auf unter 10.000 sinkt, beginnt Autoscale mit dem Einschalten einer zusätzlichen Maschine (M3), um den Bedarf gemäß konfiguriertem Kapazitätspuffer zu decken.
  - Der Lastindexwert der Maschine M3 liegt bei einer Basislast.
- Weitere Benutzersitzungen beginnen.
  - Die Sitzungen werden auf die Maschinen M1 bis M3 verteilt. Dadurch steigt der Lastindex der eingeschalteten Maschinen (M1 bis M3).
  - Die Kapazitätsreserven liegen auf einem Niveau über 10.000 gemäß Lastindex.
  - Der Lastindexwert der Maschine M3 liegt nicht mehr bei einer Basislast.

- Die Benutzersitzungslast nimmt aufgrund von Sitzungsbeendigungen ab.
  - Nachdem Benutzer sich von ihren Sitzungen abgemeldet haben oder diese aufgrund von Timeouts abgemeldet wurden, wird die freigegebene Kapazität auf Maschinen M1 bis M3 für das Hosting neuer Sitzungen wiederverwendet.
  - Steigt die gesamte freie Kapazität auf ein Niveau über 10.000 gemäß Lastindex, versetzt Autoscale eine der Maschinen (z. B. M3) in den Drainingzustand. Von anderen Benutzern gestartete Sitzungen werden nicht mehr an diese Maschine geleitet, sofern keine neuen Änderungen erfolgen. Beispielsweise Endbenutzerlast steigt wieder oder eine Geringauslastung anderer Maschinen
- Die Sitzungslast nimmt weiter ab.
  - Wenn alle Sitzungen auf Maschine M3 beendet wurden und die angegebene Ausschaltverzögerung abgelaufen ist, schaltet Autoscale M3 aus.
  - Wenn weitere Benutzer ihre Sitzungen beenden, wird die freigegebene Kapazität auf den eingeschalteten Maschinen (M1 und M2) für das Hosting neuer Sitzungen anderer Benutzer wiederverwendet.
  - Steigt die gesamte freie Kapazität auf ein Niveau über 10.000 gemäß Lastindex, versetzt Autoscale eine der Maschinen (z. B. M2) in den Drainingzustand. Von anderen Benutzern gestartete Sitzungen werden nicht mehr an diese Maschine geleitet.
- Die Sitzungslast nimmt weiter ab bis es keine Sitzungen mehr gibt.
  - Wenn alle Sitzungen auf Maschine M2 beendet wurden und die angegebene Ausschaltverzögerung abgelaufen ist, schaltet Autoscale M2 aus.
  - Der Lastindexwert der eingeschalteten Maschine (M1) liegt bei einer Basislast. Maschine M1 wird aufgrund des konfigurierten Kapazitätspuffers nicht in den Drainingzustand versetzt.

> **Hinweis:**
>
> Bei Multisitzungs-OS-Bereitstellungsgruppen gehen alle Änderungen am Desktop verloren, wenn Benutzer Sitzungen abmelden. Bei entsprechender Konfiguration werden benutzerspezifische Einstellungen jedoch zusammen mit dem Benutzerprofil weitergegeben.

### Zufällige Einzelsitzungs-OS-Bereitstellungsgruppen

Der Kapazitätspuffer wird verwendet, um plötzliche Nachfragespitzen aufzufangen, indem eine auf der Gesamtzahl der Maschinen in der Bereitstellungsgruppe basierende Zahl von Maschinen eingeschaltet bleibt. Standardmäßig beträgt der Kapazitätspuffer 10 % der Gesamtzahl der Maschinen in der Bereitstellungsgruppe.

Überschreitet die Anzahl der Maschinen (einschließlich Kapazitätspuffer) die Gesamtzahl der eingeschalteten Maschinen, werden weitere Maschinen eingeschaltet. Unterschreitet die Anzahl der Maschinen (einschließlich Kapazitätspuffer) die Gesamtzahl der eingeschalteten Maschinen, werden die überzähligen Maschinen je nach Konfiguration angehalten oder ausgeschaltet.

#### Beispielszenario

Angenommen, Sie haben das folgende Szenario:

- **Bereitstellungsgruppenkonfiguration**. Die Bereitstellungsgruppe, die von Autoscale verwaltet werden soll, enthält 10 Maschinen (M1 bis M10).
- **Autoscale-Konfiguration**
  - Der Kapazitätspuffer ist auf 10 % eingestellt.
  - Im ausgewählten Zeitplan ist keine Maschine enthalten.

Das Szenario hat folgenden Ablauf:

1. Kein Benutzer meldet sich an.
2. Die Anzahl der Benutzersitzungen erhöht sich.
3. Weitere Benutzersitzungen beginnen.
4. Die Benutzersitzungslast nimmt aufgrund von Sitzungsbeendigungen ab.
5. Die Benutzersitzungslast nimmt weiter ab, bis sie nur von lokalen Ressourcen getragen wird.

Informationen zur Funktionsweise von Autoscale in diesem Szenario finden Sie nachfolgend.

- Keine Benutzerlast (Anfangszustand)
  - Eine Maschine (M1) ist eingeschaltet. Die Maschine wird wegen des konfigurierten Kapazitätspuffers eingeschaltet. In diesem Fall gilt 10 (Anzahl der Maschinen) x 10 % (konfigurierter Kapazitätspuffer) = 1. Daher wird eine Maschine eingeschaltet.
- Der erste Benutzer meldet sich an.
  - Wenn sich ein Benutzer zum ersten Mal anmeldet, um einen Desktop zu verwenden, wird ihm ein Desktop aus einem Pool von Desktops zugewiesen, die auf den eingeschalteten Maschinen gehostet werden. In diesem Fall wird ihm ein Desktop von Maschine M1 zugewiesen.
  - Autoscale schaltet eine zusätzliche Maschine (M2) ein, um den Bedarf gemäß dem konfigurierten Kapazitätspuffer zu decken.
- Ein zweiter Benutzer meldet sich an.
  - Dem Benutzer wird ein Desktop von Maschine M2 zugewiesen.

  - Autoscale schaltet eine zusätzliche Maschine (M3) ein, um den Bedarf gemäß dem konfigurierten Kapazitätspuffer zu decken.

- Ein dritter Benutzer meldet sich an.
  - Ihm wird ein Desktop von Maschine M3 zugewiesen.
  - Autoscale schaltet eine zusätzliche Maschine (M4) ein, um den Bedarf gemäß dem konfigurierten Kapazitätspuffer zu decken.
- Ein Benutzer meldet sich ab.
  - Wenn sich ein Benutzer abmeldet oder bei einem Desktop ein Timeout auftritt, steht die freigesetzte Kapazität (z. B. M3) als Puffer zur Verfügung. Infolgedessen schaltet Autoscale Maschine M4 aus, da der Kapazitätspuffer auf 10 % festgelegt ist.
- Weitere Benutzer melden sich ab, bis keine Benutzer mehr vorhanden sind.
  - Wenn sich weitere Benutzer abmelden, schaltet Autoscale Maschinen aus (z. B. M2 oder M3).
  - Selbst wenn keine Benutzer mehr vorhanden sind, schaltet Autoscale die verbleibende Maschine (z. B. M1) nicht aus, da diese als Reserve festgelegt ist.

> **Hinweis:**
>
> Bei zufälligen Einzelsitzungs-OS-Bereitstellungsgruppen gehen alle Änderungen am Desktop verloren, wenn Benutzer Sitzungen abmelden. Bei entsprechender Konfiguration werden benutzerspezifische Einstellungen jedoch zusammen mit dem Benutzerprofil weitergegeben.

### Statische Einzelsitzungs-OS-Bereitstellungsgruppen

Der Kapazitätspuffer wird verwendet, um plötzliche Nachfragespitzen aufzufangen, indem eine auf der Gesamtzahl der nicht zugewiesenen Maschinen in der Bereitstellungsgruppe basierende Zahl nicht zugewiesener Maschinen eingeschaltet bleibt. Standardmäßig beträgt der Kapazitätspuffer 10 % der Gesamtzahl der nicht zugewiesenen Maschinen in der Bereitstellungsgruppe.

> **Wichtig:**
>
> Wenn alle Maschinen einer Bereitstellungsgruppe zugewiesen sind, spielt der Kapazitätspuffer für das Ein- und Ausschalten von Maschinen keine Rolle mehr.

Überschreitet die Anzahl der Maschinen (einschließlich Kapazitätspuffer) die Gesamtzahl der eingeschalteten Maschinen, werden weitere nicht zugewiesene Maschinen eingeschaltet. Unterschreitet die Anzahl der Maschinen (einschließlich Kapazitätspuffer) die Gesamtzahl der eingeschalteten Maschinen, werden überzählige Maschinen je nach Konfiguration angehalten oder ausgeschaltet.

Autoscale für statische Einzelsitzungs-OS-Bereitstellungsgruppen:

- Schaltet zugewiesene Maschinen zu Spitzenzeiten ein und zu Nebenzeiten aus. Aber nur dann, wenn die Eigenschaft `AutomaticPowerOnForAssigned` der entsprechenden Einzelsitzungs-OS-Bereitstellungsgruppe auf "true"festgelegt ist.
- Schaltet einen Computer während Spitzenzeiten automatisch ein, wenn er ausgeschaltet ist und die Eigenschaft `AutomaticPowerOnForAssignedDuringPeak` der Bereitstellungsgruppe, zu der er gehört, auf "true"gesetzt ist.

Um zu verstehen, wie der Kapazitätspuffer mit zugewiesenen Maschinen funktioniert, sollten Sie Folgendes beachten:

- Der Kapazitätspuffer funktioniert nur, wenn die Bereitstellungsgruppe mindestens eine nicht zugewiesene Maschinen hat.
- Wenn es in der Bereitstellungsgruppe keine nicht zugewiesenen Maschinen gibt (alle Maschinen in der Bereitstellungsgruppe sind zugewiesen), spielt der Kapazitätspuffer für das Ein- und Ausschalten von Maschinen keine Rolle mehr.
- Die Eigenschaft `AutomaticPowerOnForAssignedDuringPeak` legt fest, ob zugewiesene Maschinen zu Spitzenzeiten eingeschaltet werden. Wenn der Wert auf "True"festgelegt ist, lässt Autoscale die Maschinen zu Spitzenzeiten eingeschaltet. Autoscale schaltet sie außerdem ein, wenn sie ausgeschaltet sind.

#### Beispielszenario

Angenommen, Sie haben das folgende Szenario:

- **Bereitstellungsgruppenkonfiguration**. Die Bereitstellungsgruppe, die von Autoscale verwaltet werden soll, enthält 10 Maschinen (M1 bis M10).
- **Autoscale-Konfiguration**
  - Die Maschinen M1 bis M3 sind zugewiesen, die Maschinen M4 bis M10 sind nicht zugewiesen.
  - Der Kapazitätspuffer ist für Spitzen- und Nebenzeiten auf 10 % festgelegt.
  - Gemäß Zeitplan findet die Energieverwaltung von Maschinen durch Autoscale zwischen 09:00 Uhr und 18:00 Uhr statt.

Informationen zur Funktionsweise von Autoscale in diesem Szenario finden Sie nachfolgend.

- Beginn des Zeitplans: 09:00 Uhr
  - Autoscale schaltet Maschine M1 bis M3 ein.
  - Autoscale schaltet eine zusätzliche Maschine (z. B. M4) ein, um den Bedarf gemäß dem konfigurierten Kapazitätspuffer zu decken. Maschine M4 ist nicht zugewiesen.
- Der erste Benutzer meldet sich an.

  - Wenn sich ein Benutzer zum ersten Mal anmeldet, um einen Desktop zu verwenden, wird ihm ein Desktop aus einem Pool von Desktops zugewiesen, die auf den eingeschalteten, nicht zugewiesenen Maschinen gehostet werden. In diesem Fall wird ihm ein Desktop von Maschine M4 zugewiesen. Bei nachfolgenden Anmeldungen wird dem Benutzer derselbe Desktop wie beim ersten Mal zugewiesen.
  - Autoscale schaltet eine zusätzliche Maschine (z. B. M5) ein, um den Bedarf gemäß dem konfigurierten Kapazitätspuffer zu decken.

- Ein zweiter Benutzer meldet sich an.
  - Dem Benutzer wird ein Desktop von den nicht zugewiesenen, eingeschalteten Maschinen zugewiesen. In diesem Fall wird ihm ein Desktop von Maschine M5 zugewiesen. Bei nachfolgenden Anmeldungen wird dem Benutzer derselbe Desktop wie beim ersten Mal zugewiesen.
  - Autoscale schaltet eine zusätzliche Maschine (z. B. M6) ein, um den Bedarf gemäß dem konfigurierten Kapazitätspuffer zu decken.

- Benutzer melden sich ab.
  - Wenn sich Benutzer vom Desktop abmelden oder auf Desktops ein Timeout auftritt, bleiben die Maschinen M1 bis M5 von 09:00 Uhr bis 18:00 Uhr eingeschaltet. Wenn sich Benutzer neu anmelden, stellen sie eine Verbindung mit demselben Desktop her, der ihnen bei der ersten Verwendung zugewiesen wurde.
  - Die nicht zugewiesene Maschine M6 ist für einen neuen, nicht zugewiesenen Benutzer vorgesehen.

- Ende des Zeitplans: 18:00 Uhr
  - Um 18:00 Uhr schaltet Autoscale die Maschinen M1 bis M5 ab.
  - Die nicht zugewiesene Maschine M6 bleibt wegen des konfigurierten Kapazitätspuffers eingeschaltet. Diese Maschine ist für einen neuen, nicht zugewiesenen Benutzer vorgesehen.
  - In der Bereitstellungsgruppe sind die Maschinen M6 bis M10 nicht zugewiesen.

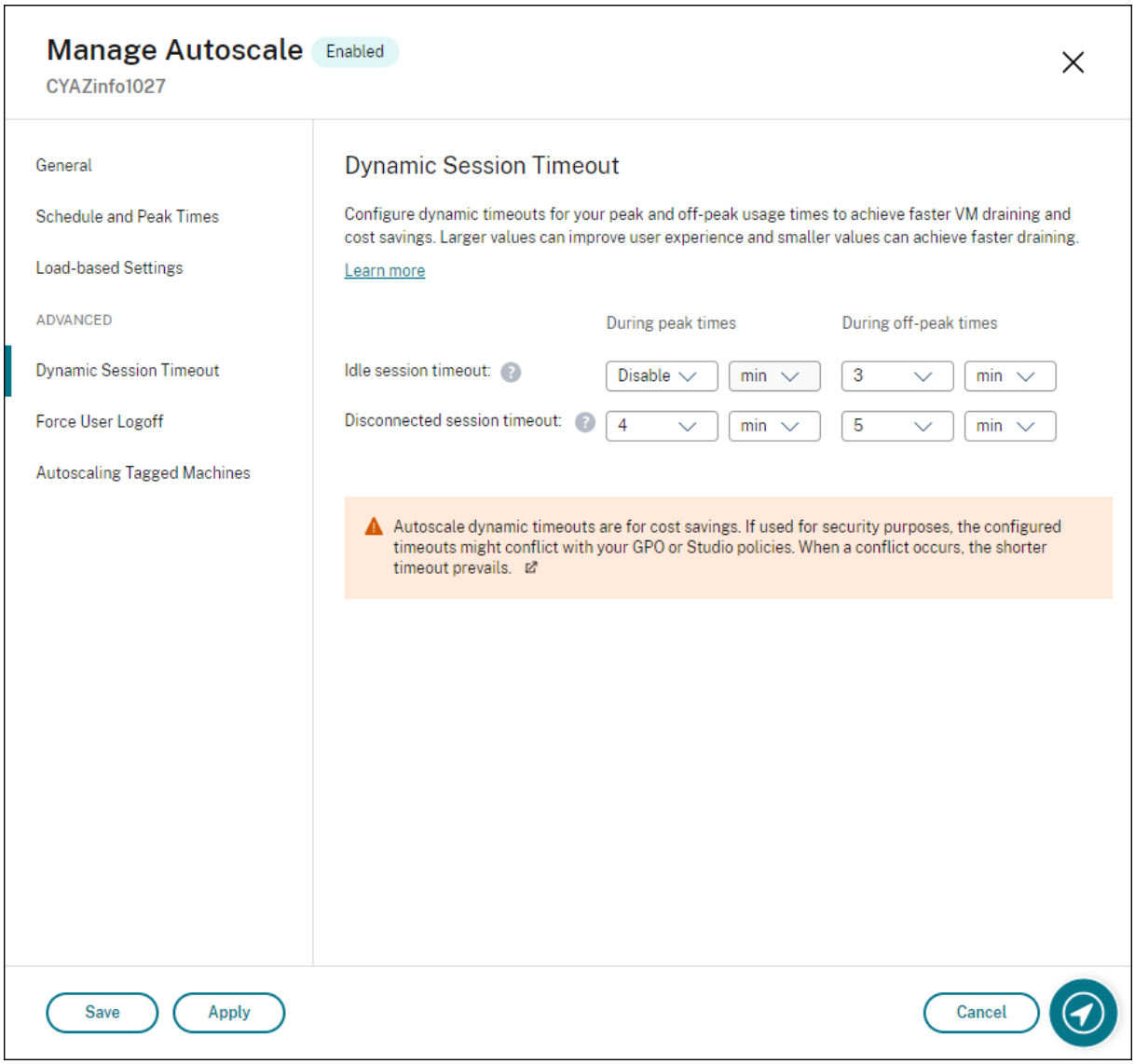
## Dynamische Sitzungstimeouts

June 27, 2024

Mit diesem Feature können Sie Timeouts für getrennte Sitzungen und Leerlaufsitzungen für Neben- und Spitzenzeiten konfigurieren, um ein schnelleres Maschinendraining und Kosteneinsparungen zu erzielen. Dieses Feature gilt für Maschinen mit Einzelsitzungs-OS und Multisitzungs-OS. VDAs melden

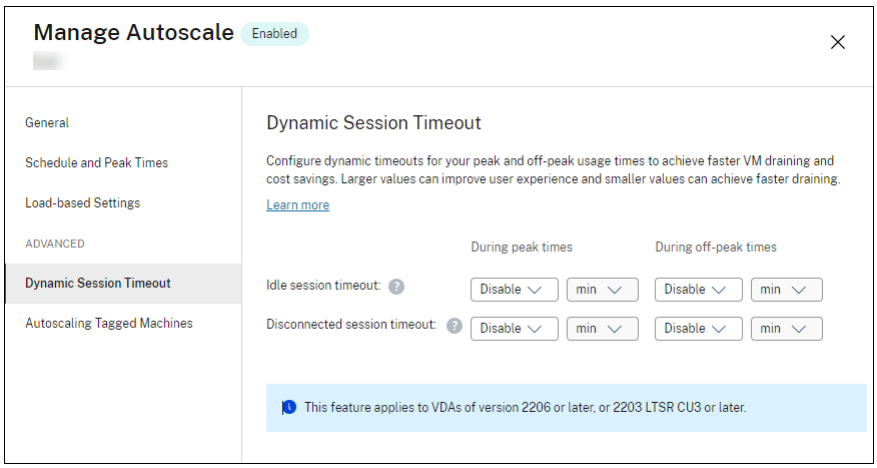
Leerlaufzeiten für Sitzungen, die über 10 Minuten im Leerlauf sind. Durch dynamische Sitzungstimeouts können daher Sitzungen nicht vor Ablauf von 10 Minuten getrennt werden. Ein geringerer Wert trennt Sitzungen früher und senkt so die Kosten.




**Hinweis:**

- Dieses Feature ist immer für Multisitzungs-OS-Bereitstellungsgruppen verfügbar.
- Für Bereitstellungsgruppen mit Einzelsitzungs-OS gilt dieses Feature für VDAs ab Version 2206 CR oder 2203 LTSR CU3 oder höher. Stellen Sie sicher, dass sich diese VDAs mindestens einmal in Citrix Cloud registriert haben. Wenn dieses Feature nicht verfügbar ist, wird die folgende Benutzeroberfläche angezeigt:




- Mit Autoscale festgelegte dynamische Timeouts dienen der Kosteneinsparung. Bei Verwendung aus Sicherheitsgründen können die konfigurierten Timeouts mit Ihren Gruppenrichtlinienobjekt- oder Verwaltungskonsolen-Richtlinien in Konflikt stehen. Bei einem Konflikt wird das kürzere Timeout verwendet.

**Timeout bei Sitzungsleerlauf:** Aktiviert oder deaktiviert einen Timer, der angibt, wie lange eine ununterbrochene Benutzerverbindung erhalten bleibt, wenn keine Benutzereingaben stattfinden. Wenn der Timer abläuft, wird die Sitzung getrennt und der **Timeout für Sitzungstrennung** angewendet. Wenn der **Timeout für Sitzungstrennung** deaktiviert ist, wird die Sitzung nicht abgemeldet.

**Wichtig:**

- Wenn Sie einen Wert angeben, der kleiner oder gleich zehn Minuten (600 Sekunden) ist, trennt Autoscale die Sitzungen nach zehn Minuten Leerlauf. Das liegt daran, dass Autoscale die von VDAs gemeldeten Leerlaufzeiten verwendet. VDAs melden Leerlaufzeiten für Sitzungen, die über 10 Minuten im Leerlauf sind.
- Eine Sitzung im Leerlauf wird auch dann getrennt, wenn der Benutzer in den letzten 5 Minuten vor Erreichen des Leerlauftimeouts mit ihr interagiert.

**Timeout für Sitzungstrennung:** Aktiviert bzw. deaktiviert einen Timer, der angibt, wie lange ein getrennter Desktop gesperrt bleibt, bevor die Sitzung abgemeldet wird. Wenn der Timer aktiviert ist, wird die getrennte Sitzung abgemeldet, wenn die Zeit abgelaufen ist.

## Autoscale von getaggten Maschinen (Cloudburst)

June 27, 2024

> **Hinweis:**
>
> Dieses Feature hieß bisher “Autoscale einschränken”.

## Einführung

Autoscale bietet die Flexibilität, die Energieverwaltung nur für eine Teilmenge der Maschinen in einer Bereitstellungsgruppe durchzuführen. Sie erreichen dies, indem Sie ein Tag auf mindestens eine Maschine anwenden und dann Autoscale so konfigurieren, dass die Energieverwaltung nur für getaggte Maschinen zutrifft.

Diese Funktion kann in Anwendungsfällen nützlich sein, in denen Sie On-Premises-Ressourcen (oder reservierte Public Cloud-Instanzen) verwenden möchten, um Workloads zu verarbeiten, bevor cloudbasierte Ressourcen zusätzliche Anforderungen (d. h. Burstworkloads) erfüllen. Damit Maschinen im eigenen Rechenzentrum (oder reservierte Instanzen) zuerst Workloads verarbeiten, müssen Sie die Tagbeschränkung zusammen mit einer Zonenpräferenzeinstellung verwenden.

Die Tagbeschränkung legt fest, für welche Maschinen Autoscale die Energieverwaltung übernimmt. Die Zonenpräferenz gibt Maschinen in der bevorzugten Zone an, um Benutzerstartanforderungen zu verarbeiten. Weitere Informationen finden Sie unter Tags und Zonenpräferenz.

Um Autoscale auf bestimmte getaggte Maschinen anzuwenden, können Sie die Vewaltungskonsole oder PowerShell verwenden.

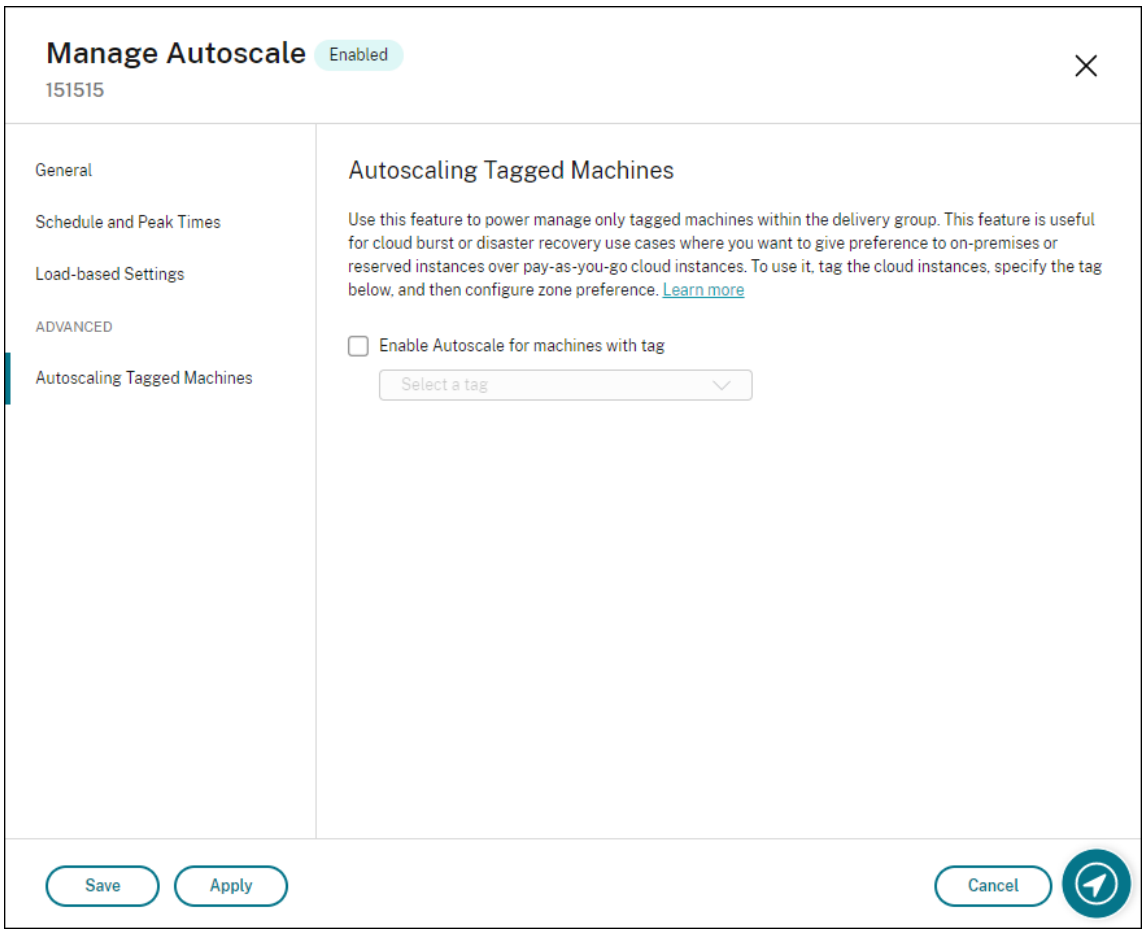
### Autoscale getaggter Maschinen über die Verwaltungskonsole

Führen Sie folgende Schritte aus, um Autoscale auf bestimmte getaggte Maschinen anzuwenden:

1. Erstellen Sie ein Tag und wenden Sie es auf die entsprechenden Maschinen in der Bereitstellungsgruppe an. Weitere Informationen finden Sie unter Verwalten von Tags und Tagbeschränkungen.
2. Wählen Sie die Bereitstellungsgruppe aus und öffnen Sie den Assistenten **Autoscale verwalten**.
3. Wählen Sie auf der Seite **Autoscale getaggte Maschinen** die Option **Autoscale für getaggte Maschinen aktivieren**, wählen Sie ein Tag in der Liste aus und klicken Sie auf **Übernehmen**, um die Änderungen zu speichern.

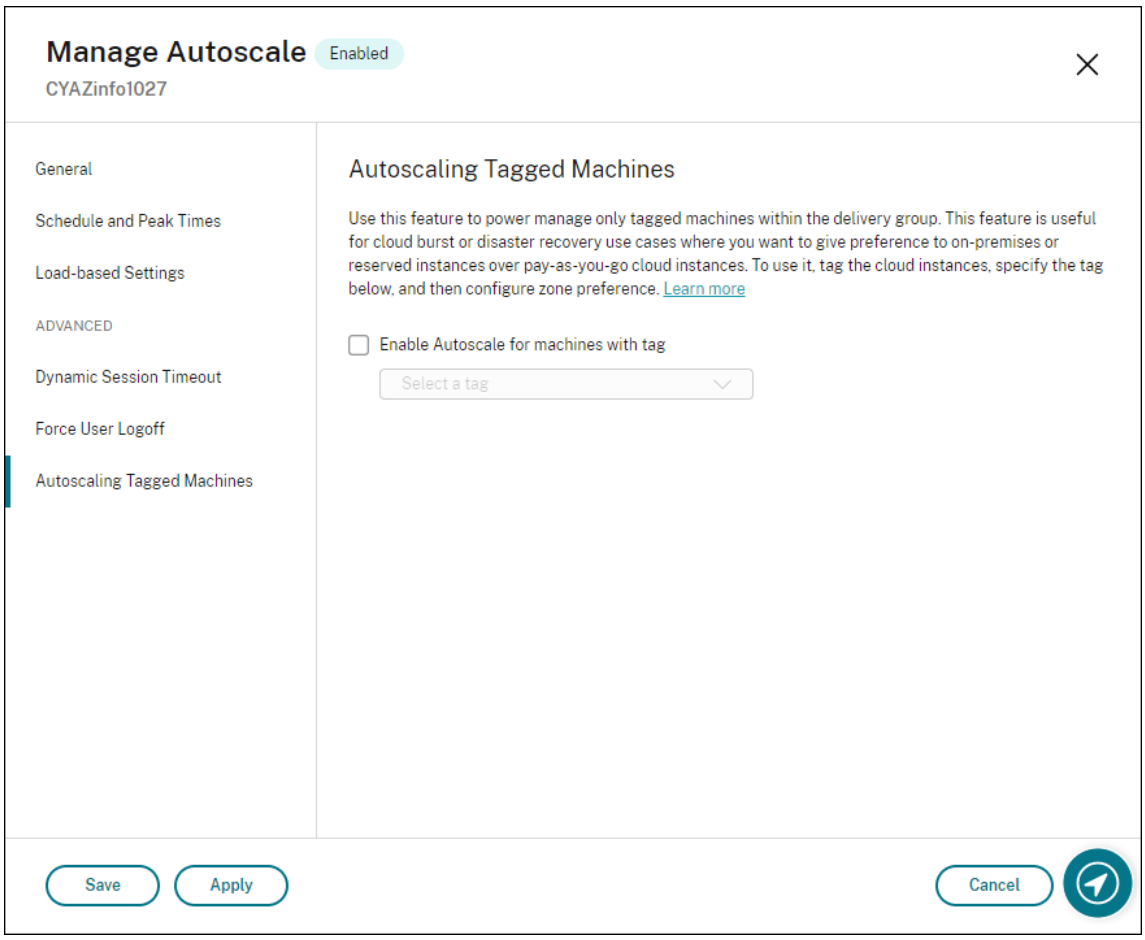
   Benutzeroberfläche für *statische* und *zufällige* Einzelsitzungs-OS-Bereitstellungsgruppen:




Benutzeroberfläche für *Multisitzungs-OS-Bereitstellungsgruppen*:




> **Warnung:**
>
> - Das Anwenden von Autoscale auf Maschinen mit einem bestimmten Tag kann dazu führen, dass das Histogramm automatisch aktualisiert wird, um die Anzahl von Maschinen für dieses Tag anzuzeigen. Auf der Seite **Zeitplan und Spitzenzeiten** können Sie jedem Zeitfenster bei Bedarf Maschinen manuell zuweisen.
> - Sie können ein auf getaggten Maschinen verwendetes Tag nicht löschen. Um ein solches Tag zu löschen, müssen Sie zuerst die Tagbeschränkung entfernen.

Nachdem Sie eine Tagbeschränkung angewendet haben, möchten Sie sie eventuell später aus der Bereitstellungsgruppe entfernen. Gehen Sie hierfür auf die Seite **Autoscale verwalten > Autoscale getaggte Maschinen** und deaktivieren Sie **Autoscale für getaggte Maschinen aktivieren**.

> **Warnung:**
>
> - Wenn Sie das Tag von den entsprechenden Maschinen entfernen, ohne **Autoscale für getaggte Maschinen aktivieren** zu deaktivieren, wird beim Öffnen des Assistenten **Autoscale verwalten** möglicherweise eine Warnung angezeigt. Durch das Entfernen des

> Tags von den Maschinen verbleiben evtl. keine Maschinen für die Autoscaleverwaltung, da das in Autoscale angegebene Tag ungültig ist. Um die Warnung aufzulösen, gehen Sie zur Seite **Autoscale getaggte Maschinen**, entfernen Sie das ungültige Tag und klicken Sie zum Speichern der Änderungen auf **Übernehmen**.

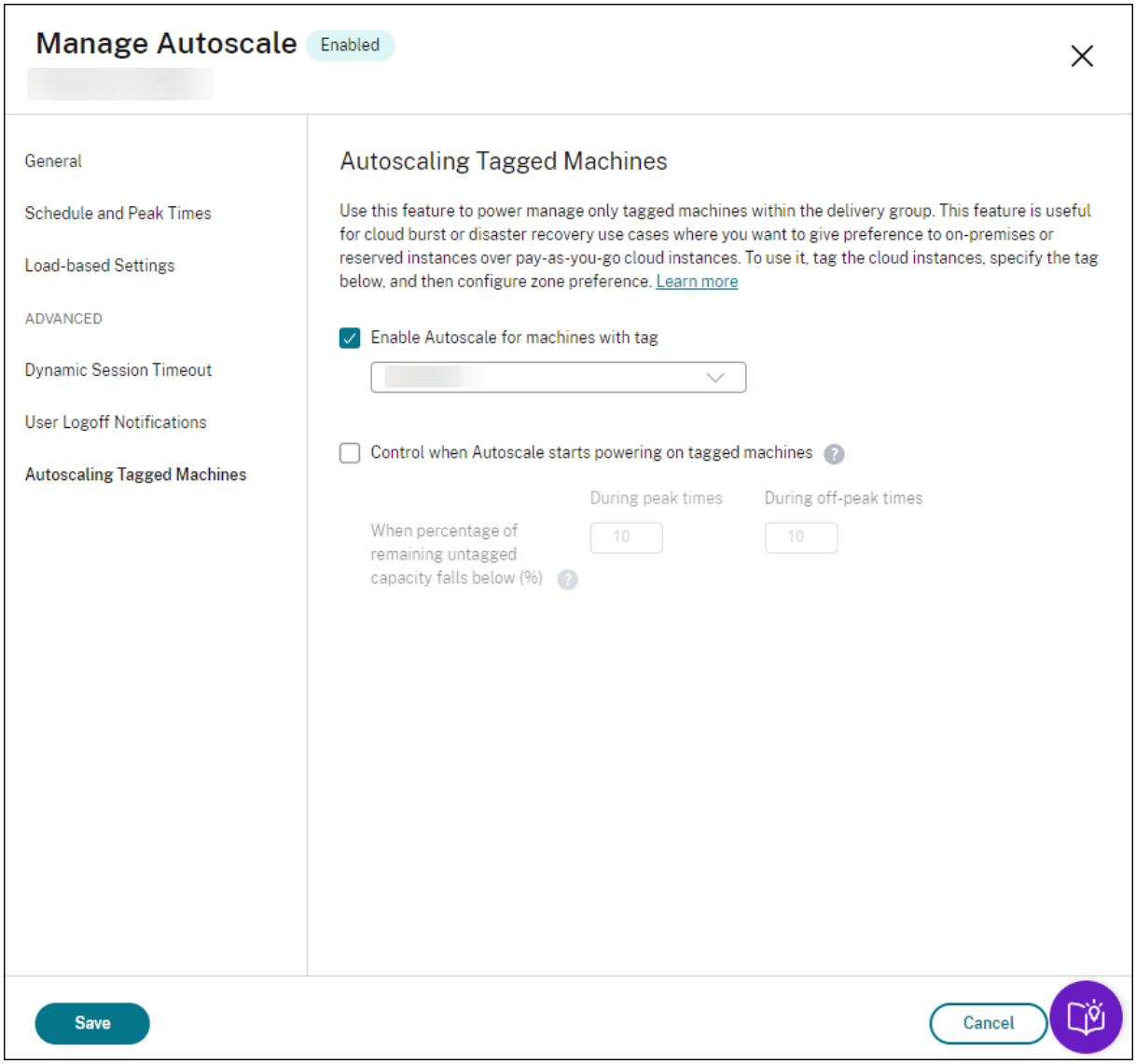
#### Steuerung des Einschaltens von Ressourcen durch Autoscale

Sie können auch steuern, wann Autoscale (basierend auf der Nutzung von ungetaggten Maschinen) mit dem Einschalten von getaggten Maschinen beginnt. Dadurch können Sie den Einsatz von getaggten Workloads oder Workloads in der öffentlichen Cloud weiter optimieren.

Führen Sie hierzu die folgenden Schritte aus:

1. Wählen Sie auf der Seite **Autoscale getaggte Maschinen** die Option **Steuern, wann Autoscale mit dem Einschalten von getaggten Maschinen beginnt**.
2. Geben Sie einen gewünschten Prozentwert für die Nutzung von ungetaggten Maschinen zu Spitzen- und Nebenzeiten ein, und klicken Sie auf **Übernehmen**. Unterstützte Werte: 0 –100.




**Tipp:**

Der Prozentsatz steuert, wann Autoscale mit dem Einschalten von getaggten Maschinen beginnt. Wenn der Prozentsatz unter den Schwellenwert fällt (Standardwert ist 10 %), beginnt Autoscale, die Maschinen mit Tag einzuschalten. Wenn der Prozentsatz den Schwellenwert überschreitet, wechselt Autoscale in den Ausschaltmodus. Bedenken Sie bei der Eingabe des Prozentwerts zwei Szenarios:

- Für Einzelsitzungs-OS-Bereitstellungsgruppen: Der Wert entspricht dem Prozentsatz aller ungetaggten Maschinen im Leerlauf. Beispiel: Sie haben 10 ungetaggte Einzelsitzungs-OS-Maschinen. Wenn nur noch eine ohne Sitzung übrig ist, schaltet Autoscale eine getaggte Maschine ein.
- Für Multisitzungs-OS-Bereitstellungsgruppen: Der Wert entspricht dem Prozentsatz

> der Gesamtkapazität (in Bezug auf den Lastindex) verfügbarer ungetaggter Maschinen. Beispiel: Sie haben 10 ungetaggte Multisitzungs-OS-Maschinen. Wenn sie zu 90 % geladen sind, schaltet Autoscale eine getaggte Maschine ein.

### Autoscale getaggter Maschinen mithilfe von PowerShell

Führen Sie die folgenden Schritte aus, um das PowerShell-SDK direkt zu verwenden:

1. **Erstellen Sie ein Tag.** Verwenden Sie den PowerShell-Befehl New-Brokertag, um ein Tag zu erstellen.
   - Beispiel: `$managed = New-BrokerTag Managed`. In diesem Fall heißt das Tag "Managed". Weitere Hinweise zum PowerShell-Befehl "New-Brokertag"finden Sie unter https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/New-BrokerTag/.
2. **Wenden Sie das Tag auf Maschinen an**. Verwenden Sie den PowerShell-Befehl Get-Brokermachine, um das Tag auf Maschinen in einem Katalog anzuwenden, die von Autoscale verwaltet werden sollen.
   - Beispiel: `Get-BrokerMachine -CatalogName "cloud"| Add-BrokerTag $managed.Name`. In diesem Fall hat der Katalog den Namen "Cloud".
   - Weitere Hinweise zum PowerShell-Befehl Get-Brokermachine finden Sie unter https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerMachine/.

   > **Hinweis:**
   >
   > Sie fügen dem Katalog vielleicht neue Maschinen hinzu, nachdem Sie das Tag angewendet haben. Das Tag wird *NICHT* automatisch auf diese neuen Maschinen angewendet.

3. **Maschinen mit Tags der Bereitstellungsgruppe hinzufügen, die von Autoscale verwaltet werden soll.** Verwenden Sie den PowerShell-Befehl Get-BrokerDesktopGroup, um der Bereitstellungsgruppe, die die Maschinen enthält, eine Einschränkung nach Tag hinzuzufügen (d. h. "Starts auf Maschinen mit Tag beschränken: X").
   - Beispiel: `Get-BrokerDesktopGroup -Uid 1 | Set-BrokerDesktopGroup -RestrictAutoscaleTagUid $managed.Uid`. In diesem Fall ist die UID der Bereitstellungsgruppe 1.
   - Weitere Hinweise zum PowerShell-Befehl Get-BrokerDesktopGroup finden Sie unter https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/.

Nachdem Sie eine Tagbeschränkung angewendet haben, möchten Sie sie eventuell später aus der Bereitstellungsgruppe entfernen. Verwenden Sie dazu den PowerShell-Befehl Get-BrokerDesktopGroup.

Beispiel: `Get-BrokerDesktopGroup –Uid 1 | Set-BrokerDesktopGroup –RestrictAutoscal $null`. In diesem Fall ist die UID der Bereitstellungsgruppe 1.

> **Hinweis:**
>
> Maschinen ohne Tags werden nach dem Ausschalten durch die Benutzer automatisch neu gestartet. Dadurch wird sichergestellt, dass sie schneller für Workloads verfügbar sind. Dies kann für einzelne Desktopgruppen mit der `AutomaticRestartForUntaggedMachines` -Eigenschaft `Set-BrokerDesktopGroup` aktiviert oder deaktiviert werden. Weitere Informationen finden Sie unter https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/.

### Beispielszenario

Angenommen, Sie haben das folgende Szenario:

- **Maschinenkatalogkonfiguration**. Es gibt zwei Maschinenkataloge (C1 und C2).
  - Katalog C1 enthält 5 Maschinen (M1 bis M5), die lokal in den On-Premises-Bereitstellungen sind.
  - Katalog C2 enthält 5 Maschinen (M6 bis M10), die remote in den Cloudbereitstellungen sind.
- **Tagbeschränkung**. Ein Tag mit dem Namen “Cloud”wird erstellt und auf Maschinen M6 bis M10 in Katalog C2 angewendet.
- **Zonenkonfiguration**. Es werden zwei Zonen (Z1 und Z2) erstellt.
  - Zone Z1 mit Katalog C1 entspricht den On-Premises-Bereitstellungen.
  - Zone Z2 mit Katalog C2 entspricht den Cloudbereitstellungen.
- **Bereitstellungsgruppenkonfiguration**
  - Die Bereitstellungsgruppe hat 10 Maschinen (M1 bis M10), 5 Maschinen aus den Katalogen C1 (M1 bis M5) und 5 aus Katalog C2 (M6 bis M10).
  - Die Maschinen M1 bis M5 werden manuell eingeschaltet und bleiben während des gesamten Zeitplans eingeschaltet.
- **Autoscale-Konfiguration**
  - Der Kapazitätspuffer ist auf 10 % eingestellt.

  - Autoscale führt die Energieverwaltung nur für Maschinen mit dem Tag "Cloud"durch. In diesem Fall führt Autoscale die Energieverwaltung für die Cloudmaschinen M6 bis M10 durch.

- **Konfiguration für veröffentlichte Anwendung oder veröffentlichten Desktop**. Zoneneinstellungen werden beispielsweise für die veröffentlichten Desktops konfiguriert. Zone Z1 wird vor Zone Z2 bevorzugt für eine Benutzerstartanforderung.

  - Zone Z1 wird als bevorzugte Zone (Homezone) für die veröffentlichten Desktops konfiguriert.

Das Szenario hat folgenden Ablauf:

1. Kein Benutzer meldet sich an.
2. Die Anzahl der Benutzersitzungen erhöht sich.
3. Die Anzahl der Benutzersitzungen erhöht sich weiter, bis alle verfügbaren On-Premises-Maschinen verbraucht sind.
4. Weitere Benutzersitzungen beginnen.
5. Die Anzahl der Benutzersitzungen nimmt ab, weil Sitzungen beendet werden.
6. Die Benutzersitzungslast nimmt weiter ab, bis sie nur von On-Premises-Maschinen getragen wird.

Informationen zur Funktionsweise von Autoscale in diesem Szenario finden Sie nachfolgend.

- Keine Benutzerlast (Anfangszustand)
  - Die On-Premises-Maschinen M1 bis M5 sind eingeschaltet.
  - Eine Maschine in der Cloud (z. B. M6) wird eingeschaltet. Die Maschine wird wegen des konfigurierten Kapazitätspuffers eingeschaltet. In diesem Fall gilt 10 (Anzahl der Maschinen) x 10.000 (Lastindex) x 10 % (konfigurierter Kapazitätspuffer) = 10.000. Daher wird eine Maschine eingeschaltet.
  - Der Lastindexwert aller eingeschalteten Maschinen (M1 bis M6) liegt bei einer Basislast (Lastindex = 0).
- Benutzer melden sich an
  - Die Sitzungen werden auf den Maschinen M1 bis M5 gehostet, dies entspricht der konfigurierten Zoneneinstellung, und es findet ein Lastausgleich zwischen diesen On-Premises-Maschinen statt.
  - Der Lastindexwert der eingeschalteten Maschinen (M1 bis M5) steigt.
  - Der Lastindexwert der eingeschalteten Maschine M6 liegt bei einer Basislast.
- Benutzer erhöhen die Last, alle On-Premises-Ressourcen werden verbraucht

  - Die Sitzungen werden auf den Maschinen M1 bis M5 gehostet, dies entspricht der konfigurierten Zoneneinstellung, und es findet ein Lastausgleich zwischen diesen On-Premises-Maschinen statt.
  - Der Lastindexwert der eingeschalteten Maschinen (M1 bis M5) erreicht 10.000.
  - Der Lastindexwert der eingeschalteten Maschine M6 bleibt bei einer Basislast.

- Ein weiterer Benutzer meldet sich an

  - Die Sitzung übersteigt die Kapazität der bevorzugten Zone und das Hosten wird an die Cloudmaschine M6 geleitet.
  - Der Lastindexwert der eingeschalteten Maschinen (M1 bis M5) erreicht 10.000.
  - Der Lastindexwert der eingeschalteten Maschine M6 erhöht sich und liegt nicht mehr bei einer Basislast. Wenn die gesamte freie Kapazität in Bezug auf den Lastindex auf unter 10.000 sinkt, beginnt Autoscale mit dem Einschalten einer zusätzlichen Maschine (M7), um den Bedarf gemäß konfiguriertem Kapazitätspuffer zu decken. Beachten Sie, dass es einige Zeit dauern kann, bis Maschine M7 eingeschaltet ist. Es könnte also eine Verzögerung geben, bis Maschine M7 bereit ist.

- Weitere Benutzer melden sich an

  - Die Sitzungen werden an Maschine M6 zum Hosten geleitet.
  - Der Lastindexwert der eingeschalteten Maschinen (M1 bis M5) erreicht 10.000.
  - Der Lastindexwert der eingeschalteten Maschine M6 steigt weiter, aber für die gesamte freie Kapazität liegt der Lastindex immer noch auf einem Niveau über 10.000.
  - Der Lastindexwert der eingeschalteten Maschine M7 bleibt bei einer Basislast.

- Noch mehr Benutzer melden sich an

  - Nachdem die Maschine M7 bereit ist, werden die Sitzungen auf den Maschinen M6 und M7 gehostet und es findet ein Lastausgleich zwischen diesen Maschinen statt.
  - Der Lastindexwert der eingeschalteten Maschinen (M1 bis M5) erreicht 10.000.
  - Der Lastindexwert der Maschine M7 liegt nicht mehr bei einer Basislast.
  - Der Lastindexwert der eingeschalteten Maschinen (M6 und M7) steigt.
  - Die Kapazitätsreserven liegen nach wie vor auf einem Niveau über 10.000 gemäß Lastindex.

- Die Benutzersitzungslast nimmt aufgrund von Sitzungsbeendigungen ab.

  - Nachdem Benutzer sich von ihren Sitzungen abgemeldet haben oder diese aufgrund von Timeouts abgemeldet wurden, wird die freigegebene Kapazität auf Maschinen M1 bis M7 für das Hosting neuer Sitzungen wiederverwendet.
  - Steigt die gesamte freie Kapazität auf ein Niveau über 10.000 gemäß Lastindex, versetzt Autoscale eine der Cloudmaschinen (M6 bis M7) in den Drainingzustand. Sitzungen, die von anderen Benutzern gestartet wurden, werden dann nicht mehr an diese Maschine (z.

B. M7) weitergeleitet, es sei denn, es treten neue Änderungen auf (beispielsweise Benutzerlast steigt wieder oder andere Cloudmaschinen haben die geringste Last).

- Die Benutzersitzungslast nimmt weiter ab, bis ein oder mehrere Cloudmaschinen nicht mehr benötigt werden
  - Wenn alle Sitzungen auf Maschine M7 beendet wurden und die angegebene Ausschaltverzögerung abgelaufen ist, schaltet Autoscale M7 aus.
  - Der Lastindexwert aller eingeschalteten Maschinen (M1 bis M5) kann unter 10.000 fallen.
  - Der Lastindexwert der eingeschalteten Maschine (M6) nimmt ab.
- Die Anzahl der Benutzersitzungen nimmt weiter ab, bis keine Cloudmaschinen mehr benötigt werden.
  - Obwohl es keine Benutzersitzungen mehr auf Maschine M6 gibt, schaltet Autoscale sie nicht aus, da sie als freie Kapazität reserviert ist.
  - Autoscale behält die nicht zugewiesene Cloudmaschine M6 eingeschaltet aufgrund des konfigurierten Kapazitätspuffers. Diese Maschine wartet darauf, einem neuen Benutzer einen Desktop bereitzustellen.
  - Sitzungen werden nicht zum Hosten an Maschine M6 geleitet, solange die On-Premises-Maschinen verfügbare Kapazität haben.

## Benachrichtigungen zur Benutzerabmeldung (früher Erzwingen von Benutzerabmeldungen)

June 27, 2024

> **Wichtig:**
>
> Das Feature ist nur in der Autoscale-Benutzeroberfläche für App-basierte Multisitzungs-Bereitstellungsgruppen verfügbar.

Zur Kosteneinsparung können Sie mit Autoscale die Abmeldung von fortbestehenden Sitzungen erzwingen. Sie können hierfür eine benutzerdefinierte Benachrichtigung an die Benutzer senden und einen Kulanzzeitraum angeben, nach dessen Ablauf die Sitzungen zwangsweise abgemeldet werden. Dies geschieht nur bei Maschinen im Drainingzustand und nicht bei allen eingeschalteten Maschinen. Um potenziellen Datenverlust durch erzwungene Benutzerabmeldungen zu vermeiden, können Sie dieses Feature so konfigurieren, dass nur Abmeldeerinnerungen gesendet werden, ohne dass eine Benutzerabmeldung erzwungen wird.

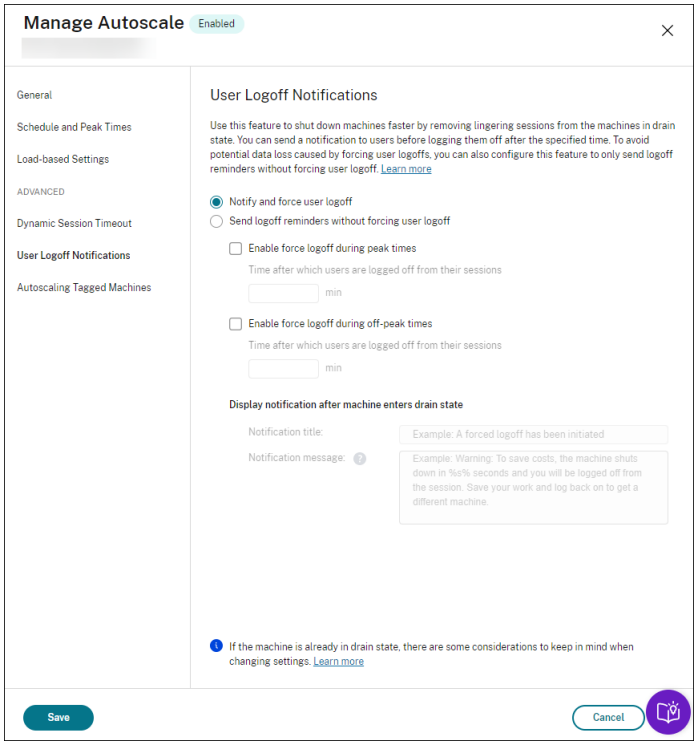
Die folgenden zwei Optionen sind verfügbar:

- **Benutzer benachrichtigen und Abmeldung erzwingen**
- **Abmeldeerinnerungen senden, ohne die Benutzerabmeldung zu erzwingen**

### Benutzer benachrichtigen und Abmeldung erzwingen

Wenn diese Option ausgewählt ist, meldet Autoscale Benutzer nach Ablauf der unten angegebenen Zeit von ihren Sitzungen ab.




‘**Abmeldung erzwingen während Spitzenzeit’aktivieren**. Wenn diese Option ausgewählt ist, meldet Autoscale Benutzer in Spitzenzeiten nach Ablauf der angegebenen Zeit von ihren Sitzungen ab.

‘**Abmeldung erzwingen während Nebenzeiten’aktivieren**. Wenn diese Option ausgewählt ist, meldet Autoscale Benutzer in Nebenzeiten nach Ablauf der angegebenen Zeit von ihren Sitzungen ab.

**Benachrichtigung anzeigen, nachdem die Maschine in den Draining-Zustand wechselt** Ermöglicht das Senden von Benachrichtigungen an Benutzer, nachdem ihre Maschine in den Drainingzustand versetzt wurde.

- **Benachrichtigungstitel**. Hier können Sie einen Titel für die Benachrichtigung angeben, die an Benutzer gesendet werden soll. Beispiel:`A forced logoff has been initiated`.
- **Benachrichtigung**. Hier können Sie den Inhalt der Benachrichtigung angeben, die an Benutzer gesendet werden soll. Sie können %s% oder %m% als Variablen verwenden, um die

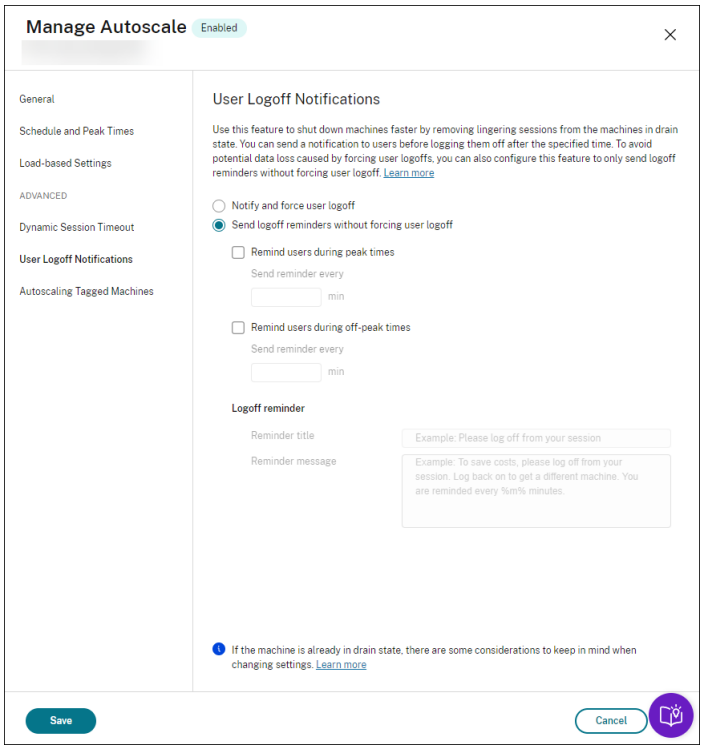
 

angegebene Uhrzeit in der Nachricht anzugeben. Um die Zeit in Sekunden auszudrücken, verwenden Sie %s%. Um die Zeit in Minuten auszudrücken, verwenden Sie %m%. Beispiel:

```
Warning: To save costs, the machine shuts down in %s% seconds and
 you will be logged off from the session. Save your work and log
back on to get a different machine.
```

### Abmeldeerinnerungen senden, ohne die Benutzerabmeldung zu erzwingen

Wenn diese Option ausgewählt ist, erhalten Benutzer eine Erinnerung, sich von ihrer Maschine abzumelden, nachdem diese in den Drainingzustand versetzt wurde. Diese Erinnerung kann so konfiguriert werden, dass sie in dem unten angegebenen Intervall gesendet wird.




**Benutzer während der Spitzenzeiten erinnern**. Wenn diese Option ausgewählt ist, erhalten Benutzer eine Erinnerung, sich zu Spitzenzeiten alle X Minuten von ihren Sitzungen abzumelden (X steht für die angegebene Zeit).

**Benutzer außerhalb der Spitzenzeiten erinnern**. Wenn diese Option ausgewählt ist, erhalten Benutzer eine Erinnerung, sich während Nebenzeiten alle X Minuten von ihren Sitzungen abzumelden (X steht für die angegebene Zeit).

**Abmeldeerinnerung**. Ermöglicht das Konfigurieren der Erinnerung, die an Benutzer gesendet wird, nachdem ihre Maschine in den Drainingzustand versetzt wurde.

- **Titel der Erinnerung**. Hier können Sie einen Titel für die Erinnerung angeben, die an Benutzer

gesendet werden soll. Beispiel: `Please log off from your session`.
- **Erinnerungsnachricht**. Hier können Sie eine Nachricht angeben, die an Benutzer gesendet werden soll. Beispiel: `Please log off from your session and log back on to save costs`.

### Überlegungen

Wenn sich die Maschine bereits im Drainingzustand befindet, beachten Sie beim Ändern der Einstellungen Folgendes:

- Wenn Sie die Einstellung von **Abmeldeerinnerungen senden, ohne die Benutzerabmeldung zu erzwingen** in **Benutzer benachrichtigen und Abmeldung erzwingen** ändern, wird die neue Einstellung sofort wirksam.
- Wenn Sie die Einstellung von **Benutzer benachrichtigen und Abmeldung erzwingen** in **Abmeldeerinnerungen senden, ohne die Benutzerabmeldung zu erzwingen** ändern, wird die neue Einstellung erst wirksam, wenn die Maschine das nächste Mal in den Drainingzustand wechselt. Der Benutzer wird nach wie vor zur Abmeldung gezwungen.

## Broker PowerShell SDK-Befehle

June 27, 2024

Sie können Autoscale für Bereitstellungsgruppen mit dem Broker PowerShell SDK konfigurieren. Um Autoscale mit PowerShell-Befehlen zu konfigurieren, müssen Sie PowerShell SDK Version 7.21.0.12 oder höher verwenden. Weitere Informationen zu den PowerShell SDKs finden Sie unter SDKs und APIs.

### Set-BrokerDesktopGroup

Deaktiviert oder aktiviert vorhandene BrokerDesktopGroup oder ändert deren Einstellungen. Weitere Informationen zu diesem Cmdlet finden Sie unter https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/.

#### Beispiele

Die folgenden Beispiele verdeutlichen die Verwendung der PowerShell-Cmdlets:

Autoscale aktivieren

- Angenommen, Sie möchten Autoscale für die Bereitstellungsgruppe "MyDesktop"aktivieren. Verwenden Sie den PowerShell-Befehl `Set-BrokerDesktopGroup`. Beispiel:

  ```
  PS C:\> Set-BrokerDesktopGroup "MyDesktop"-AutoscalingEnabled $true
  ```

Kapazitätspuffer für Spitzen- und Nebenzeiten separat festlegen

- Angenommen, Sie möchten für die Bereitstellungsgruppe "MyDesktop"den Kapazitätspuffer für Spitzenzeiten auf 20 % und für Nebenzeiten auf 10 % festlegen. Verwenden Sie den PowerShell-Befehl `Set-BrokerDesktopGroup`. Beispiel:

  ```
  PS C:\> Set-BrokerDesktopGroup "MyDesktop"-PeakBufferSizePercent 20 -OffPeakBufferSizePercent 10
  ```

Einstellung **Timeout für "Wenn getrennt"** konfigurieren

- Angenommen, Sie möchten für die Bereitstellungsgruppe "MyDesktop"den Wert **Timeout für "Wenn getrennt"** auf 60 Minuten für Spitzenzeiten und auf 30 Minuten für Nebenzeiten festlegen. Verwenden Sie den PowerShell-Befehl `Set-BrokerDesktopGroup`. Beispiel:

  ```
  PS C:\> Set-BrokerDesktopGroup "MyDesktop"-PeakDisconnectTimeout 60 -OffPeakDisconnectTimeout 30
  ```

Einstellung **Timeout für "Wenn abgemeldet"** konfigurieren

- Angenommen, Sie möchten für die Bereitstellungsgruppe "MyDesktop"den Wert **Timeout für "Wenn abgemeldet"** auf 60 Minuten für Spitzenzeiten und auf 30 Minuten für Nebenzeiten festlegen. Verwenden Sie den PowerShell-Befehl `Set-BrokerDesktopGroup`. Beispiel:

  ```
  PS C:\> Set-BrokerDesktopGroup "MyDesktop"-PeakLogOffTimeout 60 -OffPeakLogOffTimeout 30
  ```

Einstellung **Ausschaltverzögerung** konfigurieren

- Angenommen, Sie möchten die Ausschaltverzögerung für die Bereitstellungsgruppe "MyDesktop"auf 15 Minuten festlegen. Verwenden Sie den PowerShell-Befehl `Set-BrokerDesktopGroup`. Beispiel:

  ```
  PS C:\> Set-BrokerDesktopGroup "MyDesktop"-PowerOffDelay 15
  ```

Konfigurieren eines Zeitraums, in dem die Ausschaltverzögerung nicht angewendet wird

- Angenommen, Sie möchten die Ausschaltverzögerung für die Bereitstellungsgruppe "MyDesktop"auf 30 Minuten festlegen. Verwenden Sie den PowerShell-Befehl `Set-BrokerDesktopGroup`. Beispiel:

- `C:\PS> Set-BrokerDesktopGroup "MyDesktop"-SettlementPeriodBeforeAutoSh`
  `30.`

Eigenschaft **Maschineninstanzkosten** konfigurieren

- Angenommen, Sie möchten für die Bereitstellungsgruppe "MyDesktop"die Maschineninstanzkosten pro Stunde auf 0,2 Dollar festlegen. Verwenden Sie den PowerShell-Befehl `Set-BrokerDesktopGroup`. Beispiel:

  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop"-MachineCost 0.2`

### New-BrokerPowerTimeScheme

Erstellt ein BrokerPowerTimeScheme für eine Bereitstellungsgruppe. Weitere Informationen finden Sie unter https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerPowerTimeScheme/.

#### Beispiel

Angenommen, Sie möchten ein Energiezeitschema für die Bereitstellungsgruppe mit dem UID-Wert 3 erstellen. Das neue Schema gilt für Wochenenden, Montage und Dienstage. Der Zeitraum von 8:00 bis 18:30 Uhr gilt als Spitzenzeit für die Tage im ausgewählten Zeitplan. Für Spitzenzeiten beträgt die Poolgröße (die Anzahl der eingeschalteten Maschinen) 20. Für Nebenzeiten sind es 5 Maschinen. Sie können den PowerShell-Befehl `Set-BrokerDesktopGroup` verwenden. Beispiel:

```
PS C:\> $ps48=(0..47 | %{ if ($_ -lt 16 -or $_ -gt 37){ 5 } else
{ 20 } } )
PS C:\> $pt48=(0..47 | %{ if ($_ -lt 16 -or $_ -gt 37){ $false }
else { $true } } )
PS C:\> New-BrokerPowerTimeScheme -Name 'First Half Week'-DaysOfWeek
 Weekend,Monday,Tuesday -DesktopGroupUid 3 -PeakHalfHours $pt48 -
PoolSize $ps48
```

### Parameter für dynamische Sitzungstimeouts

Die folgenden Broker PowerShell SDK-Cmdlets wurden für dynamische Sitzungstimeouts erweitert, indem mehrere neue Parameter unterstützt werden:

- Get-BrokerDesktopGroup
- New-BrokerDesktopGroup
- Set-BrokerDesktopGroup

Zu diesen Parametern gehören:

- **DisconnectPeakIdleSessionAfterSeconds:** Zeit in Sekunden, nach der eine Leerlaufsitzung während der Spitzenzeit getrennt wird. Die Eigenschaft hat den Standardwert 0 und das zugehörige Verhalten während der Spitzenzeit ist somit deaktiviert. Ein Wert über 0 aktiviert das Verhalten für die Bereitstellungsgruppe während der Spitzenzeit.
- **DisconnectOffPeakIdleSessionAfterSeconds:** Zeit in Sekunden, nach der eine Leerlaufsitzung während der Nebenzeit getrennt wird. Die Eigenschaft hat den Standardwert 0 und das zugehörige Verhalten während der Nebenzeit ist somit deaktiviert. Ein Wert über 0 aktiviert das Verhalten für die Bereitstellungsgruppe während der Nebenzeit.
- **LogoffPeakDisconnectedSessionAfterSeconds:** Zeit in Sekunden, nach der eine getrennte Sitzung während der Spitzenzeit beendet wird. Die Eigenschaft hat den Standardwert 0 und das zugehörige Verhalten während der Spitzenzeit ist somit deaktiviert. Ein Wert über 0 aktiviert das Verhalten für die Bereitstellungsgruppe während der Spitzenzeit.
- **LogoffOffPeakDisconnectedSessionAfterSeconds:** Zeit in Sekunden, nach der eine getrennte Sitzung während der Nebenzeit beendet wird. Die Eigenschaft hat den Standardwert 0 und das zugehörige Verhalten während der Nebenzeit ist somit deaktiviert. Ein Wert über 0 aktiviert das Verhalten für die Bereitstellungsgruppe während der Nebenzeit.

#### Beispiel

Einsatzbeispiel: Sie möchten das Timeout für Leerlaufsitzungen während der Spitzenzeit für die Bereitstellungsgruppe "MyDesktop"auf 3.600 Sekunden einstellen. Verwenden Sie den PowerShell-Befehl `Set-BrokerDesktopGroup`. Beispiel:

- ```
  C:\PS> Set-BrokerDesktopGroup "MyDesktop"-DisconnectOffPeakIdleSessionAfte
  3600
  ```

Dadurch werden in der Nebenzeit Sitzungen der Bereitstellungsgruppe "MyDesktop"getrennt, die länger als eine Stunde im Leerlauf sind.

## Citrix Insight Services

June 27, 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 linken Bereich von Web Studio den Knoten **Einstellungen** und deaktivieren Sie die Einstellung für das **Citrix Programm zur Verbesserung der Benutzerfreundlichkeit**.

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 Telemetriediensts festgelegt werden (z. B. C:\Programme\Citrix\Telemetry Service\)

### Aktivieren von Call Home während der Komponenteninstallation

**VDA-Installation/-Upgrade:** Wenn Sie einen Virtual Delivery Agent über die grafische Benutzeroberfläche des Produktinstallationsprogramms installieren oder aktualisieren, werden Sie gefragt, ob Sie an Call Home teilnehmen möchten. Es gibt zwei Optionen:

- An Call Home teilnehmen
- Nicht an Call Home teilnehmen

Wenn Sie einen VDA aktualisieren und zuvor für Call Home registriert waren, wird diese Seite des Assistenten nicht angezeigt.

**Controller-Installation/-Upgrade:** Wenn Sie einen Delivery Controller über die grafische Benutzeroberfläche installieren oder aktualisieren, werden Sie gefragt, ob Sie an Call Home teilnehmen 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.

  ```
  $cred = Get-Credential
  Enable-CitrixCallHome -Credential $cred
  <!--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.

  ```
  $timespan = New-TimeSpan – Hours hours -Minutes minutes
  ```

```
Set-CitrixCallHomeSchedule -TimeOfDay $timespan -DayOfWeek day
    -UploadFrequency {
Daily|Weekly }

<!--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.

```
$timespan = New-TimeSpan -Hours 22 -Minutes 20
Set-CitrixCallHomeSchedule -TimeOfDay $timespan -UploadFrequency Daily
<!--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.

```
$timespan = New-TimeSpan -Hours 22 -Minutes 20
Set-CitrixCallHomeSchedule -TimeOfDay $timespan -DayOfWeek Wed -
    UploadFrequency Weekly
<!--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.

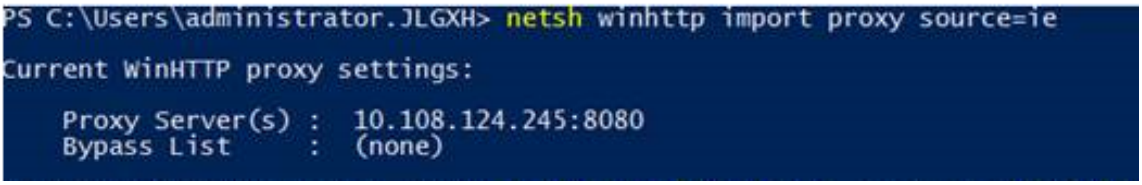
```
Enable-CitrixTrace -Listen'{ "trace":{ "enabled":false,"persistDirectory
":"C:\Users\Public","maxSizeBytes":1000000, "sliceDurationSeconds
":300 } } '
```

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.

```
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 "{
 'wmi':{
 'enabled':false }
  }
 " -UploadHeader "{
 'key1':'value1' }
 " -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

June 27, 2024

### Einführung

Citrix Scout sammelt Diagnosen und führt Systemintegritätsprüfungen durch. Sie können die Ergebnisse zur Pflege 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, Virtual Delivery Agents (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.

> **Hinweis:**
>
> Die Prozeduren **Ablauf verfolgen und reproduzieren**, **Zeitplan** und **Integritätsprüfung** sind derzeit für Linux VDA nicht verfügbar.

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 DaaS (ehemals 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 %PROGRAMDATA%\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.

### Scout-Konfiguration

Scout kann für Linux VDAs konfiguriert werden. Weitere Informationen zum Linux VDA und Telemetrie finden Sie unter Integration in den Citrix Telemetriedienst.

Auf dem Linux-VDA ändert sich möglicherweise automatisch der `ctxtelemetry`-Socketport oder der Port für den Telemetriedienst. In diesem Fall müssen Sie den Port manuell konfigurieren.

1. Navigieren Sie zu C:\Programme\Citrix\Telemetry Service
2. Öffnen Sie die Datei ScoutUI.exe.config.
3. Ändern Sie den Wert von LinuxVDATelemetryServicePort oder LinuxVDATelemetryWakeupPort gemäß der Konfiguration auf dem Linux-VDA:

- `<add key="LinuxVDATelemetryServicePort"value="7502"/>`

- `<add key="LinuxVDATelemetryWakeupPort"value="7503"/>`

1. Speichern Sie die Änderungen und schließen Sie die Datei.
2. Öffnen Sie Scout erneut, um sicherzustellen, dass die neueste Konfiguration geladen wird.

## 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 Sitzungsstarts auf VDAs überprüft Scout Folgendes:

- Verfügbarkeit der Sitzungsstart-Kommunikationsports
- Status der Sitzungsstartdienste
- Windows-Firewallkonfiguration für den Sitzungsstart
- Clientzugriffslizenzen für VDA-Remotedesktopdienste
- VDA-Anwendungsstartpfad
- Registrierungseinstellungen für den Sitzungsstart

Für die Zeitzonenumleitung auf VDAs überprüft Scout Folgendes:

- Windows-Hotfixinstallation
- Citrix Hotfixinstallation
- Microsoft-Gruppenrichtlinieneinstellungen
- Citrix Gruppenrichtlinieneinstellungen

Für die Profilverwaltung auf VDAs überprüft Scout Folgendes:

- Hypervisor-Erkennung
- Provisioning-Erkennung
- Citrix Virtual Apps and Desktops
- Konfiguration persönlicher vDisks
- Benutzerspeicher
- Profilverwaltungsdienst-Statuserkennung
- Winlogon.exe-Hookingtest

Für Prüfungen der Profilverwaltung muss diese auf dem VDA installiert und aktiviert sein. Weitere Informationen zur Prüfung der Konfiguration der Profilverwaltung finden Sie im Knowledge Center-Artikel CTX132805.

#### 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 die 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.

### 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. Klicken Sie auf **Maschine suchen**, um Maschinen zu finden. 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 und VDA-Maschinen) finden Sie unter Manuelles Hinzufügen von Maschinen und Importieren von VDA-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

### 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.
  - Legen Sie die Skriptausführungsrichtlinie mindestens auf `RemoteSigned` fest, damit die Skripts ausgeführt werden können. Beispiel: `Set-ExecutionPolicy RemoteSigned`. **Hinweis:** Andere Skriptausführungsberechtigungen funktionieren ggf. auch.
- 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.

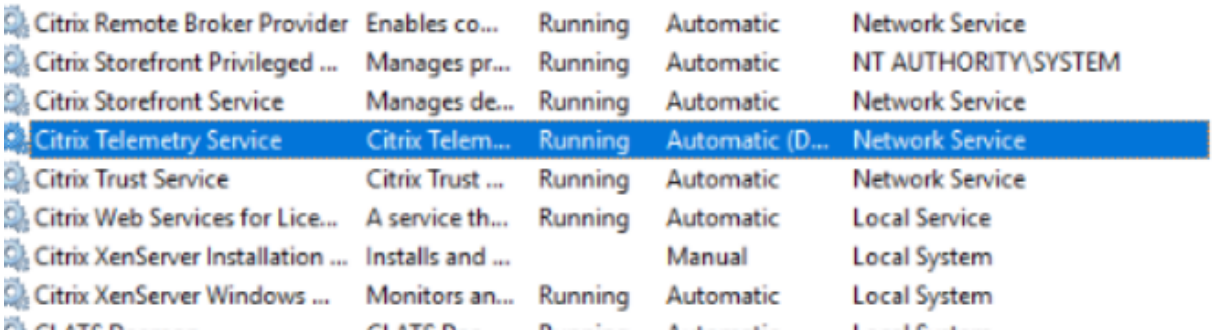
 

- Um einen Zeitplan für die Diagnoseerfassung festzulegen, muss auf der Maschine eine kompatible Scout-Version ausgeführt werden.

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.

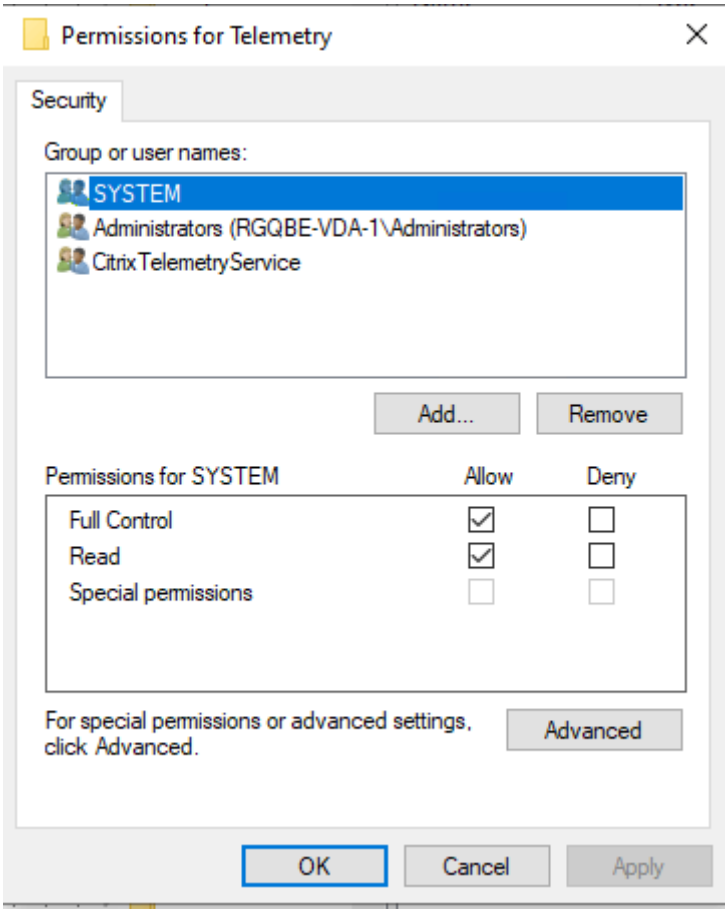
Der Telemetriedienst für Windows wird unter dem Netzwerkdienst ausgeführt.




Der Ordner "AOT Trace"wird in `C:\ProgramData\Citrix\TelemetryService\CitrixAOT` gespeichert.

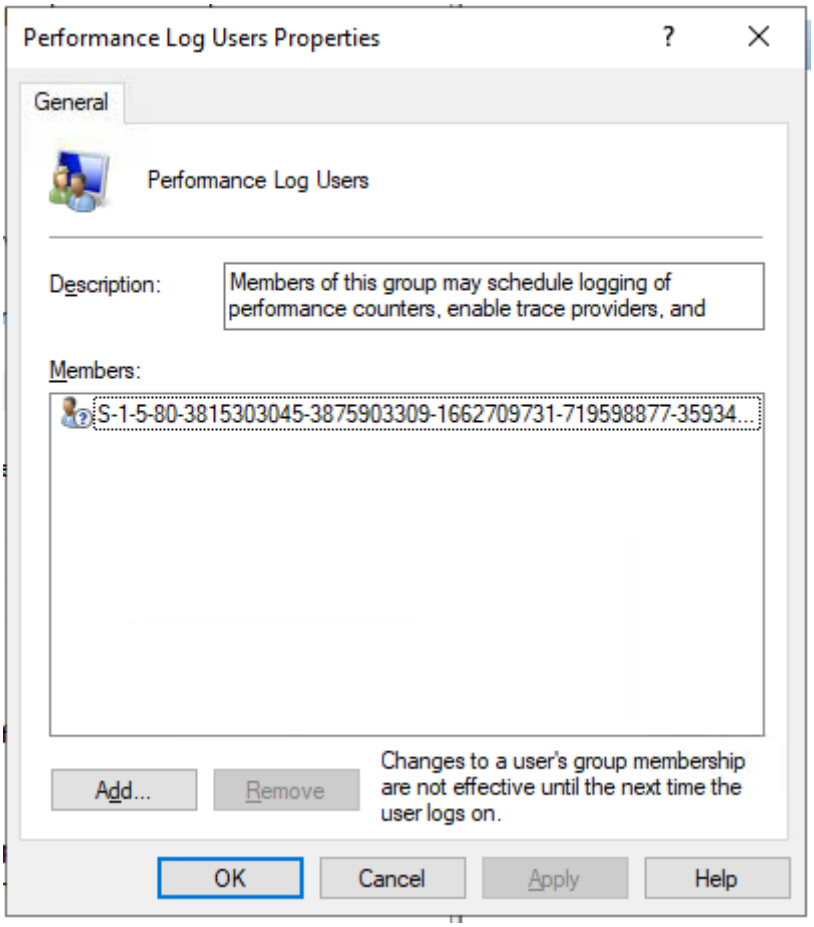
Nur Benutzer in der Administratorgruppe, das System und die Telemetriedienst-SID haben Zugriff auf `HKEYLOCALMACHINE:SOFTWARE\Citrix\Telemetry` in der Registrierung.




Die Telemetriedienst-SID verbleibt nach der Deinstallation des Telemetriediensts in der Gruppe "Leistungsprotokollbenutzer". Sie können sie jedoch manuell entfernen.




### 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.
- **Scout kann keine Verbindung zu Systemd-Socket auf diesem Computer herstellen:** Stellen Sie Folgendes sicher:
  - Port 7503 ist geöffnet. Stellen Sie sicher, dass systemd ctxtelemetry.socket Port 7503 auf der Maschine überwacht. Der Port kann anders sein, wenn der ctxtelemetry.socket-Port geändert wurde. Siehe Scout-Konfiguration zum Ändern der Ports.
  - Die Verbindung mit dem Netzwerk funktioniert ordnungsgemäß. (Dazu gehört u. U. eine Überprüfung der ordnungsgemäßen Konfiguration der Firewall.)
- **Der Linux VDA-Telemetriedienst wurde auf diesem Computer nicht gestartet:** Stellen Sie sicher dass:
  - Port 7502 geöffnet ist. Stellen Sie sicher, dass der Linux VDA-Telemetriedienst auf der Maschine installiert ist und gestartet wurde. Der Port ist ggf. anders, wenn der Telemetriedienst-Port geändert wurde. Siehe Scout-Konfiguration zum Ändern der Ports.
  - Die Verbindung mit dem Netzwerk funktioniert ordnungsgemäß. (Dazu gehört u. U. eine Überprüfung der ordnungsgemäßen Konfiguration der Firewall.)

### 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, 7.1–7.13 | Ja | Nein |
| Unterstützung von XenApp 6.x, 7.5 bis 7.13 | Ja | Nein |
| Erhältlich mit Produkt | 7.1–7.13 | 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 | – | Ja |

| Feature | Scout 2.23 | Scout 3.0 |
|---|---|---|
| Unterstützung von Skripts | Befehlszeile (nur lokaler Controller) | PowerShell mit Call Home-Cmdlets (jede Maschine mit installiertem Telemetriedienst) |
| Integritätsprüfungen | Nein | Ja |
| 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 auf der Maschine nicht aktualisieren, wird sie 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.

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** ak-

tivieren 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.

### Maschine suchen

Für die Prozeduren **Sammeln**, **Ablauf verfolgen und reproduzieren** und **Planen** listet Scout die automatisch erkannten Controller und VDAs auf.

Wenn Sie Scout Health Check über den Delivery Controller ausführen, klicken Sie auf **Maschine suchen**, um Delivery Controller, VDAs, Lizenzserver und StoreFront-Server zu ermitteln.

Wenn Sie Scout Health Check auf einer domänengebundenen Maschine ausführen, die kein Delivery Controller ist, kann Scout Maschinen nicht automatisch ermitteln. Sie müssen Maschinen manuell hinzufügen oder VDA-Maschinen importieren.

### 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.

### VDA-Maschinen importieren

Sie können VDA-Maschinen in die Bereitstellung importieren, wenn Sie Integritätsprüfungen ausführen.

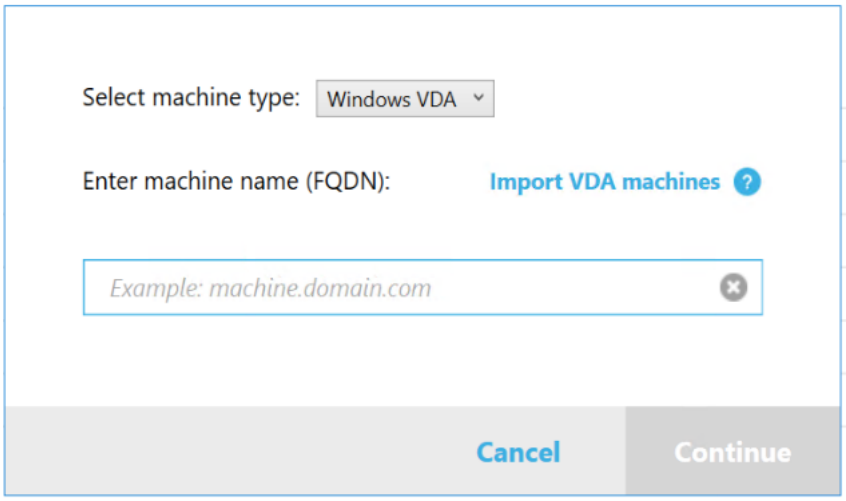
1. Generieren Sie auf dem Delivery Controller oder Connector die Maschinenlistendatei mit dem PowerShell-Befehl. Auf dem Connector müssen Sie Citrix Anmeldeinformationen eingeben und den Kunden im Dialogfeld auswählen.

   ```
   Get-BrokerMachine| foreach { $_.DnsName } | out-file C:\machineList
   .txt
   ```

2. Kopieren Sie die Datei machineList.txt auf die domänengebundene Maschine, auf der Sie Scout Health Check starten möchten.
3. Klicken Sie auf der Scout Health Check-Seite auf **Maschine hinzufügen**.
4. Wählen Sie den Maschinentyp **Windows-VDA** aus.
5. Klicken Sie auf **VDA-Maschinen importieren**.
6. Wählen Sie die Datei machineList.txt aus.
7. Klicken Sie auf **Öffnen**.

Die importierten VDA-Maschinen werden auf der Scout Health Check-Seite aufgeführt.




### Diagnosedaten sammeln

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 einem Controller auf der Seite **Maschinen wählen** werden alle VDAs und Controller der Site aufgelistet. Sie können die Anzeige nach Maschinennamen filtern. Informationen zum manuellen Hinzufügen weiterer Maschinen (z. B. von StoreFront- oder Citrix Provisioning-Servern) finden Sie unter Manuelles Hinzufügen von Maschinen.
   - Bei anderen Komponenten (z. B. VDA-Servern) wird auf der Seite **Maschinen auswählen** nur die lokale Maschine aufgeführt. Manuelles Hinzufügen von Maschinen wird nicht unterstützt.

   Aktivieren Sie das Kontrollkästchen neben jeder Maschine, auf der Sie Diagnosedaten sammeln möchten, und klicken Sie auf **Weiter**.

   Scout überprüft automatisch jede ausgewählte Maschine auf Erfüllung der unter Tests zur Überprüfung aufgeführten Kriterien. Wenn eine Maschine die Überprüfung nicht besteht, wird eine Meldung in der Spalte **Status** angezeigt und das Kontrollkästchen deaktiviert. Sie haben nun folgende Möglichkeiten:

   - Beheben Sie das Problem und aktivieren Sie das Kontrollkästchen erneut. Dadurch wird eine Wiederholung des Tests ausgelöst.
   - Überspringen Sie die Maschine (Kontrollkästchen deaktiviert lassen). Auf ihr werden dann keine Diagnosedaten gesammelt.

Nach Abschluss der Überprüfung klicken Sie auf **Weiter**.

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:

   - Ein Windows-Dialogfeld zum **Speichern** wird 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 **Continue**. 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 Kontrollkästchen 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 Ablaufverfolgungs-/Diagnosedaten 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 **Continue**. 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.

### Sammeln zusätzlicher Protokolle aktivieren

Wenn Sie das **Sammeln zusätzlicher Protokolle** aktivieren, können Sie die Trace- und Reproduktionsfunktion mit weiteren Tools wie perfmon, Netsh, DebugView und Wireshark verwenden.

> **Hinweis:**
>
> Dies gilt nur für lokale Maschinen.

So richten Sie das Sammeln zusätzlicher Protokolle ein:

1. Starten Sie Citrix Scout.
2. Klicken Sie auf **Einstellungen** (Zahnradsymbol).
3. Klicken Sie auf **Enable additional log collection with more tools**.
4. Klicken Sie auf **Speichern**.

So sammeln Sie zusätzliche Protokolle:

1. Klicken Sie auf der Homepage von Scout auf **Ablauf verfolgen und reproduzieren**.
2. Klicken Sie auf der Seite **Maschine auswählen** auf das Zahnrad auf der rechten Seite der lokale Maschine.
3. Klicken Sie auf der Seite **Select the tools required for logging** auf **Download Tools**.
4. Wählen Sie auf der Seite **Download Tools** die Tools aus, die Sie verwenden möchten, und klicken Sie auf **Download**. Die Tools werden dann heruntergeladen, mit Ausnahme von Wireshark. Wireshark kann nur manuell heruntergeladen und installiert werden.
   Hinweis: Wenn Sie andere Tools manuell herunterladen möchten, müssen Sie den Inhalt der heruntergeladenen ZIP-Datei in `C:\ProgramData\Citrix\TelemetryService\CDC\Lib\Resources\Tools\<toolname>` extrahieren. Wenn Sie beispielsweise die Datei DebugView.zip herunterladen, entpacken Sie den Inhalt der Datei in `C:\ProgramData\Citrix\TelemetryService\CDC\Lib\Resources\Tools\DebugView\`.
5. Klicken Sie auf der Seite **Select the tools required for logging** auf **Refresh Status**. Alle ausgewählten Tools werden in der Spalte Status als **Present** angezeigt.
6. Wählen Sie die Tools zum Protokollieren aus und klicken Sie dann auf **Weiter**.
7. Folgen Sie den Anweisungen zum Verfolgen und Reproduzieren von Abläufen.
8. Überprüfen Sie nach Abschluss die Protokolle in der Zip-Datei. Die Protokolle werden im Ordner *CDCLogs* gezippt.

> **Hinweis:**
>
> Wenn das Procmon-Tool für die Ablaufverfolgung ausgewählt ist, können die Process Monitor-Protokolle schnell groß werden. Stellen Sie sicher, dass Sie nur die benötigten Tools auswählen. Sie können die Größe der Protokolle auch unter *%temp%\Scout-CDC-Log*überwachen.

### 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 Diagnosedaten (oder Ablaufverfolgungsdaten) gesammelt.

   Nach Abschluss der Überprüfung klicken Sie auf **Weiter**.

   Auf der Seite Zusammenfassung werden die Maschinen aufgelistet, auf die der Zeitplan angewendet wird. Klicken Sie auf **Continue**.
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 **Continue**.

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 **Continue**.

   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.

## Datenmaskierung

Die mit Citrix Scout gesammelten Diagnoseinformationen enthalten möglicherweise vertrauliche Daten. Mit der Citrix Scout-Datenmaskierung können Sie vertrauliche Daten in Diagnosedateien maskieren, bevor Sie sie in Citrix hochladen.

Mit der Scout-Datenmaskierung können IP-Adressen, SIDs und die Namen von Maschinen, Domänen, Benutzern, Hypervisors, Bereitstellungsgruppen, Katalogen und Anwendungen maskiert werden.

> **Hinweis:**
>
> CDF-Traces sind verschlüsselt und können nicht maskiert werden.
>
> Linux VDA-Protokolle werden im `.tar.gz2`-Format komprimiert und können nicht maskiert werden.

#### Erfassung neuer Diagnoseinformationen und Ausführen einer Datenmaskierung

Um die Citrix Scout-Datenmaskierungsfunktion zu verwenden, starten Sie Scout über die Befehlszeile.

1. Öffnen Sie in Windows die Eingabeaufforderung als Administrator.
2. Wechseln Sie zum Verzeichnis, in dem Scout installiert ist: `cd C:\Program Files\Citrix\Telemetry Service`.
3. Starten Sie Scout: `ScoutUI.exe datamasking`.
4. Klicken Sie auf **Sammeln** oder **Ablauf verfolgen und reproduzieren**, um Diagnosedaten zu sammeln.
5. Nachdem die Sammlung abgeschlossen ist, wählen Sie **Datenmaskierung aktivieren**. Diese Option ist standardmäßig aktiviert.
6. Konfigurieren Sie die Datenmaske. Sie können die Standardregeln verwenden oder die Regeln anpassen.
7. Wählen Sie aus, ob Sie die Diagnosesammlung hochladen oder speichern möchten.
    - Bei Auswahl von **Gesammelte Diagnosedaten zu Citrix hochladen** werden die maskierten Diagnosedateien in Citrix hochgeladen.
    - Wenn Sie **Diagnosedaten auf lokaler Maschine speichern** wählen, werden die ursprünglichen und die maskierten Diagnosedaten am angegebenen Speicherort gespeichert.

#### Datenmaskierung bei bestehenden Diagnosedaten

1. Öffnen Sie in Windows die Eingabeaufforderung als Administrator.
2. Wechseln Sie zum Verzeichnis, in dem Scout installiert ist: `cd C:\Program Files\Citrix\Telemetry Service`.
3. Starten Sie Scout direkt im Datenmaskierungsmodus: `ScoutUI.exe datamasking filePath`.
4. Wählen Sie "Enable data masking", um fortzufahren. Diese Option ist standardmäßig aktiviert.

5. Konfigurieren Sie die Datenmaske. Sie können die Datenmaskierung mit den Standardregeln ausführen oder die Regeln anpassen.
6. Wählen Sie aus, ob Sie die Diagnosesammlung hochladen oder speichern möchten.
    - Bei Auswahl von **Gesammelte Diagnosedaten zu Citrix hochladen** werden die maskierten Diagnosedateien in Citrix hochgeladen.
    - Wenn Sie **Diagnosedaten auf lokaler Maschine speichern** wählen, werden die ursprünglichen und die maskierten Diagnosedaten am angegebenen Speicherort gespeichert.

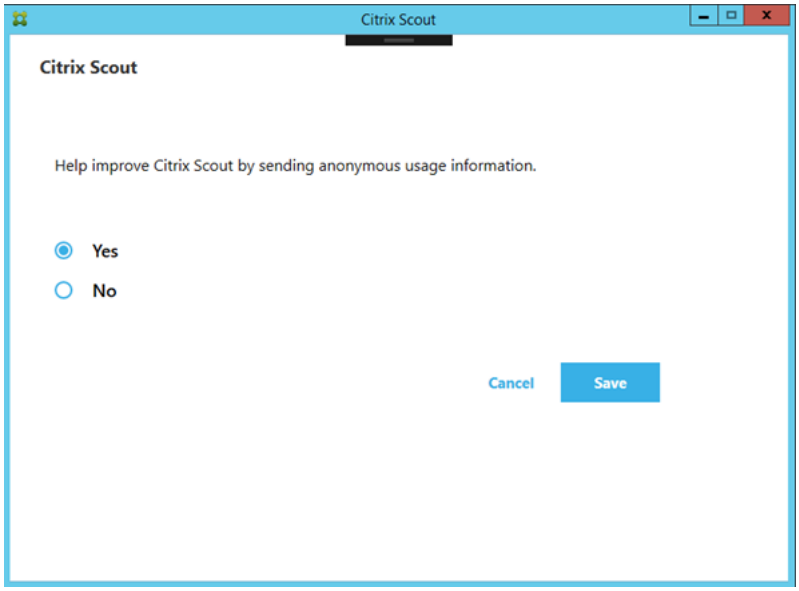
#### Speicherorte der maskierten Datendatei und der Zuordnungsdatei

Nach dem Hochladen oder Speichern der Diagnosesammlung klicken Sie auf den Link, um die ursprüngliche und die maskierte Diagnose zu öffnen, und öffnen die Zuordnungsinformationsdatei.

### Erfassung von Nutzungsdaten

Wenn Sie Scout verwenden, erfasst Citrix mit Google Analytics anonyme Nutzungsdaten, die für zukünftige Produktfeatures und Verbesserungen verwendet werden. Die Datenerfassung ist standardmäßig aktiviert.

Um die Erfassung und den Upload von Nutzungsdaten zu ändern, klicken Sie auf das **Einstellungen**-Zahnradsymbol in der Scout-Benutzeroberfläche. Wählen Sie dann durch Klicken auf **Ja** oder **Nein** aus, ob die Informationen gesendet werden sollen, und klicken Sie auf **Speichern**.



# Aufzeichnen einer Citrix Diagnostic Facility (CDF)-Trace beim Systemstart

June 27, 2024

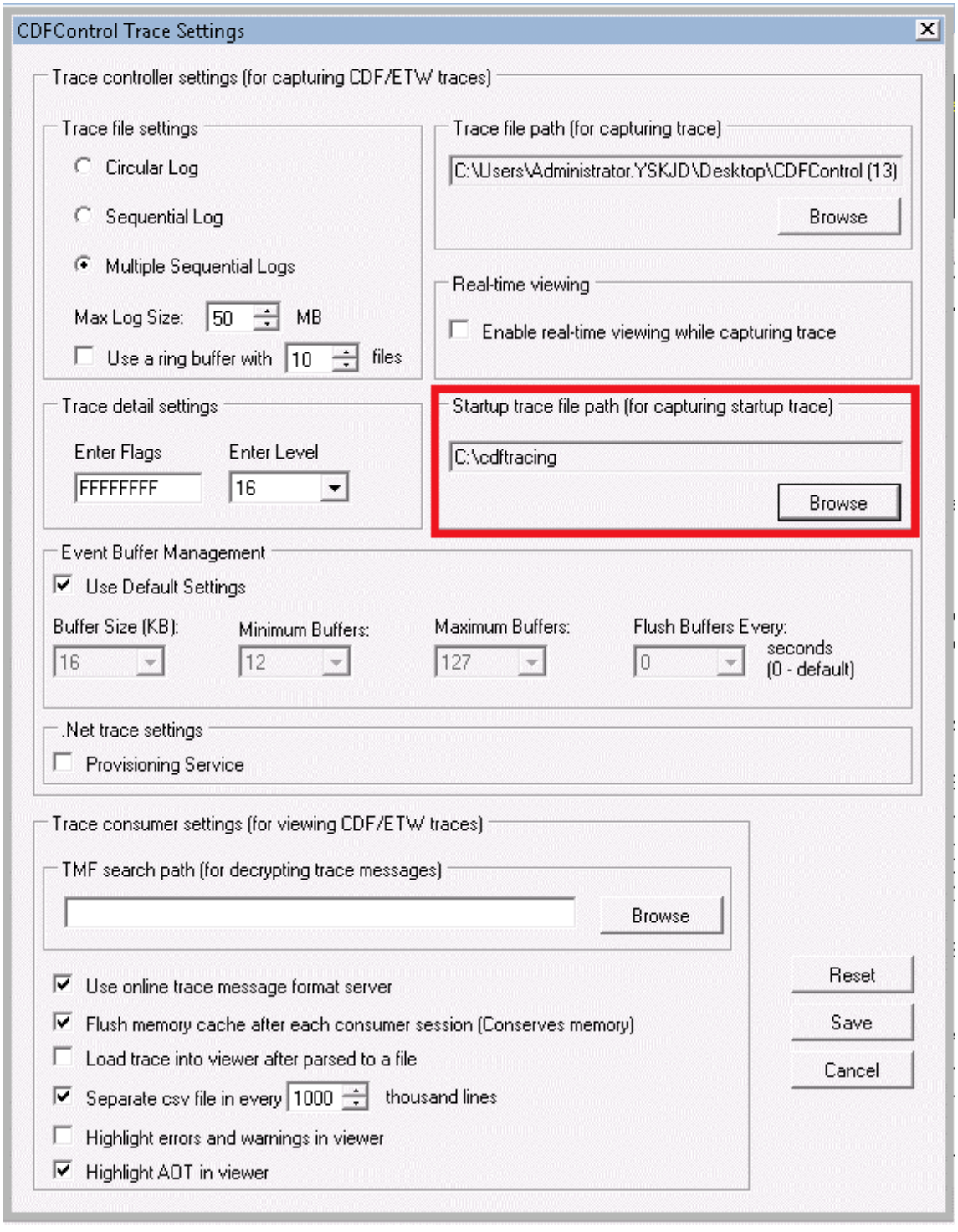
Das Hilfsprogramm CDFControl ist ein Ablaufverfolgungscontroller zum Erfassen der CDF-Meldungen der verschiedenen Citrix Ablaufverfolgungsanbieter. Es wurde entwickelt, um komplexe Probleme mit Citrix Systemen zu beheben, die Filterunterstützung zu analysieren und Leistungsdaten zu erfassen. Informationen zum Download von CDFControl finden Sie unter CTX111961.

## Aufzeichnen einer Trace beim Systemstart

Zum Aufzeichnen eines CDF-Tracingberichts beim Systemstart verwenden Sie das folgende Verfahren. Sie benötigen Administratorrechte.

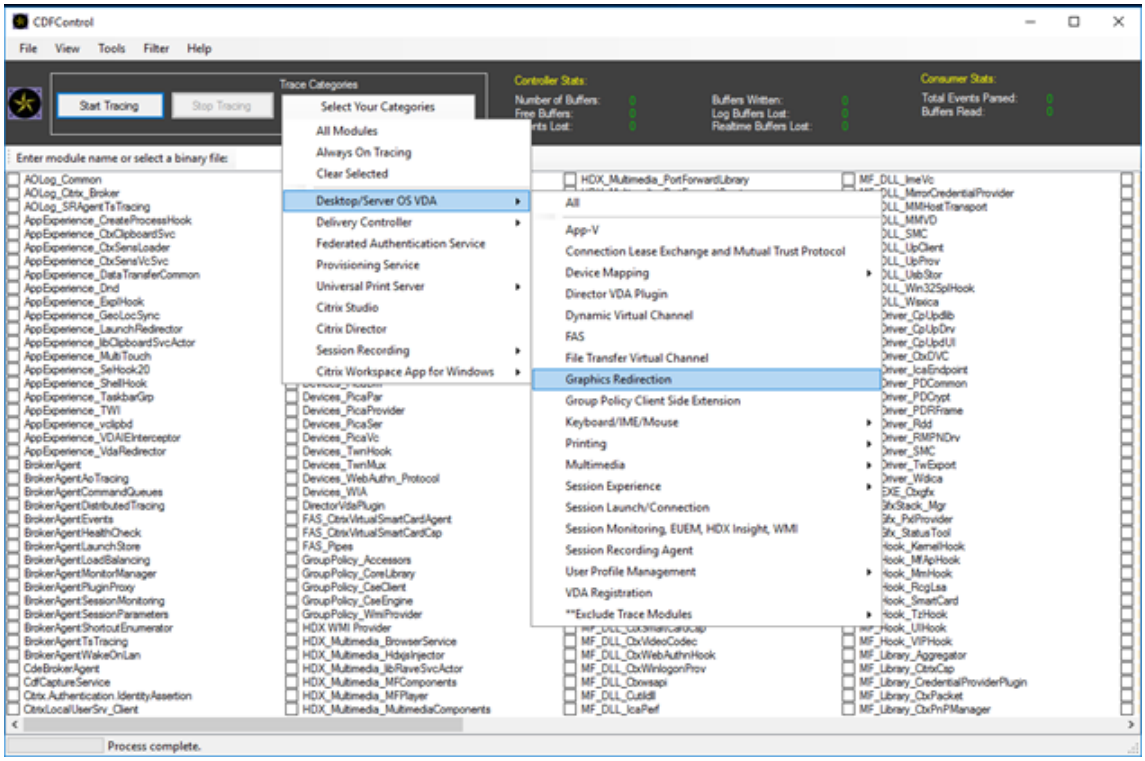
1. Starten Sie **CDFControl** und wählen Sie **Options** im Menü **Tools**.
2. Geben Sie im Abschnitt **Startup trace file path for capturing startup trace** den Pfad für die Systemstart-Tracedatei ein. Klicken Sie auf **Speichern**.




3. Wählen Sie unter **Trace Categories** die vom Citrix Support empfohlenen Kategorien. (Im folgenden Beispiel ist die **Grafikumleitung** ausgewählt. Diese Auswahl ist nur ein Beispiel. Citrix empfiehlt, dass Sie die Anbieter für das spezifische Problem aktivieren, das Sie beheben möchten.)




4. Wählen Sie **Startup Tracing** gefolgt von **Enable** im Menü **Tools**.

   Nach Auswahl von **Enable** beginnt die Leiste zu scrollen. Diese Aktivität hat keinen Einfluss auf das Verfahren. Fahren Sie mit dem nächsten Schritt fort.

5. Schließen Sie nach dem Aktivieren von **Startup Tracing** das Hilfsprogramm **CDFControl** und starten Sie das System neu.

6. Starten Sie das Hilfsprogramm **CDFControl**. Nachdem das System neu gestartet wurde und der Fehler angezeigt wird, deaktivieren Sie die Option durch Auswählen von **Startup Tracing** im Menü **Tools** und Auswählen von **Disable**.

7. Gehen Sie zum in Schritt 2 festgelegten Speicherort der Tracingdatei und sammeln Sie die Protokolldatei (.etl) zur Analyse.

## Delegierte Administration

June 27, 2024

> **Hinweis:**
>
> Sie können Ihre Citrix Virtual Apps and Desktops-Bereitstellung mithilfe von zwei Verwaltungskonsolen verwalten: Web Studio (webbasiert) und Citrix Studio (Windows-basiert). Dieser

> Artikel behandelt nur Web Studio. Informationen zu Citrix Studio finden Sie im entsprechenden Artikel in Citrix Virtual Apps and Desktops 7 2212 oder früher.

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). |

| Rolle | Berechtigungen |
| --- | --- |
| 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. |
| 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 funktionale 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.

Führen Sie folgende Schritte aus, um Administratoren zu erstellen und zu verwalten:

1. Melden Sie sich bei Web Studio an, klicken Sie im linken Bereich auf **Administratoren** und klicken Sie dann auf die Registerkarte **Administratoren**.
2. Folgen Sie den Anweisungen für die Aufgabe, die Sie ausführen möchten:

    - **Erstellen eines Administrators:** Klicken Sie in der Aktionsleiste auf **Administrator erstellen**. Geben Sie den Namen eines Benutzerkontos ein oder navigieren Sie 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 aus und klicken Sie in der Aktionsleiste 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 aus und klicken Sie in der Aktionsleiste auf **Administrator bearbeiten**. Sie können die Rollen-/Geltungsbereichspaare bearbeiten oder löschen und neue hinzufügen.
    - **Löschen eines Administrators:** Wählen Sie den Administrator aus und klicken Sie in der Aktionsleiste 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

> **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 in der Aktionsleiste auf **Administrator bearbeiten**.
    2. Wählen Sie im Fenster **Administratorname und -details** das Rollen-/Bereichspaar aus und klicken Sie auf **Löschen**.
    3. Klicken Sie zum Schluss auf **Speichern**.

- Löschen Sie den Administrator.

    1. Klicken Sie in der Aktionsleiste auf **Administrator löschen**.
    2. Klicken Sie im Bestätigungsfenster 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 benutzerdefinierte Rollen unterstützen, haben diese Einträge in der Aktionsleiste.

Führen Sie folgende Schritte aus, um Rollen zu erstellen und zu verwalten:

1. Melden Sie sich bei Web Studio an, klicken Sie im linken Bereich auf **Administratoren** und klicken Sie dann auf die Registerkarte **Rollen**.
2. Folgen Sie den Anweisungen für die Aufgabe, die Sie ausführen möchten:

    - **Anzeigen von Rollendetails:** Wählen Sie die Rolle aus. Im unteren Bereich werden die Objekttypen und die zugehörigen Berechtigungen für die Rolle angezeigt. Klicken Sie im unteren Bereich auf die Registerkarte **Administratoren**, um eine Liste der Administratoren anzuzeigen, die derzeit diese Rolle haben.

- **Erstellen einer benutzerdefinierten Rolle**: Klicken Sie in der Aktionsleiste 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 und klicken Sie in der Aktionsleiste auf **Rolle kopieren**. Ändern Sie den Namen und die Beschreibung sowie die Objekttypen und Berechtigungen nach Bedarf.
- **Bearbeiten einer benutzerdefinierten Rolle:** Wählen Sie die Rolle und klicken Sie in der Aktionsleiste auf **Rolle bearbeiten**. Ändern Sie den Namen und die Beschreibung sowie die Objekttypen und Berechtigungen nach Bedarf.
- **Löschen einer benutzerdefinierten Rolle:** Wählen Sie die Rolle und klicken Sie in der Aktionsleiste 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.

Regeln zum Erstellen und Verwalten von Geltungsbereichen:

- 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.
- Geltungsbereichsbeschreibungen 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.

Führen Sie folgende Schritte aus, um Geltungsbereiche zu erstellen und zu verwalten:

1. Melden Sie sich bei Web Studio an, klicken Sie im linken Bereich auf **Administratoren** und klicken Sie auf die Registerkarte **Geltungsbereiche**.
2. Folgen Sie den Anweisungen für die Aufgabe, die Sie ausführen möchten:
   - **Erstellen eines Geltungsbereichs:** Klicken Sie in der Aktionsleiste 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.
   - **Kopieren eines Geltungsbereichs:** Wählen Sie den Geltungsbereich und klicken Sie in der Aktionsleiste auf **Geltungsbereich kopieren**. Geben Sie einen Namen und eine Beschreibung ein. Ändern Sie bei Bedarf die Objekttypen und Berechtigungen.
   - **Bearbeiten eines Geltungsbereichs:** Wählen Sie den Geltungsbereich und klicken Sie in der Aktionsleiste auf **Geltungsbereich bearbeiten**. Ändern Sie den Namen und die Beschreibung sowie die Objekttypen und Objekte nach Bedarf.
   - **Löschen eines Geltungsbereichs:** Wählen Sie den Geltungsbereich und klicken Sie in der Aktionsleiste 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 Web Studio.

  Führen Sie folgende Schritte aus, um den Bericht zu erstellen:

  1. Melden Sie sich bei Web Studio an und klicken Sie im linken Bereich auf **Administratoren**.
  2. Wählen Sie einen Administrator aus, und klicken Sie in der Aktionsleiste 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 |
| -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.

```
1 & "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\
2 Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"
3 -Path Roles.html  – Show
4 <!--NeedCopy-->
```

Mit dem Befehl im folgenden Beispiel wird eine CSV-Tabelle in eine Datei namens Roles.csv geschrieben. Die Tabelle wird nicht angezeigt.

```
1 & "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\
2 Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"
3  – 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-->
```

## Delivery Controller

June 27, 2024

> **Hinweis:**
>
> Sie können Ihre Citrix Virtual Apps and Desktops-Bereitstellung mithilfe von zwei Verwaltungskonsolen verwalten: Web Studio (webbasiert) und Citrix Studio (Windows-basiert). Dieser Artikel behandelt nur Web Studio. Informationen zu Citrix Studio finden Sie im entsprechenden Artikel in Citrix Virtual Apps and Desktops 7 2212 oder früher.

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 muss eine Produktionssite immer mindestens zwei Controller auf unterschiedlichen physischen Servern haben. Wenn ein Controller ausfällt, können die anderen die Verwaltung der Verbindungen und der Site übernehmen.
- **Skalierbarkeit:** Je intensiver die Aktivität einer Site, umso mehr nehmen CPU-Auslastung auf dem Controller und die Datenbankaktivität zu. Zusätzliche Controller bieten die Möglichkeit, mehr Benutzer, Anwendungen und Desktopanforderungen zu verarbeiten und die Reaktionszeit insgesamt zu verbessern.

Jeder Controller kommuniziert direkt mit der Sitedatenbank. In einer Site mit mehreren Zonen kommunizieren die Controller in jeder Zone mit der Datenbank in der primären Zone.

> **Wichtig:**
>
> Ändern Sie weder den Computernamen noch die Domänenmitgliedschaft eines Controllers,

> nachdem Sie die Site konfiguriert haben.

### Verfahren der Registrierung von VDAs bei Controllern

VDAs können erst verwendet werden, wenn sie bei einem Delivery Controller in der Site registriert wurden (Herstellen der Kommunikation). Weitere Informationen zur VDA-Registrierung finden Sie unter VDA-Registrierung bei Controllern.

### 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 Sie einer Site einen Delivery Controller hinzufügen, konfigurieren Sie Anmeldeinformationen für diese Maschine auf allen Replikatmaschinen mit SQL Server, die Sie für hohe Verfügbarkeit verwenden.

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.
- Um die Spiegelung nach dem Hinzufügen, Entfernen oder Verschieben eines Controllers zu überprüfen, führen Sie das PowerShell-Cmdlet `Get-configdbconnection` aus. Das Cmdlet stellt sicher, dass der Failoverpartner in der Verbindungszeichenfolge auf den Spiegel festgelegt 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 noch keine Site vorliegt, führen Sie Citrix Site Manager auf diesem Controller aus, um eine Site zu erstellen. Die IP-Adresse dieses Controllers wird der neuen Site automatisch hinzugefügt.

   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, gehen Sie wie folgt vor:

   a) Führen Sie Citrix Site Manager auf diesem Controller aus, klicken Sie auf **Vorhandener Site beitreten** und geben Sie die Adresse eines Controllers in der Site ein, der Sie beitreten möchten.
   b) Führen Sie das Studio-Konfigurationstool aus, um den Controller Web Studio hinzuzufügen.

### 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 Web 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.

Nachdem Sie einen Controller entfernt haben:

- VDAs, die automatische Updates verwenden, werden neu bei anderen verfügbaren Controllern registriert. Diese Neuregistrierung erfolgt nur, wenn automatische Updates aktiviert sind und

die VDAs andere Controller erreichen können (in derselben sekundären Zone wie der entfernte Controller oder in der primären Zone für On-Premises-Bereitstellungen).

- Aktualisieren Sie Controllerinformationen in Citrix StoreFront. Weitere Informationen finden Sie unter Controller verwalten.
- Aktualisieren Sie in Citrix StoreFront die Secure Ticket Authority (STA)-URLs für den Remotezugriff über Citrix Gateway. Weitere Informationen finden Sie unter Verwalten von Secure Ticket Authorities.
- Aktualisieren Sie in Citrix Gateway alle STA-URLs für virtuelle Server. Weitere Informationen finden Sie unter Citrix Gateway.

> **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 Web Studio in weniger als einer Stunde geladen wird. Sobald Web Studio den zu entfernenden Controller geladen hat, müssen alle Dienste auf dem Controller ausgeführt werden und der Controller ausgeschaltet sein.
2. Melden Sie sich bei Web Studio an und wählen Sie im linken Bereich **Einstellungen**.
3. Suchen Sie die **Delivery Controller**-Kachel und klicken Sie auf **Bearbeiten**.
4. Wählen Sie auf der Seite **Delivery Controller verwalten** den Controller, den Sie entfernen möchten.
5. Wählen Sie **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.

   Web Studio führt vor dem Entfernen eines Controllers eine Vorabprüfung durch. Ein Controller kann sicher entfernt werden, wenn er ausgeschaltet ist und sich nicht im folgenden Dienststatus befindet:

   - Unbekannt
   - Ausstehender Fehler
   - Ältere Version
   - Neuere Version
   - Versionsänderung wird ausgeführt
   - Obligatorische Feature fehlen

   Wenn der Controller nicht ausgeschaltet ist und sich in einem oben genannten Dienststatus befindet, fordert Web Studio Sie auf, den Controller auszuschalten.
6. Sie müssen das Maschinenkonto des Controllers auf dem Datenbankserver entfernen. Überprüfen Sie vor dem Entfernen, ob das Konto von einem anderen Dienst verwendet wird.

Nachdem Sie mit Web 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 dieses Verschieben auf die VDA-Registrierung und andere Vorgänge auswirken kann.

1. Wählen Sie im linken Bereich **Zone**.
2. Wählen Sie im mittleren Bereich eine Zone und wählen Sie dann einen Controller.
3. Wählen Sie in der Aktionsleiste **Elemente verschieben**.
4. Wählen Sie auf der daraufhin angezeigten Seite **Elemente verschieben** die Zone aus, in die Sie den Controller verschieben möchten.
5. Klicken Sie auf **Speichern**.

#### 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 oder wenn Sie ein in einer Testsite erstelltes VDA-Image in eine Produktionssite verschieben. Mit Maschinenerstellungsdienste (MCS) bereitgestellte VDAs können nicht von einer Site in eine andere verschoben werden. MCS unterstützt nicht das Ändern der ListOfDDCs, die VDAs prüfen, um sich bei einem Controller zu registrieren. 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 eingegangene Liste der Controller (da automatische Updates deaktiviert sind) und wählt einen der in der Richtlinie angegebenen Controller, d. h. einen der Controller in Site 2.

3. Wenn der VDA erfolgreich bei einem Controller der Site 2 registriert wurde, empfängt er die Liste "ListOfDDCs"und die Richtlinieninformationen von Site 2, für die automatische Updates standardmäßig aktiviert sind. Der Controller, bei dem der VDA in Site 1 registriert war, ist nicht in der vom Controller in Site 2 gesendeten Liste ist. Daher wählt der VDA bei seiner Neuregistrierung einen Controller in der Liste von Site 2 aus. Ab sofort wird der VDA automatisch mit Informationen von Site 2 aktualisiert.

Informationen zum Verwenden des Gruppenrichtlinien-Editors finden Sie unter Citrix Richtlinien.

## Unterstützung für IPv4/IPv6

June 27, 2024

Dieses Release unterstützt reines IPv4, reines IPv6 und Bereitstellungen mit dualem Stapel, bei denen überlappende IPv4- und IPv6-Netzwerke verwendet werden.

Die folgenden Komponenten unterstützen nur IPv4. Alle anderen unterstützen IPv4 und IPv6.

- XenServer
- Nicht über die Richtlinieneinstellung **Nur IPv6-Controllerregistrierung verwenden** gesteuerte Virtual Delivery Agents (VDAs)

Die IPv6-Kommunikation wird mit zwei verbindungsspezifischen Citrix Richtlinieneinstellungen für VDAs gesteuert:

- **Primäre Einstellung, die die Verwendung von IPv6 durchsetzt:** Nur IPv6-Controllerregistrierung verwenden.

Diese Richtlinieneinstellung steuert das Format der Adresse, die vom VDA für die Registrierung beim Delivery Controller verwendet wird:

Wenn aktiviert, wird der VDA beim Controller mit einer einzelnen IPv6-Adresse registriert und verwendet sie für die Kommunikation. Die Auswahl der IPv6-Adresse unterliegt der folgenden Reihenfolge: 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. Dies ist der Standardwert.

Wenn ein Team häufig ein IPv6-Netzwerk verwendet, veröffentlichen Sie die Desktops und Anwendungen für diese Benutzer basierend auf einem Image oder einer Organisationseinheit (OU), für die die Richtlinieneinstellung **Nur IPv6-Controllerregistrierung verwenden** aktiviert ist.

Wenn ein Team häufig ein IPv4-Netzwerk verwendet, veröffentlichen Sie die Desktops und Anwendungen für diese Benutzer basierend auf einem Image oder einer Organisationseinheit, für die die Richtlinieneinstellung **Nur IPv6-Controllerregistrierung verwenden** deaktiviert ist.

- **Abhängige Einstellung, die eine IPv6-Netzmaske definiert:** IPv6-Netzwerkmaske für Controllerregistrierung.

  Eine Maschine kann mehrere IPv6-Adressen haben. Mit dieser Richtlinieneinstellung kann der VDA auf ein bevorzugtes Subnetz limitiert werden, anstelle einer globalen IP, sofern eine registriert ist. Mit dieser Einstellung geben Sie 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. Standard = leere Zeichenfolge

## Überlegungen zur Bereitstellung

Wenn Ihre Umgebung sowohl IPv4- und IPv6-Netzwerke umfasst, erstellen 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.

HINWEIS: Diese Überlegungen gelten nicht, wenn Sie die DNS-Auflösung aktiviert haben.

# Lizenzierung von Citrix Virtual Apps and Desktops über Web Studio

June 27, 2024

> **Hinweis:**
>
> Sie können Ihre Citrix Virtual Apps and Desktops-Bereitstellung mithilfe von zwei Verwaltungskonsolen verwalten: Web Studio (webbasiert) und Citrix Studio (Windows-basiert). Dieser Artikel behandelt nur Web Studio. Informationen zu Citrix Studio finden Sie im entsprechenden Artikel in Citrix Virtual Apps and Desktops 7 2212 oder früher.

Sie können die Lizenzierung in Web Studio verwalten und nachverfolgen, wenn der Lizenzserver in derselben Domäne wie Web Studio oder in einer vertrauenswürdigen Domäne ist. Informationen zu Lizenzierungsaufgaben finden Sie in der Dokumentation zur Lizenzierung und unter Multityplizenzierung.

In der folgenden Tabelle werden die unterstützten Editionen und Lizenzierungsmodelle aufgeführt:

| Produkte | Editionen | Lizenzmodelle |
|---|---|---|
| Citrix Virtual Apps | Premium, Advanced, Standard | Gleichzeitig |
| Citrix Virtual Desktops | Premium, Advanced, Standard | Benutzer/Gerät und Gleichzeitig |

Weitere Informationen finden Sie unter CCU-Lizenz und Benutzer-/Gerätelizenz.

## Unterstütztes aktuelles Release (CRs) und Long Term Service Release (LTSRs)

In der folgenden Tabelle sind die **kompatiblen LS-Mindestversionen** für Citrix Virtual Apps and Desktops, XenApp und XenDesktop aufgeführt. Weitere Informationen zu den Lebenszyklusdaten von Citrix Produkten finden Sie in der Produktmatrix.

> **Wichtig:**
>
> Die Informationen in der folgenden Tabelle dienen nur zur Information über die Produktkompatibilität. Citrix empfiehlt dringend, immer die neueste Version von Citrix Lizenzserver zu verwenden, um von den enthaltenen Funktions- oder Sicherheitsverbesserungen profitieren zu können.
>
> **Hinweis:**
>
> Lizenzserver VPX ist veraltet und erhält keine weiteren Wartungs- oder Sicherheitsfixes. Kunden, die Lizenzserver VPX 11.16.6 oder frühere Versionen verwenden, wird empfohlen, so bald wie

> möglich auf die neueste Version von License Server für Windows zu migrieren.

| Aktuelle Version | Kompatible LS-Mindestversion |
|---|---|
| 2305 | 11.17.2.0 Build 35000 |
| 2303 | 11.17.2.0 Build 35000 |
| 2212 | 11.17.2.0 Build 35000 |
| 2209 | 11.17.2.0 Build 35000 |
| 2206 | 11.17.2.0 Build 35000 |
| 2203 | 11.17.2.0 Build 35000 |
| 2112 | 11.17.2.0 Build 35000 |
| 2109 | 11.17.2.0 Build 35000 |
| 2106 | 11.17.2.0 Build 35000 |
| 2103 | 11.16.3.0 Build 28000 |

| Long Term Service Release | Kompatible LS-Mindestversion |
|---|---|
| 2203 LTSR | 11.17.2.0 Build 35000 |
| 1912 LTSR | 11.16.3.0 Build 28000 |
| 7.15 LTSR | 11.15.0.0 Build 24100 |
| 7.6 LTSR | 11.14.0.1 Build 21103 |

Informationen zu Legacy-Produkten und -Produktversionen finden Sie in der Legacyproduktmatrix.

Sie müssen Volladministrator für die Lizenzierung sein, um die folgenden Aufgaben ausführen zu können. Zum Anzeigen der Lizenzinformationen in Web Studio muss der Administrator mindestens Lesezugriff als delegierter Administrator für die Lizenzierung haben. Die integrierten Rollen Volladministrator und Lesezugriffadministrator haben diese Berechtigung.

### Download und Installation einer Citrix-Lizenz mit Web Studio

1. Melden Sie sich bei Web Studio an und wählen Sie im linken Bereich **Lizenzierung**.
2. Wählen Sie in der Aktionsleiste **Lizenzen zuteilen**.
3. Geben Sie den Lizenzzugangscode ein, den Sie nach Kauf bzw. Verlängerung von Lizenzen per E-Mail von Citrix erhalten haben.

4. Wählen Sie ein Produkt und dann **Lizenzen zuteilen**. Die für das Produkt verfügbaren Lizenzen werden zugeteilt und heruntergeladen. Wenn Sie alle Lizenzen für einen bestimmten Lizenzzugangscode zugeteilt und heruntergeladen haben, können Sie den Lizenzzugangscode nicht erneut verwenden. Zum Durchführen weiterer Transaktionen mit demselben Code melden Sie sich bei "Mein Konto"an.

### Hinzufügen von Lizenzen, die auf dem lokalen Computer oder im Netzwerk gespeichert sind

1. Melden Sie sich bei Web Studio an und wählen Sie im linken Bereich **Lizenzierung**.
2. Wählen Sie in der Aktionsleiste **Lizenzen hinzufügen**.
3. Navigieren Sie zu einer Lizenzdatei und fügen Sie sie dem Lizenzserver hinzu.

### Ändern des Lizenzservers

1. Melden Sie sich bei Web Studio an und wählen Sie im linken Bereich **Lizenzierung**.
2. Wählen Sie in der Aktionsleiste **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. Melden Sie sich bei Web Studio an und wählen Sie im linken Bereich **Lizenzierung**.
2. Wählen Sie in der Aktionsleiste **Produktedition bearbeiten**.
3. Aktualisieren Sie die entsprechenden Optionen.

Um auf die License Administration Console zuzugreifen, wählen Sie in der Aktionsleiste 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.

> **Hinweis:**
>
> Wenn Sie Lizenzen in Web Studio wechseln, dauert es bis zu 5 Minuten, bis die Änderung in Citrix Director angezeigt wird. Beispielsweise beim Wechsel zwischen Advanced und Premium wechseln.

### Hinzufügen eines Lizenzierungsadministrators

1. Melden Sie sich bei Web Studio an und wählen Sie im linken Bereich **Lizenzierung**.
2. Wählen Sie die Registerkarte **Lizenzierungsadministratoren**.
3. Wählen Sie in der Aktionsleiste **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. Melden Sie sich bei Web Studio an und wählen Sie im linken Bereich **Lizenzierung**.
2. Wählen Sie die Registerkarte **Lizenzierungsadministratoren** und dann den Administrator.
3. Wählen Sie in der Aktionsleiste **Lizenzierungsadministrator bearbeiten** bzw. **Lizenzierungsadministrator löschen**.

### Hinzufügen einer Lizenzierungsadministratorgruppe

1. Melden Sie sich bei Web Studio an und wählen Sie im linken Bereich **Lizenzierung**.
2. Wählen Sie die Registerkarte **Lizenzierungsadministratoren**.
3. Wählen Sie in der Aktionsleiste **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 Lizenzadministratorengruppe oder Löschen einer Lizenzierungsadministratorengruppe

1. Melden Sie sich bei Web Studio an und wählen Sie im linken Bereich **Lizenzierung**.
2. Wählen Sie die Registerkarte **Lizenzierungsadministratoren** und dann die Administratorgruppe.
3. Wählen Sie in der Aktionsleiste **Lizenzierungsadministratorengruppe bearbeiten** bzw. **Lizenzierungsadministratorengruppe löschen**.

### Anzeigen der Lizenzinformationen

Melden Sie sich bei Web Studio an und wählen Sie im linken Bereich **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.

### Anzeigen von Warnungen zum Lizenzablauf

Web Studio ruft Lizenzdatei-Ablaufdatum vom Citrix Lizenzserver ab. Administratoren erhalten in Web Studio auf der Registerkarte “Übersicht”eine Warnung, wenn der Ablauf von Lizenzdateien ansteht oder diese abgelaufen sind.

### Verwandte Links

- Siehe Citrix On-Premises-Abonnement für jährliche und befristete Volllizenzen (Retail).
- Siehe Übergang und Trade-Up (TTU) mit Hybridrechten.

## Multityplizenzierung

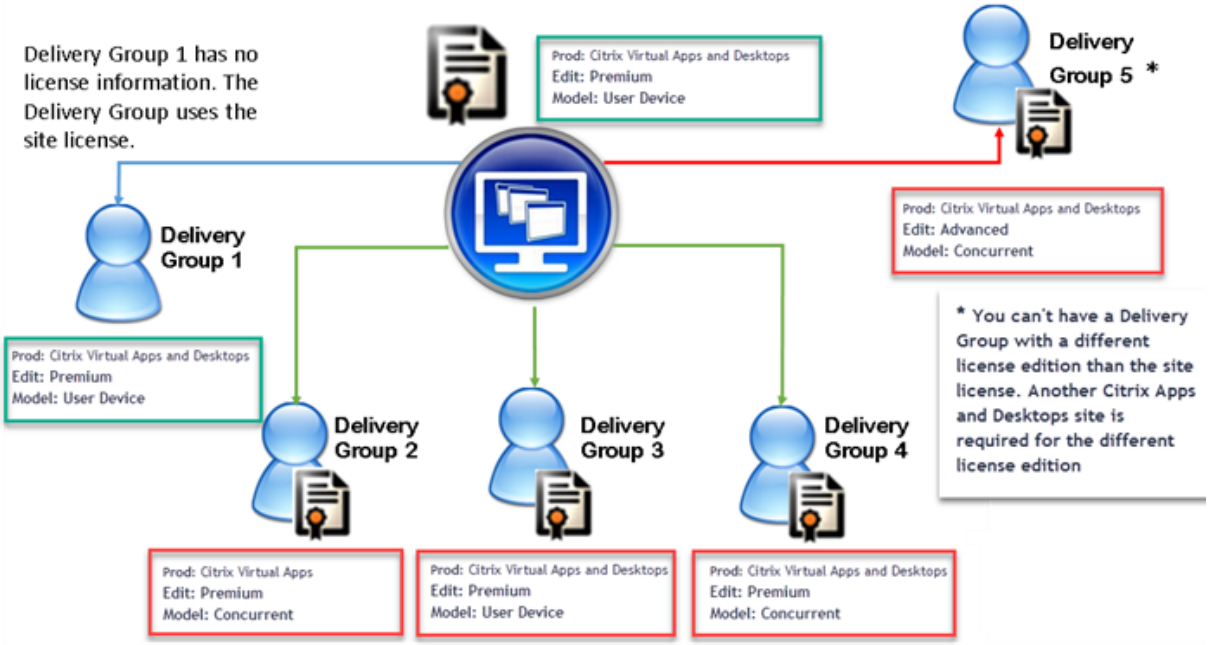
June 27, 2024

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
- citrix.com

Das Customer Success Services-Datum ist spezifisch für die Lizenzdatei, jedes Produkt und das Modell. Bereitstellungsgruppen mit unterschiedlichen Einstellungen können unterschiedliche Customer Success Services-Daten haben.

### 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 ist bei Citrix Virtual Apps Standard- und Citrix Virtual Desktop Standard-Lizenzen nicht verfügbar.

### 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. 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

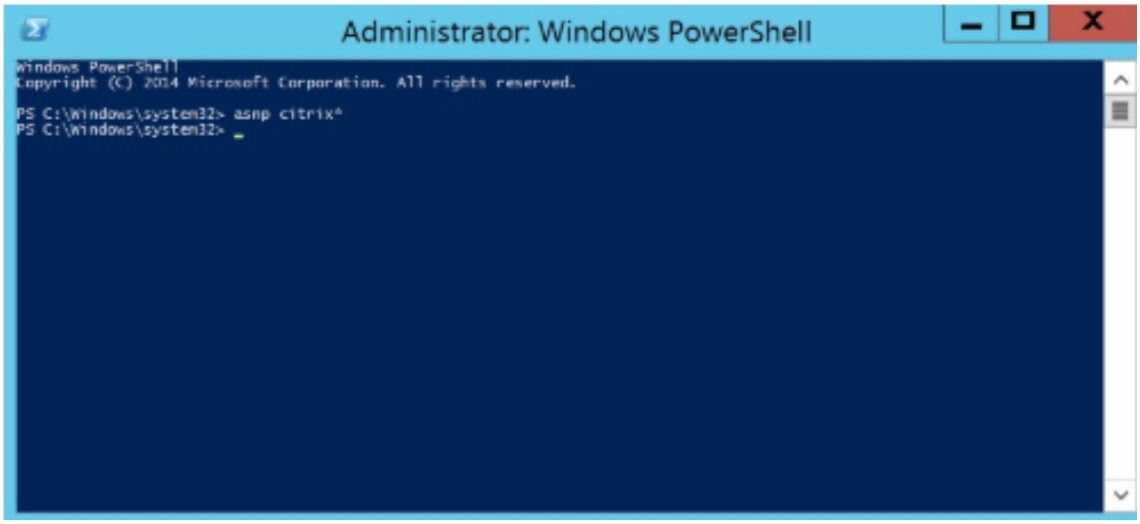
 

die Eigenschaften nicht mit New-BrokerDesktopGroup oder Set-BrokerDesktopGroup festgelegt wurden, werden Null-Werte zurückgegeben. Im Fall eines Null-Werts werden das Site-übergreifende Lizenzierungsmodell und der Site-übergreifende Produktcode verwendet. Weitere Informationen zu diesem Cmdlet finden Sie unter https://citrix.github.io/delivery-controller-sdk/Broker/Get-BrokerDesktopGroup/.

### Verschiedene Lizenzprodukte und -modelle pro Bereitstellungsgruppe konfigurieren

> **Hinweis:**
>
> Sie können nicht mehrere unterschiedliche Produkttypen, Editionen oder Lizenzmodelle für eine einzelne Bereitstellungsgruppe konfigurieren. Wenn Sie über unterschiedliche Produkttypen, Editionen oder Lizenzmodelle verfügen, konfigurieren Sie diese in separaten Bereitstellungsgruppen.

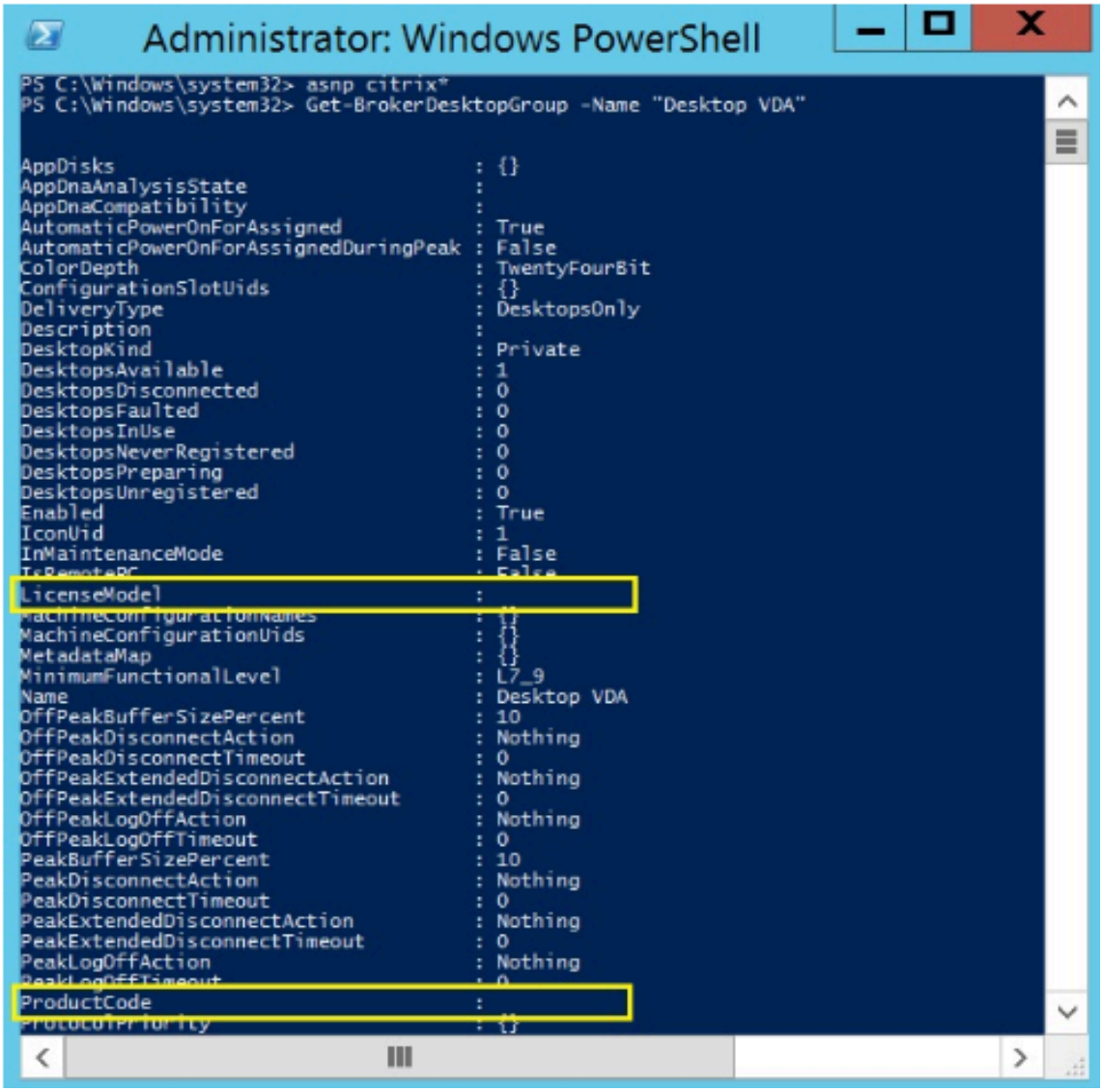
1. Öffnen Sie PowerShell mit Administratorrechten und fügen Sie das Citrix Snap-In hinzu.




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.

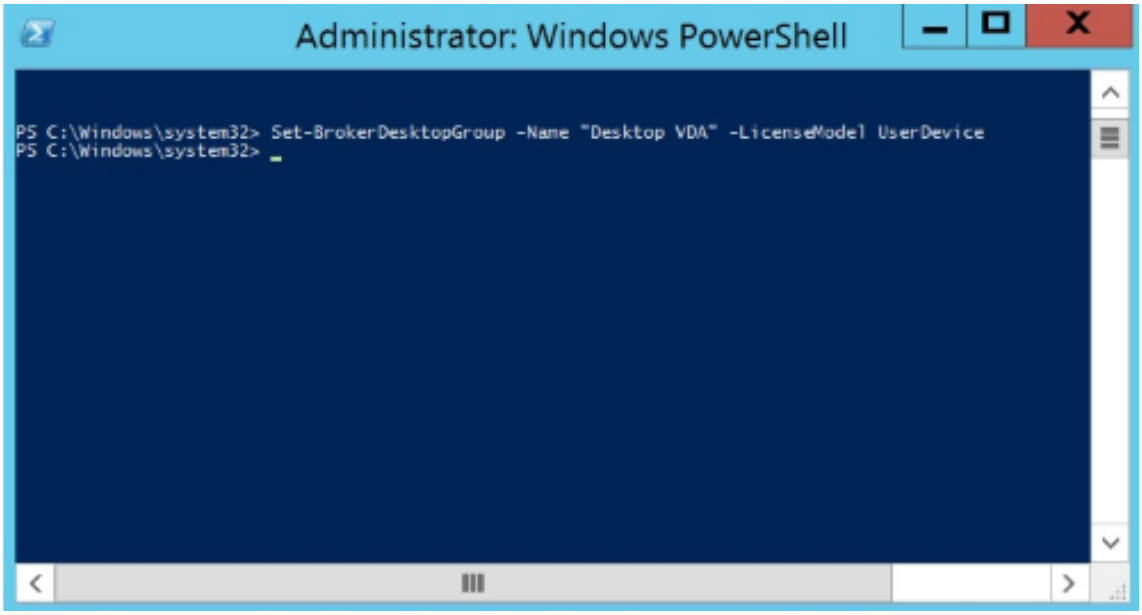
   > **Hinweis:**
   >
   > Wenn für eine Bereitstellungsgruppe keine Lizenzinformationen festgelegt sind, wird standardmäßig die **Sitelizenz auf Siteebene** eingestellt.

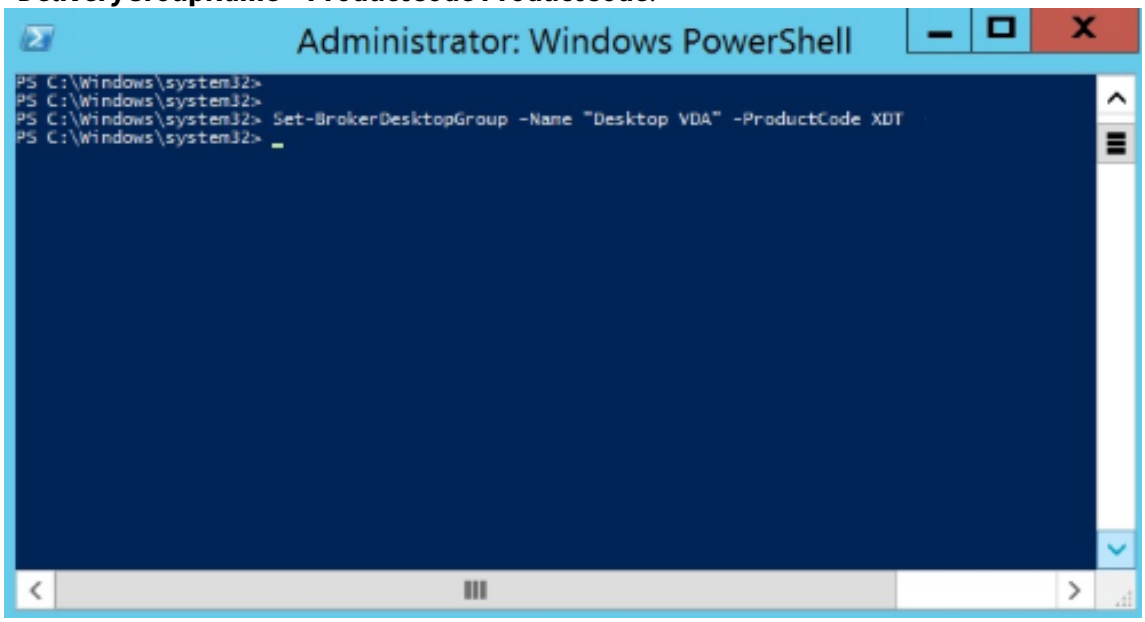



3. Ändern Sie das Lizenzmodell durch Ausführen des Befehls **Set-BrokerDesktopGroup –Name “DeliveryGroupName”–LicenseModel LicenseModel**.



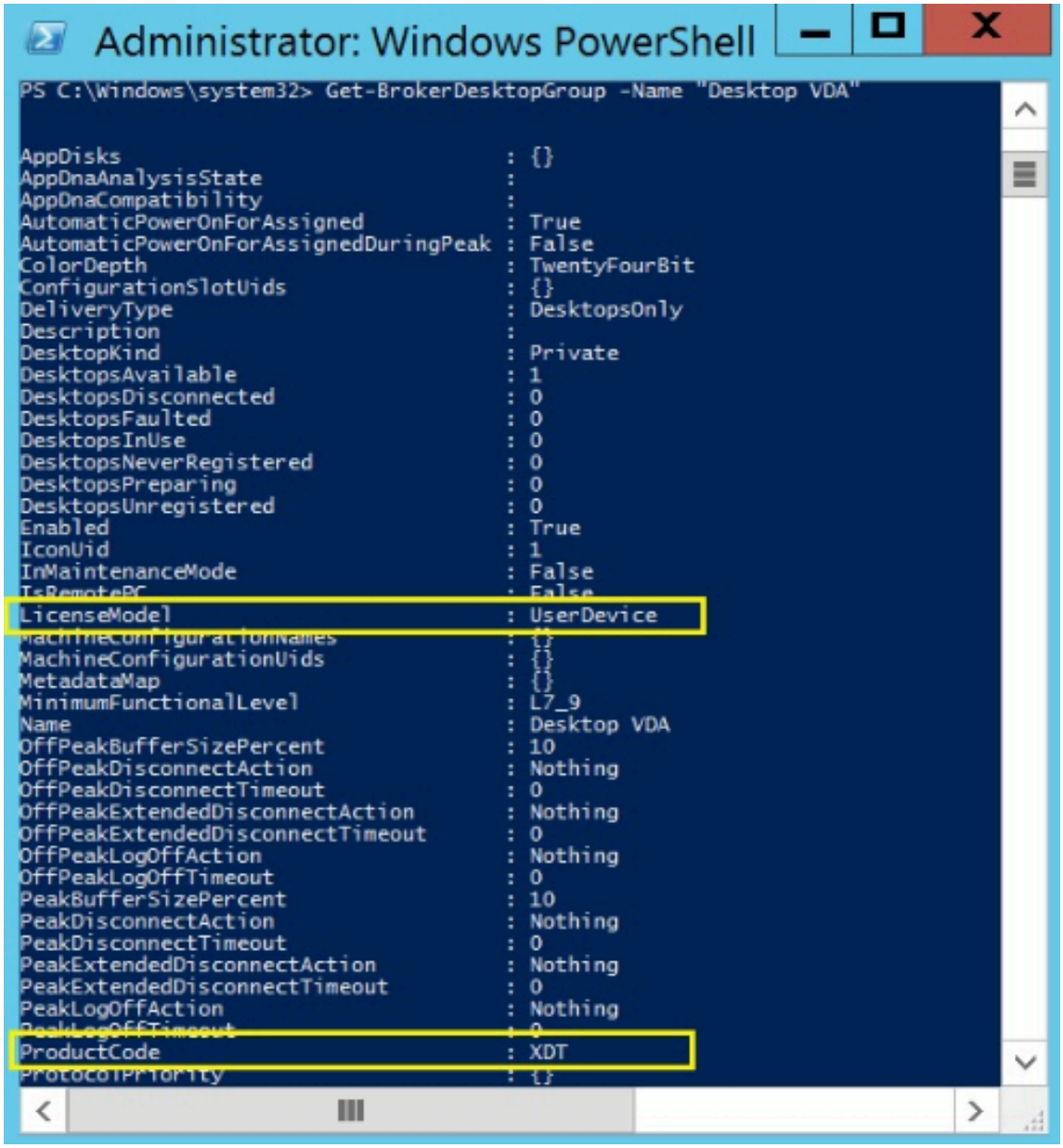

4. Ändern Sie das Lizenzprodukt durch Ausführen des Befehls **Set-BrokerDesktopGroup** –**Name “DeliveryGroupName”**–**ProductCode ProductCode**.




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.

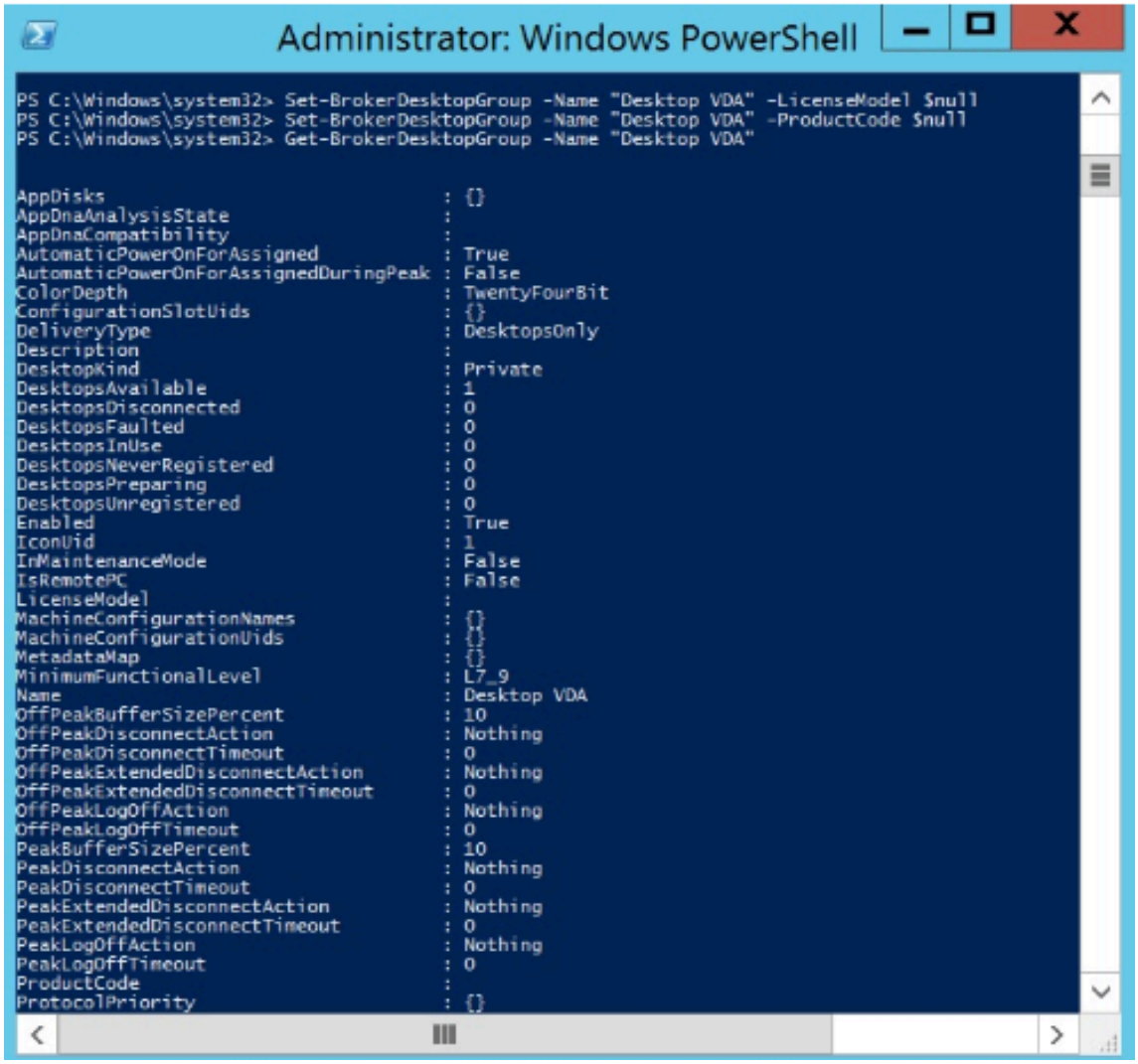
 




6. Entfernen Sie die Lizenzkonfiguration durch Ausführen der o. a. **Set-BrokerDesktopGroup**-Befehle und Festlegen des Werts auf **$null**.

> **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**

## Häufig gestellte Fragen zur Lizenzierung

June 27, 2024

> **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 Lizenzierung.

### Citrix Lizenzierung

#### Wie erhalte ich meine Lizenzdatei?

Wir senden den Lizenzzugangscode per E-Mail. Es gibt drei Möglichkeiten, Lizenzdateien mit dem Lizenzzugangscode zu generieren:

- Option **Lizenzen verwalten** auf der Seite “Mein Konto”auf `citrix.com`. Weitere Informationen finden Sie unter Verwalten von Lizenzen auf citrix.com.
- Web 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 Installieren von Lizenzen.

#### Wie teilt man eine Lizenz auf “Mein Konto”zu?

Siehe Zuteilen von Lizenzen.

### Wie fügt man dem Lizenzserver zugeteilte Lizenzen hinzu?

Siehe Ändern von Lizenzen.

#### 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 Desktops-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.

### Wo ist die Citrix License Administration Console?

Die License Administration Console wird nicht mehr unterstützt und ist in der Lizenzserverversion 11.16.6 nicht mehr enthalten. Wir empfehlen, Citrix Licensing Manager zu verwenden.

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 Citrix Licensing Manager.

#### 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.

#### 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?

Citrix Licensing Manager und Studio enthalten Details zur Echtzeit-Lizenzverwendung.

#### Notfallwiederherstellung und Wartung des Lizenzservers

Informationen zur Notfallwiederherstellung und Wartung des Lizenzservers finden Sie unter Notfallwiederherstellung und Wartung in der Dokumentation zur Citrix Lizenzierung.

### Lizenzierung für Citrix Virtual Apps and Desktops

#### 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 zuteilen. 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-/Gerätelizenz und zum Gleichzeitig-Modell unter CCU-Lizenz.

### 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. Weitere Informationen finden Sie unter Evaluierungslizenzen.

Citrix DaaS (ehemals 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. Weitere Informationen finden Sie unter CCU-Lizenz.

### 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.

**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.

**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 und XenServer Servicing-Optionen.

**Wie funktionieren die gepoolten Stunden für den Remote Browser Isolation (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.

**Kann ich Remote-PC-Zugriff mit CCU-Lizenzen verwenden?**

Ja.

Informationen über Remote-PC-Zugriff finden Sie unter Remote-PC-Zugriff.

**Was passiert, wenn die Softwarewartung für meine Citrix-Umgebung abläuft?**

Nach einer 30-tägigen Nachfrist erhalten Benutzer nach dem Start der Sitzung eine Warnmeldung, dass Ihre Citrix Virtual Apps and Desktops nicht unterstützt werden.
Warnung von Citrix Virtual Apps and Desktops:

```
Your corporate Citrix environment is currently unsupported. Please
contact your IT department to resolve any support related issues.
```

## Benutzer- oder Gerätelizenzen

### Wie teilt 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. Weitere Informationen finden Sie unter Benutzer-/Gerätelizenz.

### 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 | – | 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 | – | – | – |

**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 zugeteilt 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 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.

**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.

**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. Weitere Informationen finden Sie unter Anzeige oder Freigabe von Lizenzen für Benutzer oder Geräte.

**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. Erwerben Sie eine neue Lizenz und stellen Sie sie bereit, 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.

**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.

### CCU-Lizenzen

**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 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.

**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.

**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.

## Überziehungslizenzen

**Wie erhalte ich Überziehungslizenzen?**

Produkte (mit Ausnahme von Citrix Cloud), die Benutzer-/Gerätelizenzen bzw. Benutzerlizenzen oder Gerätelizenzen unterstützen, umfassen eine Lizenzüberziehungsfunktion, mit der Ihnen eine begren-

zte Anzahl zusätzlicher Lizenzen zur Verfügung steht, um die Verweigerung von Zugriff zu verhindern. Die Überziehungsfunktion wird als Hilfe angeboten und ist nicht als Lizenzberechtigung zu verstehen. CCU- und Serverlizenzen enthalten keine Überziehungen. Die verwendeten Überziehungslizenzen müssen innerhalb von 30 Tagen nach der ersten Nutzung erworben werden. Die Nutzung ist jedoch nicht auf 30 Tage beschränkt. Citrix behält sich das Recht vor, die Überziehungsfunktion in neuen Produktreleases zu entfernen. Weitere Informationen finden Sie unter Lizenzüberziehung.

#### 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?

Erwerben Sie Überziehungslizenzen innerhalb von 30 Tagen nach der ersten Verwendung.

### Andere produktspezifische Lizenzierungsinformationen

- Citrix ADC
- Citrix Cloud
- Citrix Endpoint Management
- Citrix Gateway
- XenServer
- Citrix Lizenzierung

# Lastausgleich bei Maschinen

June 27, 2024

> **Hinweis:**
>
> Diese Funktion gilt für alle Kataloge –also für Kataloge für Einzel- oder Multisitzungs-OS. Der vertikale Lastausgleich gilt nur für Maschinen mit Multisitzungs-OS.

Der Lastausgleich kann auf Siteebene und auf Bereitstellungsgruppenebene konfiguriert werden. Sie haben zwei Möglichkeiten: vertikal und horizontal. Standardmäßig ist der horizontale Lastausgleich aktiviert.

## Lastausgleichseinstellungen auf Siteebene

- **Vertikaler Lastausgleich:** Weist eine eingehende Benutzersitzung der Maschine zu, die am stärksten ausgelastet ist, jedoch die Maximallast noch nicht erreicht hat. Dadurch werden vorhandene Maschinen vollständig genutzt, bevor zu neuen Maschinen gewechselt wird. Das Trennen der Verbindung von vorhandenen Maschinen durch Benutzer gibt Kapazität auf diesen Maschinen frei. Eingehende Lasten werden dann diesen Maschinen zugewiesen. Der vertikale Lastausgleich beeinträchtigt die Benutzererfahrung, senkt jedoch die Kosten (Sitzungen maximieren die Kapazität der eingeschalteten Maschinen).

  Beispiel: Sie haben zwei Maschinen für jeweils zehn Sitzungen konfiguriert. Die erste Maschine verarbeitet die ersten zehn gleichzeitigen Sitzungen. Die zweite Maschine verarbeitet die elfte Sitzung.

  > **Tipp:**
  >
  > Um die maximale Anzahl von Sitzungen anzugeben, die von einer Maschine gehostet werden können, verwenden Sie die Richtlinieneinstellung Sitzungshöchstanzahl.

  Alternativ können Sie den vertikalen Lastausgleich mit PowerShell für die gesamte Site aktivieren oder deaktivieren. Verwenden Sie die Einstellung `UseVerticalScalingForRdsLaunches` im Cmdlet `Set-BrokerSite`. Verwenden Sie `Get-BrokerSite`, um den Wert der Einstellung `UseVerticalScalingForRdsLaunches` anzuzeigen. Weitere Informationen finden Sie in der Cmdlet-Hilfe.

- **Horizontaler Lastausgleich:** Weist eine eingehende Benutzersitzung der am wenigsten ausgelasteten, eingeschalteten Maschine zu. Der horizontale Lastausgleich verbessert die Benutzererfahrung, erhöht jedoch die Kosten, da mehr Maschinen eingeschaltet bleiben. Standardmäßig ist der horizontale Lastausgleich aktiviert.

Beispiel: Sie haben zwei Maschinen für jeweils zehn Sitzungen konfiguriert. Die erste Maschine verarbeitet die ersten fünf gleichzeitigen Sitzungen. Die zweite Maschine verarbeitet ebenfalls fünf Sitzungen.

Um dieses Feature zu konfigurieren, wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Einstellungen**. Wählen Sie eine Option unter **Lastausgleich für Multisitzungskataloge**.

### Lastausgleicheinstellungen auf Bereitstellungsgruppenebene

Wenn Sie den Lastausgleich auf Bereitstellungsgruppenebene konfigurieren, können Sie die von der Siteebene übernommenen Lastausgleicheinstellungen außer Kraft setzen. Sie können die maximale Auslastung für jede Maschine erreichen, wenn Sie den vertikalen Lastausgleich auf Bereitstellungsgruppenebene auswählen. Dies trägt zur Senkung der Kosten in öffentlichen Clouds bei. Diese Konfiguration kann bei Erstellung einer neuen Bereitstellungsgruppe oder der Bearbeitung einer vorhandenen vorgenommen werden.

**Horizontaler Lastausgleich:** Die Sitzungen werden auf die eingeschalteten Maschinen verteilt. Wenn Sie beispielsweise zwei Maschinen für jeweils zehn Sitzungen konfiguriert haben, verarbeitet die erste Maschine fünf gleichzeitige Sitzungen und die zweite Maschine verarbeitet ebenfalls fünf.

**Vertikaler Lastausgleich:** Die Kapazität der eingeschalteten Maschinen werden maximiert, was Maschinenkosten spart. Wenn Sie beispielsweise zwei Maschinen für jeweils zehn Sitzungen konfiguriert haben, verarbeitet die erste Maschine die ersten zehn gleichzeitigen Sitzungen. Die zweite Maschine verarbeitet die elfte Sitzung.

## Lokaler Hostcache

June 27, 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 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.

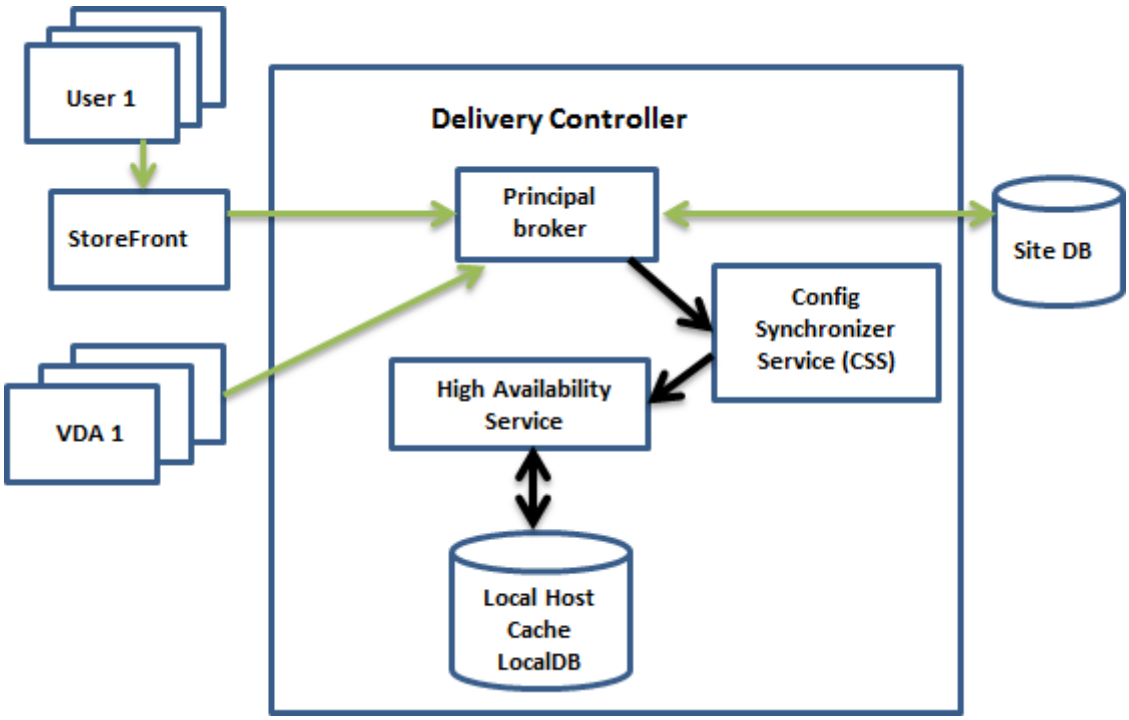
Er enthält außerdem Informationen zu aktiven Verbindungen, die eingerichtet wurden, während die Hauptdatenbank nicht verfügbar war:

- 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 *principal broker* (auch "Citrix Broker Service") auf einem Controller akzeptiert Verbindungsanfragen von StoreFront. Der Broker kommuniziert mit der Sitedatenbank, um Benutzer mit VDAs zu verbinden, die beim Controller registriert sind
- Citrix Config Sync-Dienst (CSS) überprüft ungefähr alle 5 Minuten bei dem Broker, ob Änderungen vorgenommen wurden. Änderungen können von einem Administrator (z. B. Ändern der Eigenschaft einer Bereitstellungsgruppe) oder durch Systemaktionen (z. B. Maschinenzuweisungen) hervorgerufen werden.
- Wenn seit der letzten Überprüfung eine Konfigurationsänderung stattgefunden hat, synchronisiert (kopiert) der CSS die Informationen auf einen sekundären Broker auf dem Controller. (Der sekundäre Broker wird auch als "Dienst für hohe Verfügbarkeit"bezeichnet.)

  Dabei werden nicht nur die seit der letzten Prüfung geänderten Elemente, sondern alle Konfigurationsdaten kopiert. Der CSS importiert die Konfigurationsdaten in eine Microsoft SQL Server Express-LocalDB-Datenbank auf dem Controller. Diese Datenbank wird als lokale Hostcachedatenbank bezeichnet. Der CSS stellt sicher, dass die Informationen in der lokalen Hostcachedatenbank des sekundären Brokers mit den Informationen in der Sitedatenbank übereinstimmen. Die lokale Hostcachedatenbank wird bei jeder Synchronisierung neu erstellt.

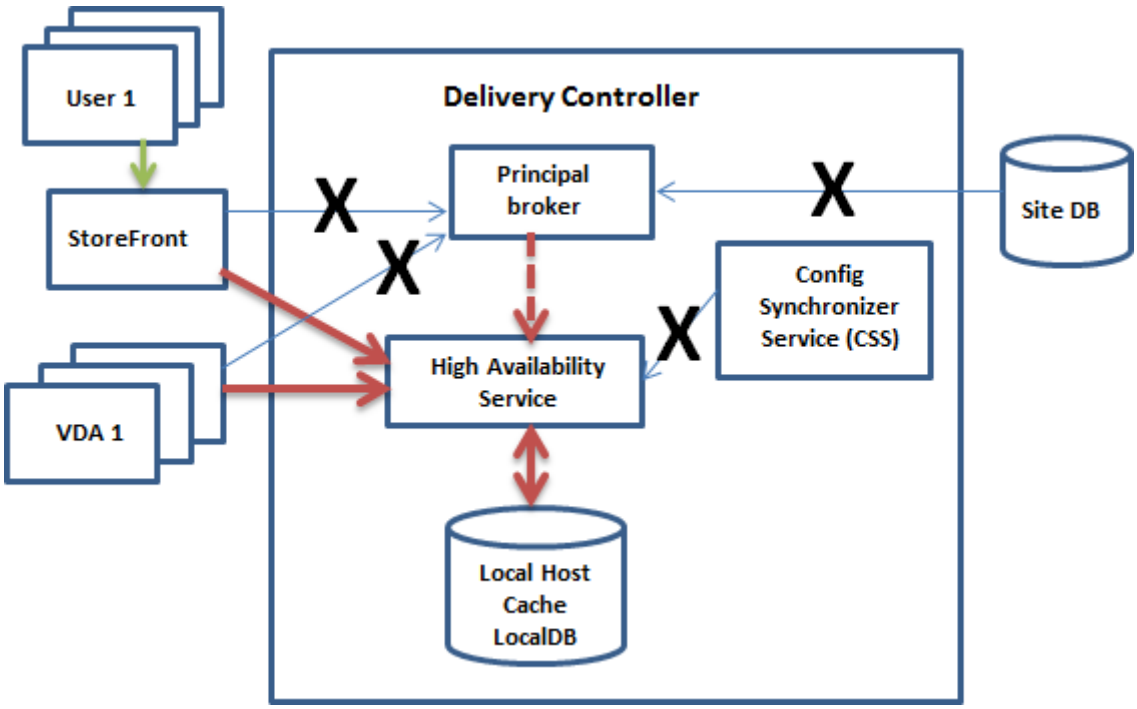
  SQL Server Express LocalDB zur Verwendung mit dem lokalen Hostcache wird automatisch installiert, wenn Sie einen Controller installieren. (Sie können diese Installation unterbinden,

wenn Sie einen Controller über die Befehlszeile installieren.) Die lokale Hostcachedatenbank kann nicht für mehrere Controller freigegeben werden. Sie müssen die lokale Hostcachedatenbank nicht sichern. Sie wird jedes Mal neu erstellt, wenn eine Konfigurationsänderung erkannt wird.

- 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).




**Bei einem Ausfall**

Wenn ein Ausfall beginnt:

- Der sekundäre Broker beginnt auf Verbindungsanforderungen zu prüfen und diese zu verarbeiten.
- Bei Ausfallbeginn hat der sekundäre Broker keine aktuellen VDA-Registrierungsdaten, doch wenn ein VDA mit ihm kommuniziert, wird eine Registrierung ausgelöst. Während dieses Vorgangs erhält der sekundäre Broker auch aktuelle Sitzungsinformationen zu dem betreffenden VDA.
- Während der sekundäre Broker Verbindungen verarbeitet, überwacht der Brokerprinzipal weiterhin die Verbindung. Wenn die Verbindung wiederhergestellt ist, weist der Brokerprinzipal den sekundären Broker an, die Prüfung auf Verbindungsinformationen einzustellen, und nimmt das Verbindungsbrokering wieder auf. Wenn ein VDA das nächste Mal mit dem Brokerprinzipal kom-

muniziert, wird eine Neuregistrierung ausgelöst. Der sekundäre Broker entfernt alle verbleibenden VDA-Registrierungen aus dem vorherigen Ausfall. Der CSS nimmt die Synchronisierung von Informationen wieder auf, wenn er Konfigurationsänderungen in der Bereitstellung erkennt.

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.

Es gibt keine zeitliche Begrenzung für den Betrieb in Ausfallmodus.

Der Wechsel zwischen dem normalen und dem Ausfallmodus wirkt sich nicht auf bestehende Sitzungen aus. Er wirkt sich nur auf den Start neuer Sitzungen aus.

Sie können einen Ausfall auch absichtlich auslösen. Informationen zu Zweck und Vorgehensweise finden Sie unter Erzwingen eines Ausfalls.

#### Sites mit mehreren Controllern

Unter anderem hat der CSS die Aufgabe, den sekundären Broker regelmäßig mit Informationen zu allen Controllern in der Zone zu versorgen. (Enthält Ihre Bereitstellung nicht mehrere Zonen, wirkt sich diese Aktion auf alle Controller in der Site aus.) Anhand dieser Informationen ist jeder sekundäre Broker über sekundäre Peerbroker, die auf anderen Controllern in der Zone ausgeführt werden, informiert.

Die sekundären Broker kommunizieren miteinander über einen anderen Kanal. Anhand einer alphabetischen Liste der FQDNs der Maschinen, auf denen sie ausgeführt werden, ermitteln (wählen) diese Broker, welcher sekundäre Broker bei einem Ausfall das Brokering in der Zone übernimmt. Bei einem Ausfall registrieren sich alle VDAs bei dem gewählten sekundären Broker. Die nicht gewählten sekundären Broker in der Zone weisen eingehende Verbindungs- und VDA-Registrierungsanfragen aktiv ab.

Wenn ein gewählter sekundärer Broker während eines Ausfalls selbst ausfällt, wird stattdessen ein anderer sekundärer Broker gewählt und die VDAs registrieren sich bei diesem.

Wird bei einem Ausfall ein Controller neu gestartet, passiert Folgendes:

- Handelt es sich bei dem Controller nicht um den gewählten Broker, hat der Neustart keine Auswirkungen.
- Handelt es sich um den gewählten Broker, wird ein anderer Controller gewählt und somit werden die VDAs registriert. Wenn der Neustart des Controllers beendet ist, übernimmt er automatisch das Brokering und somit werden die VDAs erneut registriert. In diesem Szenario kann es während der Registrierungen 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 Broker ausgewählt wurde.

Die Ereignisprotokolle enthalten Informationen zu diesen Wahlen.

### Während eines Ausfalls nicht verfügbare Elemente und weitere Unterschiede

Es gibt keine zeitliche Begrenzung für den Betrieb in Ausfallmodus. Citrix empfiehlt jedoch, die Verbindung so schnell wie möglich wiederherzustellen.

Bei einem Ausfall:

- Sie können Studio nicht verwenden.
- Sie haben eingeschränkten Zugriff auf das PowerShell-SDK.
  - Sie müssen zuerst Folgendes tun:
    * Fügen Sie einen Registrierungsschlüssel `EnableCssTestMode` mit dem Wert `1` hinzu: `New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTestMode -PropertyType DWORD -Value 1`
    * Verwenden Sie Port 89: `Get-BrokerMachine -AdminAddress localhost:89 | Select MachineName, ControllerDNSName, DesktopGroupName, RegistrationState`
  - Nachdem Sie diese Befehle ausgeführt haben, können Sie auf Folgendes zugreifen:
    * Alle `Get-Broker*`-Cmdlets.
- Hypervisor-Anmeldeinformationen können nicht vom Hostdienst abgerufen werden. Bei allen Maschinen ist der Energiezustand unbekannt, es können keine Energievorgänge ausgelöst werden. Auf dem Host eingeschaltete VMs können jedoch für Verbindungsanfragen verwendet werden.
- Zugewiesene Maschinen können nur verwendet werden, wenn die Zuweisung während des normalen Betriebs erfolgte. Neue Zuweisungen sind bei einem Ausfall nicht möglich.
- Die automatische Registrierung und Konfiguration von Remote-PC-Zugriff-Maschinen ist nicht möglich. Im normalen Betrieb registrierte und konfigurierte Maschinen können dagegen verwendet werden.
- Benutzer servergehosteter Anwendungen und Desktops können möglicherweise mehr Sitzungen verwenden als das für sie konfigurierte Sitzungslimit zulässt, wenn die Ressourcen in verschiedenen Zonen sind.

- Benutzer können Anwendungen und Desktops nur von registrierten VDAs in der Zone starten, die den aktuell aktiven/gewählten sekundären Broker enthält. Startvorgänge über Zonen hinweg (von einem sekundären Broker 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.
- Die Zonenpräferenz kann nicht konfiguriert werden. Eventuell konfigurierte Präferenzen werden für den Sitzungsstart nicht berücksichtigt.
- 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.

### Unterstützung für Anwendungen und Desktops

Der lokale Hostcache unterstützt servergehostete Anwendungen und Desktops und statische (zugewiesene) Desktops.

Der lokale Hostcache unterstützt Desktop-VDAs in gepoolten Bereitstellungsgruppen wie folgt:

- 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:

  Siteweit:

  ```
  Set-BrokerSite -ReuseMachinesWithoutShutdownInOutageAllowed $true
  ```

  Führen Sie den folgenden PowerShell-Befehl für jede betroffene Bereitstellungsgruppe aus:

  ```
  Set-BrokerDesktopGroup -Name "name"-ReuseMachinesWithoutShutdownInOutage
   $true
  ```

Führen Sie den folgenden PowerShell-Befehl aus, um die Bereitstellungsgruppeneinstellung standardmäßig zu aktivieren:

```
Set-BrokerSite -DefaultReuseMachinesWithoutShutdownInOutage $true
```

Diese Einstellung gilt für alle neuen Bereitstellungsgruppen, die nach dem Aktivieren dieser Einstellung erstellt werden.

Führen Sie den folgenden PowerShell-Befehl aus, um diese Einstellung für die vorhandenen Bereitstellungsgruppen zu aktivieren:

```
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 sekundäre Broker 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 sekundäre Broker 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 1 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 weitere E/A-Vorgänge: ca. 3 MB Schreibvorgänge pro Sekunde bei mehreren Hunderttausend Lesevorgängen.

#### Leistung

Bei einem Ausfall verarbeitet ein sekundärer Broker alle Verbindungen. In Sites (oder Zonen) mit Lastausgleich zwischen mehreren Controllern muss der sekundäre Broker daher möglicherweise viel mehr Anfragen verarbeiten als im Normalbetrieb. Die CPU-Anforderungen sind somit höher. Jeder sekundäre Broker in der Site (Zone) muss in der Lage sein, die zusätzliche, von der lokalen Hostcache-datenbank und allen betroffenen VDAs verursachte Last zu verarbeiten, da der sekundäre Broker bei einem Ausfall wechseln kann.

VDI-Grenzwerte:

- In einer einzonigen VDI-Bereitstellung können während eines Ausfalls bis zu 10.000 VDAS effektiv bewältigt werden.
- In einer VDI-Bereitstellung mit mehreren Zonen können bis zu 10.000 VDAs pro Zone und insgesamt bis zu 40.000 VDAs pro Site gehandhabt werden. Beispielsweise ist ein effektives Handling der folgenden Sites während eines Ausfalls möglich:
  - Eine Site mit vier Zonen mit je 10.000 VDAs
  - Eine Site mit sieben Zonen, von denen eine 10.000 VDAs enthält und die restlichen sechs je 5.000 VDAs

Bei einem Ausfall kann die Lastverwaltung der Site beeinträchtigt werden. Lastauswertungsprogramme (und insbesondere Sitzungszahlregeln) werden möglicherweise überschritten.

Während der Zeit, die für die Registrierung aller VDAs bei einem sekundären Broker benötigt wird, hat der Dienst 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"sekundären Broker) ist unvermeidlich. Auf Sitzungen, die bei Ausfallbeginn verbunden waren, hat das Übergangsintervall keine Auswirkungen, doch bei neuen Sitzungen und erneuten Sitzungsverbindungen ist eine Beeinträchtigung möglich.

Das Intervall tritt immer dann auf, wenn die VDAs sich registrieren müssen:

- Ausfallbeginn: bei der Migration von einem Hauptbroker zu einem sekundären Broker
- Fehler am sekundären Broker während eines Ausfalls: bei der Migration von dem fehlerhaften sekundären Broker zu dem neu gewählten sekundären Broker
- Wiederherstellung nach Ausfall: bei Wiederaufnahme des Normalbetriebs und der erneuten Übernahme der Steuerung durch den Hauptbroker

Sie können das Intervall verringern, indem Sie den Registrierungswert `HeartbeatPeriodMs` für Citrix Broker Protocol verringern (Standardwert = 600000 ms, d. h. 10 Minuten). 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 sekundären Brokern erhöht sich mit steigender Anzahl der Objekte (VDAs, Anwendungen, Gruppen usw.). Die Synchronisierung von 5000 VDAs kann beispielsweise 10 Minuten oder länger dauern.

#### 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. Nur der sekundäre Broker 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 die Option `/exclude "Local Host Cache Storage (LocalDB)"`. Der lokale Hostcache funktioniert allerdings nicht ohne die Datenbank und Sie können keine andere Datenbank für den sekundären Broker verwenden.

Die Installation der LocalDB-Datenbank ist irrelevant für die Entscheidung, ob Sie SQL Server Express zur Verwendung als Sitedatenbank installieren.

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` gesetzt 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:

- Vergewissern Sie sich, dass Synchronisierungsimporte erfolgreich abgeschlossen werden. Überprüfen Sie die Ereignisprotokolle.
- Vergewissern Sie sich, dass die LocalDB von SQL Server Express auf jedem Delivery Controller erstellt wurde. Dadurch wird bestätigt, dass der sekundäre Broker bei Bedarf übernehmen kann.
  - Gehen Sie auf dem Delivery Controller-Server zu `C:\Windows\ServiceProfiles\NetworkService`.
  - Überprüfen Sie, ob `HaDatabaseName.mdf` und `HaDatabaseName_log.ldf` erstellt wurden.
- 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 ungefähr 15 Minuten dauern.

### Ereignisprotokolle

Ereignisprotokolle enthalten Informationen zu Synchronisierungen und Ausfällen. In Ereignisanzeige-Protokollen wird der Ausfallmodus als *HA mode*bezeichnet.*

**Config Synchronizer Service:**

Im Normalbetrieb können die folgenden Ereignisse auftreten, wenn der CSS die Konfigurationsdaten mit dem lokalen Hostcachebrokers in die lokale Hostcachedatenbank importiert.

- 503: Der Citrix Config Sync-Dienst erhielt eine aktualisierte Konfiguration. Das Ereignis zeigt den Beginn des Synchronisationsprozesses an.
- 504: Der Citrix Config Sync-Dienst hat eine aktualisierte Konfiguration importiert. Der Konfigurationsimport wurde erfolgreich abgeschlossen.
- 505: Fehler bei einem Import in den Citrix Config Sync-Dienst. Der Konfigurationsimport wurde nicht erfolgreich abgeschlossen. Wenn eine frühere, erfolgreich importierte Konfiguration verfügbar ist, wird diese bei einem Ausfall verwendet. Sie ist jedoch im Vergleich zur aktuellen Konfiguration veraltet. Wenn keine vorherige Konfiguration vorliegt, kann sich der Dienst bei

einem Ausfall nicht an der Sitzungsvermittlung beteiligen. Lesen Sie in diesem Fall den Abschnitt Fehlerbehebung und wenden Sie sich an den Citrix Support.
- 507: Der Citrix Config Sync Service hat einen Importvorgang abgebrochen, weil ein Systemausfall vorliegt und der lokale Hostcachebroker für die Vermittlung verwendet wird. Der Dienst hat eine neue Konfiguration erhalten, der Import wurde jedoch abgebrochen, da ein Ausfall aufgetreten ist. Dieses Verhalten wird erwartet.
- 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:**

Dieser Dienst wird auch als lokaler Hostcachebroker bezeichnet.

- 3502: Ein Ausfall ist aufgetreten und der lokale Hostcachebroker führt Brokervorgänge durch.
- 3503: Ein Ausfall wurde behandelt und der Normalbetrieb wieder aufgenommen.
- 3504: Gibt an, welcher lokale Hostcachebroker gewählt wurde und welche anderen lokalen Hostcachebroker bei der Wahl beteiligt waren.
- 3507: Stellt alle 2 Minuten eine Statusaktualisierung des lokalen Hostcache bereit, die angibt, dass der Modus "Lokaler Hostcache"auf dem ausgewählten Broker aktiv ist. Enthält eine Zusammenfassung des Ausfalls, einschließlich Ausfalldauer, VDA-Registrierung und Sitzungsinformationen.
- 3508: Gibt an, dass der lokale Hostcache auf dem ausgewählten Broker nicht mehr aktiv ist und dass der normale Betrieb wiederhergestellt wurde. Enthält eine Zusammenfassung des Ausfalls, einschließlich Ausfalldauer, Anzahl der Maschinen, die während des lokalen Hostcache-Ereignisses registriert wurden, und der Anzahl erfolgreicher Starts während des lokalen Hostcache-Ereignisses.
- 3509: Gibt an, dass der lokale Hostcache auf dem bzw. den nicht ausgewählten Broker(n) aktiv ist. Liefert alle 2 Minuten Angaben zur Ausfalldauer und gibt den ausgewählten Broker an.
- 3510: Gibt an, dass der lokale Hostcache auf dem bzw. den nicht ausgewählten Broker(n) nicht mehr aktiv ist. Enthält die Ausfalldauer und gibt den ausgewählten Broker an.

## Erzwingen eines Ausfalls

In folgenden Situationen kann das Erzwingen eines Ausfalls 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 (und somit häufige VDA-Registrierungen) vermieden.

- Zum Testen eines Notfallwiederherstellungsplans
- Zur Prüfung des ordnungsgemäßen Betriebs des lokalen Hostcache
- Beim Ersetzen oder Warten des Sitedatenbankservers

Zum Erzwingen eines Ausfalls bearbeiten Sie die Registrierung aller Server, die einen Delivery Controller enthalten. Erstellen Sie für `HKLM\Software\Citrix\DesktopServer\LHC` `OutageModeForced` und legen Sie `REG_DWORD` auf 1 fest. Durch diese Einstellung wird der lokale Hostcachebroker angewiesen, unabhängig vom Zustand der Datenbank in den Ausfallmodus zu wechseln. Wenn Sie den Wert auf `0` festlegen, wird der Ausfallmodus auf dem lokalen Hostcachebroker beendet.

Überprüfen Sie die Ereignisse in der Protokolldatei `Current_HighAvailabilityService` in `C:\ProgramData\Citrix\WorkspaceCloud\Logs\Plugins\HighAvailabilityService` .

### Problembehandlung

Mehrere Problembehandlungstools sind verfügbar, wenn ein Synchronisierungsimport in die lokale Hostcachedatenbank fehlschlägt und ein 505-Ereignis verzeichnet wird.

**Ablaufverfolgung mit CDF:** Enthält Optionen für die Module `ConfigSyncServer` und `BrokerLHC`. In Kombination mit anderen Brokermodulen kann mit diesen Optionen das Problem in der Regel identifiziert werden.

**Bericht:** Wenn ein Synchronisierungsimport fehlschlägt, können Sie einen Bericht erstellen. Der Bericht endet mit dem Objekt, das den Fehler verursacht hat. Das Berichtsfeature wirkt sich auf die Synchronisierungsgeschwindigkeit aus. Deshalb empfiehlt Citrix, es zu deaktivieren, wenn es nicht verwendet wird.

Zum Aktivieren von CSS und Erstellen eines Ablaufverfolgungsberichts geben Sie folgenden Befehl ein:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name
EnableCssTraceMode -PropertyType DWORD -Value 1
```

Der HTML-Bericht wird unter `C:\Windows\ServiceProfiles\NetworkService\AppData` `\Local\Temp\CitrixBrokerConfigSyncReport.html` veröffentlicht.

Wenn der Bericht generiert wurde, deaktivieren Sie das Berichtsfeature durch Eingabe des folgenden Befehls:

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name
EnableCssTraceMode -Value 0
```

**Exportieren der Brokerkonfiguration:** stellt die exakte Konfiguration zum Debuggen zur Verfügung.

```
Export-BrokerConfiguration | Out-File <file-pathname>
```

Beispiel: `Export-BrokerConfiguration | Out-File C:\\BrokerConfig.xml`.

#### PowerShell-Befehle für den lokalen Hostcache

Sie können den lokalen Hostcache auf Ihren Delivery Controllern mithilfe von PowerShell-Befehlen verwalten.

Das PowerShell-Modul befindet sich auf den Delivery Controllern im folgenden Verzeichnis:

```
C:\Program Files\Citrix\Broker\Service\ControlScripts
```

> **Wichtig:**
>
> Führen Sie dieses Modul nur auf den Delivery Controllern aus.

**PowerShell-Modul importieren** Um das Modul zu importieren, führen Sie folgenden Befehl auf dem Delivery Controller aus.

```
cd C:\Program Files\Citrix\Broker\Service\ControlScripts Import-
Module .\HighAvailabilityServiceControl.psm1
```

**PowerShell-Befehle zur Verwaltung des lokalen Hostcache** Mit den folgenden Befehlen können Sie den Modus "Lokaler Hostcache"auf den Delivery Controllern aktivieren und verwalten.

| Cmdlets | Funktion |
| --- | --- |
| `Enable-LhcForcedOutageMode` | Versetzen Sie den Broker in den Modus "Lokaler Hostcache". Datenbankdateien für den lokalen Hostcache müssen erfolgreich vom ConfigSync-Dienst erstellt worden sein, damit `Enable-LhcForcedOutageMode` ordnungsgemäß funktioniert. Dieses Cmdlet erzwingt den lokalen Hostcache nur auf dem Delivery Controller, auf dem es ausgeführt wurde. Um den lokalen Hostcache zu aktivieren, muss dieser Befehl auf allen Delivery Controllern innerhalb der Zone ausgeführt werden. |

| Cmdlets | Funktion |
| --- | --- |
| `Disable-LhcForcedOutageMode` | Beendet den Modus “Lokaler Hostcache”auf dem Broker. Dieses Cmdlet deaktiviert den Modus “Lokaler Hostcache”nur auf dem Delivery Controller, auf dem es ausgeführt wurde. `Disable-LhcForcedOutageMode` muss auf allen Delivery Controllern innerhalb der Zone ausgeführt werden. |
| `Set-LhcConfigSyncIntervalOverride` | Legt das Intervall fest, in dem Citrix Config Synchronizer Service (CSS) nach Konfigurationsänderungen innerhalb der Site sucht. Das Zeitintervall kann zwischen 60 Sekunden (eine Minute) und 3600 Sekunden (eine Stunde) liegen. Diese Einstellung gilt nur für den Delivery Controller, auf dem er ausgeführt wurde. Damit alle Delivery Controller übereinstimmen, sollten Sie das Cmdlet auf jedem Delivery Controller ausführen. Beispiel: `Set-LhcConfigSyncIntervalOverride -Seconds 1200` |
| `Clear-LhcConfigSyncIntervalOverride` | Legt das Intervall fest, in dem Citrix Config Synchronizer Service (CSS) nach Konfigurationsänderungen innerhalb der Site sucht. Standardwert 300 Sekunden (5 Minuten). Diese Einstellung gilt nur für den Delivery Controller, auf dem er ausgeführt wurde. Damit alle Delivery Controller übereinstimmen, sollten Sie das Cmdlet auf jedem Delivery Controller ausführen. |
| `Enable-LhcHighAvailabilitySDK` | Aktiviert den Zugriff auf alle Cmdlets `Get-Broker*` innerhalb des Delivery Controller, auf dem es ausgeführt wurde. |
| `Disable-LhcHighAvailabilitySDK` | Deaktiviert den Zugriff auf die Broker-Cmdlets innerhalb des Delivery Controller, auf dem es ausgeführt wurde. |

> **Hinweis:**
>
> - Verwenden Sie Port 89, wenn Sie die Cmdlets `Get-Broker*` auf dem Delivery Controller ausführen. Beispiel:
>
>   ```
>   Get-BrokerMachine -AdminAddress localhost:89
>   ```
>
> - Wenn sich der Broker des lokalen Hostcache auf dem Delivery Controller nicht im Modus "Lokaler Hostcache"befindet, enthält er nur Konfigurationsinformationen.
> - Im Modus "Lokaler Hostcache"enthält der Broker des lokalen Hostcache auf dem ausgewählten Delivery Controller die folgenden Informationen:
>   - Ressourcenzustände
>   - Sitzungsdetails
>   - VDA-Registrierungen
>   - Konfigurationsangaben

## Maschinen und Sitzungen mit der Suche überwachen und verwalten

June 27, 2024

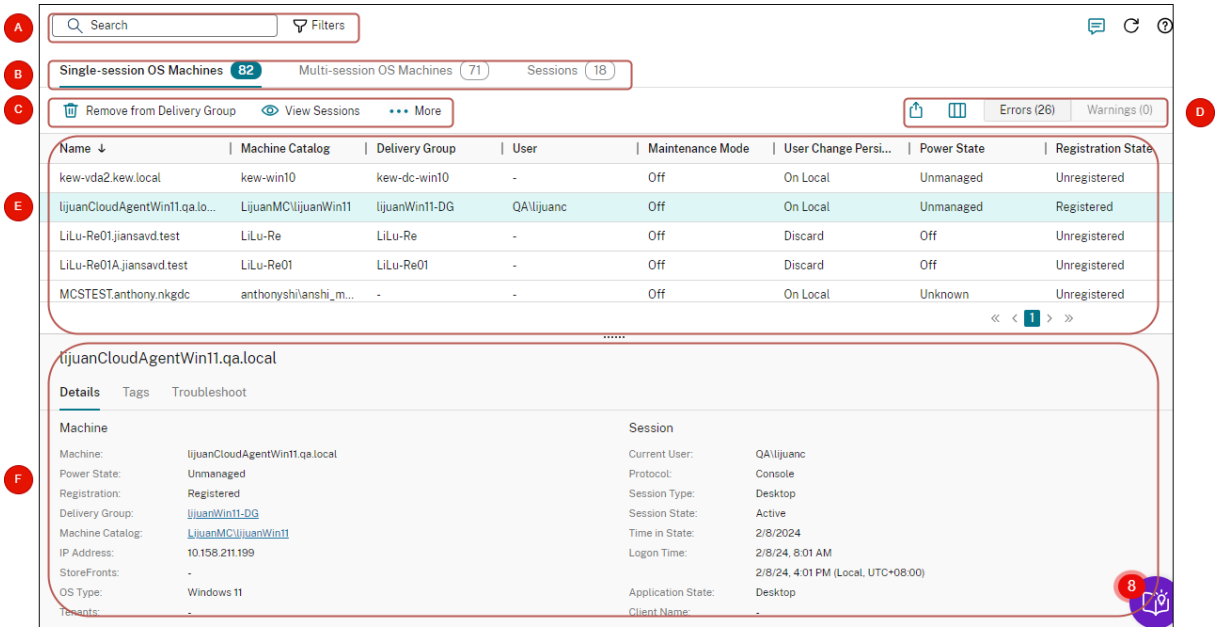
> **Hinweis:**
>
> Sie können Ihre Citrix Virtual Apps and Desktops-Bereitstellung mithilfe von zwei Verwaltungskonsolen verwalten: Web Studio (webbasiert) und Citrix Studio (Windows-basiert). Dieser Artikel behandelt nur Web Studio. Informationen zu Citrix Studio finden Sie im entsprechenden Artikel in Citrix Virtual Apps and Desktops 7 2212 oder früher.

In diesem Artikel erfahren Sie, wie Sie Maschinen und Sitzungen mit dem Knoten **Vollständige Konfiguration > Suchen** überwachen und verwalten.

### Weitere Informationen über den Knoten

Der Knoten **Suche** bietet einen zentralen Ort für die Überwachung und Verwaltung von Maschinen und Benutzersitzungen.




| Legende | Bereich | Beschreibung |
|---|---|---|
| A | Suchleiste | Bietet eine Schnellsuche und eine filterbasierte Suche, mit der Sie komplexe Suchkriterien definieren können. Weitere Informationen finden Sie unter Nach Instanzen suchen. |
| B | Typ-Registerkarten | Zeigt Registerkarten an, auf denen Maschinen nach Typ oder alle Sitzungen aufgelistet werden. Die Anzahl der Instanzen wird in den Registerkartennamen angezeigt. |
| C | Aktionen auf Instanzebene | Zeigt Aktionen an, die Sie auf den *ausgewählten Instanzen* (Maschinen oder Sitzungen) ausführen können. Weitere Informationen finden Sie unter Maschinenaktionen und Sitzungsaktionen. |
| D | Aktionen auf Listenebene | Zeigt Aktionen an, die Sie für die aktuelle *Liste* ausführen können<br>**Exportsymbol**: Exportiert die Liste der in der Hauptansicht angezeigten Instanzen in eine CSV-Datei.<br>-Symbol für **anzuzeigende Spalte**: Passt die Hauptansicht |

| Legende | Bereich | Beschreibung |
| --- | --- | --- |
| E | Hauptansicht | Zeigt die Instanzen und ihre Eigenschaften an. Sie können die Hauptansicht anpassen, indem Sie das Symbol **Anzuzeigende Spalte** auswählen. Weitere Informationen zu den verfügbaren Spalten finden Sie unter Maschinenspalten und Sitzungsspalten. |
| F | Bereich “Details” | Zeigt die folgenden Details an<br>Details der ausgewählten Instanz (Maschine oder Sitzung)<br>Auf die ausgewählte Maschine angewendete Tags<br>Details zu Fehlern oder Warnungen mit der ausgewählten Maschine, einschließlich Problemen, möglichen Ursachen und Lösungsvorschlägen |

## Nach Instanzen suchen

Verwenden Sie die Suchfunktion, um bestimmte Maschinen und Sitzungen zu finden.

- Mit Filtern suchen
- Aktuellen Filtersatz für eine schnelle Suche speichern
- Filterfeld in der Suchleiste fixieren
- Mit dem Schnellsuchfeld suchen
- Tipps zur Verbesserung der Suche

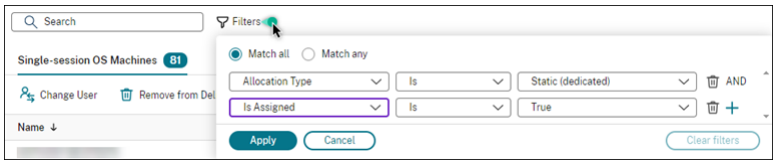
### Mit Filtern suchen

Beispiel: Gehen Sie wie folgt vor, um alle Maschinen mit Einzelsitzungs-OS zu finden, die *statisch* und *Benutzern zugewiesen* sind:

1. Klicken Sie auf der Registerkarte **Maschinen mit Einzelsitzungs-OS** auf das Symbol **Filter**. Das Fenster “Filter”wird angezeigt.

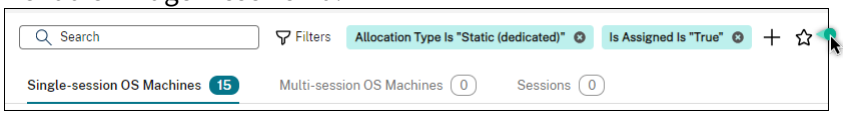
2. Fügen Sie die erforderlichen Filterkriterien hinzu.




3. Wählen Sie **Übereinstimmung mit allen** (AND-Operator), wenn die Suche Ergebnisse zurückgeben soll, die allen Filterkriterien entsprechen. Wählen Sie **Beliebige Übereinstimmung** (OR-Operator), wenn die Suche Ergebnisse zurückgeben soll, die einem der Filterkriterien entsprechen.

4. Klicken Sie auf **Anwenden**.

   In der gefilterten Liste werden alle Maschinen mit Einzelsitzungs-OS angezeigt, die statisch und Benutzern zugewiesen sind.




### Aktuellen Filtersatz für eine schnelle Suche speichern

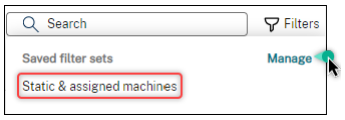
Gehen Sie beispielsweise folgendermaßen vor, um den Filtersatz für Maschinen mit Einzelsitzungs-OS zu speichern, die statisch und Benutzern für die zukünftige Verwendung zugewiesen sind:

1. Nachdem Sie eine filterbasierte Suche durchgeführt haben, klicken Sie in der Suchleiste auf das **Sternsymbol**, wie in der vorherigen Abbildung dargestellt.

2. Geben Sie auf der angezeigten Seite einen Namen für diesen Filtersatz ein (z. B. *Statische und zugewiesene Maschinen*).

3. Klicken Sie auf **Speichern**.

   Der gespeicherte Filtersatz wird in der Liste des Suchverlaufs angezeigt, wenn Sie auf das Suchfeld klicken.



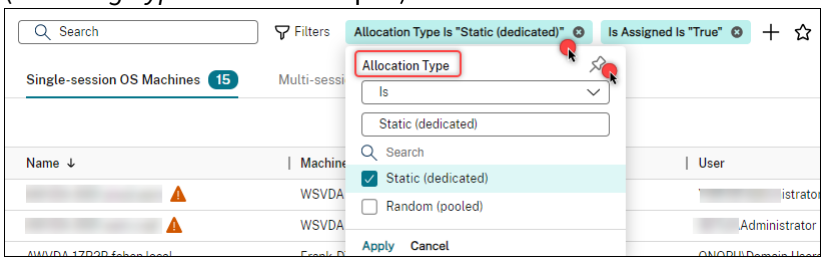

> **Hinweis:**
>
> Filtersätze werden pro Benutzerkonto gespeichert. Um gespeicherte Filtersätze zu verwalten, wählen Sie **Verwalten**.

### Filterfeld in der Suchleiste fixieren

Fixieren Sie häufig verwendete *Filterfelder* in der Suchleiste, um den Zugriff zu erleichtern. Beispiel: Nachdem Sie eine filterbasierte Suche durchgeführt haben, möchten Sie **Zuteilungstyp** in der Suchleiste fixieren. Führen Sie folgende Schritte aus:

1. Klicken Sie in der Suchleiste auf die *Filtereinstellung*.
2. Klicken Sie im daraufhin angezeigten Fenster auf das **Anheftsymbol**, um das Filterfeld (*Zuteilungstyp* für dieses Beispiel) in der Suchleiste zu fixieren.




### Mit dem Schnellsuchfeld suchen

Das Schnellsuchfeld bietet eine bequeme Möglichkeit, anhand namensbezogener Eigenschaften oder gespeicherter Filtersätze nach Instanzen zu suchen. Verfahren:

1. Klicken Sie auf das Suchfeld. Ihre letzten Suchanfragen und gespeicherten Filtersätze werden in der Dropdownliste angezeigt. Sie können auf eine vorherige Suche oder einen Filtersatz klicken, um eine Schnellsuche durchzuführen.
2. Um eine neue Suche zu starten, geben Sie einen vollständigen oder teilweisen Namen aus den folgenden Optionen ein:
    - Maschinenname oder DNS-Name
    - Maschinenkatalogname
    - Bereitstellungsgruppenname
    - Sitzungsbenutzername
    - Name des Sitzungsclients
    - Der vom Hypervisor verwendete Anzeigename der VM, die die Sitzung hostet.
    - Hostingservername

### Tipps zur Verbesserung der Suche

Beachten Sie bei der Verwendung der Suchfunktion die folgenden Tipps:

- Wählen Sie im Knoten **Suchen** eine beliebige Spalte, um Elemente zu sortieren.

- Um weitere Eigenschaften in die Anzeige zu integrieren, anhand derer Sie dann suchen und sortieren können, wählen Sie **Spalten auswählen** oder klicken Sie auf eine beliebige Spalte und wählen Sie **Spalten auswählen**. Aktivieren Sie im Fenster **Spalten auswählen** das Kontrollkästchen neben den anzuzeigenden Elementen, und wählen Sie **Speichern** zum Beenden.

  > **Hinweis:**
  >
  > Spalten, die die Leistung beeinträchtigen, sind mit **Beeinträchtigt die Leistung** gekennzeichnet.

- 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 aufzulisten, wählen Sie im linken Bereich **Bereitstellungsgruppen**. Wählen Sie die Gruppe aus, und wählen Sie dann in der Aktionsleiste oder im Kontextmenü **Maschinen anzeigen**.

Beachten Sie bei Sortierungsvorgängen Folgendes:

- Wenn die Anzahl der Elemente 5000 nicht überschreitet, können Sie auf eine beliebige Spalte klicken, um die darin enthaltenen Elemente zu sortieren. Über 5000 Elemente können Sie nur nach Namen oder nach dem aktuellen Benutzer (je nach gerade geöffneter Registerkarte) sortieren. Filtern Sie die Elemente, um deren Anzahl auf maximal 5.000 zu reduzieren und die Sortierung zu ermöglichen.
- Bei einer Anzahl Elemente von 501 bis 5000 geschieht Folgendes:
  - Alle Daten werden lokal zwischengespeichert, um die Sortierleistung zu verbessern. Auf den Registerkarten **Maschinen mit Betriebssystemen für Einzelsitzungen** und **Maschinen mit Multisitzungs-OS** werden die Daten zwischengespeichert, wenn Sie zum ersten Mal zum Sortieren auf eine Spalte klicken (mit Ausnahme der Spalte **Name**). Auf der Registerkarte **Sitzungen** werden die Daten zwischengespeichert, wenn Sie zum ersten Mal zum Sortieren auf eine Spalte klicken (mit Ausnahme der Spalte **Aktueller Benutzer**). Die Sortierung nimmt daher mehr Zeit in Anspruch. Sortieren Sie für eine schnellere Leistung nach dem Namen oder dem aktuellen Benutzer oder verwenden Sie Filter, um die Anzahl der Elemente zu reduzieren.
  - Die folgende Meldung unterhalb der Tabelle weist darauf hin, dass die Daten zwischengespeichert wurden: Zuletzt aktualisiert: <the time when you refreshed the table>. In diesem Fall basiert die Sortierung auf den zuvor geladenen Elementen. Diese Elemente sind möglicherweise nicht auf dem neuesten Stand. Um sie auf den neuesten Stand zu bringen, klicken Sie auf das Aktualisierungssymbol.

### Anpassen der Spaltenanzeige

Erstellen Sie eine personalisierte Hauptansicht, um die Eigenschaften und Status anzuzeigen, die für Ihren täglichen Betrieb entscheidend sind. Verfahren:

1. Wählen Sie im Knoten **Suchen** nach Bedarf die Registerkarte **Maschine mit Multisitzungs-OS**, **Maschinen mit Einzelsitzungs-OS** oder **Sitzungen**.
2. Klicken Sie in der Aktionsleiste auf das Symbol **Anzuzeigende Spalten** und wählen Sie die Spalten aus.

   Weitere Informationen zu den verfügbaren Spalten und ihren Beschreibungen finden Sie unter Maschinenspalten und Sitzungsspalten.

Beim Auswählen der Spalten werden einige Spalten mit dem Hinweis **Beeinträchtigt die Leistung** ausgewiesen. Das Auswählen dieser Spalten kann die Leistung der Konsole beeinträchtigen. Beachten Sie diese Überlegungen:

- Nachdem Sie Ihre Anpassung abgeschlossen haben, wird die Tabelle aktualisiert, um die ausgewählten Spalten anzuzeigen. Ihr Vorhandensein kann zu Verzögerungen führen, wenn Sie die Tabelle aktualisieren.
- Nachdem Sie den Browser aktualisiert oder sich von der Konsole abgemeldet und dann angemeldet haben, wird eine Meldung angezeigt, in der Sie gefragt werden, ob diese Spalten beibehalten werden sollen. Wenn Sie sich dafür entscheiden, sie beizubehalten, können Sie die Tabelle nur einmal pro Minute aktualisieren, um eine optimale Konsolenleistung zu erzielen. Für häufigere Aktualisierungen entfernen Sie alle Spalten, die die Leistung beeinträchtigen.

## Maschinen und Sitzungen verwalten

Verwenden Sie Aktionen im Suchknoten, um Maschinen- und Sitzungsprobleme zu beheben oder Benutzeranfragen zu verarbeiten.

#### Nützliche Info

Sie können Maschinen auf verschiedenen Ebenen verwalten:

- Auf der Ebene der einzelnen Maschinen. Verwenden Sie den **Suchknoten**, um Zielmaschinen zu finden und Aktionen auszuführen.
- Auf Maschinenkatalogebene, beispielsweise beim Ändern von Masterimages für einen Katalog, Löschen von Maschinen aus einem Katalog und Hinzufügen von Maschinen zu einem Katalog. Weitere Informationen finden Sie unter Verwalten von Maschinenkatalogen.

- Auf Bereitstellungsgruppenebene, beispielsweise beim Ein- oder Ausschalten des Wartungsmodus für Maschinen in einer Gruppe. Weitere Informationen finden Sie unter Bereitstellungsgruppen verwalten.

Zusätzlich zur individuellen Sitzungsebene können Sie Sitzungen auch auf Bereitstellungsgruppenebene verwalten, indem Sie beispielsweise Sitzungsvorabstart und Sitzungsfortbestehen für eine Bereitstellungsgruppe konfigurieren. Weitere Informationen finden Sie unter Bereitstellungsgruppen verwalten.

#### Aktionen auf Maschinen oder Sitzungen ausführen

Gehen Sie folgendermaßen vor, um Maschinen oder Sitzungen auf der Ebene der einzelnen Instanzen zu verwalten:

1. Wählen Sie im Knoten **Suchen** die Registerkarte **Maschine mit Multisitzungs-OS**, **Maschinen mit Einzelsitzungs-OS** oder **Sitzungen**.
2. Wählen Sie je nach Bedarf eine oder mehrere Instanzen aus.
3. Wählen Sie in der Aktionsleiste oder im Rechtsklickmenü eine Aktion aus, die auf den Problemen basiert, die bei diesen Instanzen oder Benutzeranforderungen auftreten.

   Weitere Informationen zu den verfügbaren Aktionen und deren Beschreibungen finden Sie unter Maschinenaktionen und Sitzungsaktionen.

> **Hinweis:**
>
> Wenn Sie zwei oder mehr Instanzen auswählen, sind nur Aktionen verfügbar, die für alle Instanzen gelten.

### Maschinen- oder Sitzungsdaten in CSV-Dateien exportieren

Exportieren Sie die Liste der Instanzen (Maschinen oder Sitzungen), die auf einer Registerkarte angezeigt werden (bis zu 30.000 Elemente), in eine CSV-Datei. Verfahren:

1. Wählen Sie im Knoten **Suchen** nach Bedarf die Registerkarte **Maschine mit Multisitzungs-OS**, **Maschinen mit Einzelsitzungs-OS** oder **Sitzungen**.
2. Klicken Sie dazu auf das **Exportsymbol** in der oberen rechten Ecke.
3. Klicken Sie in dem daraufhin angezeigten Dialogfeld auf **Weiter**.

   Es kann mehrere Minuten dauern, bis der Export abgeschlossen ist. Sie finden die Datei im Standard-Download-Ordner Ihres Browsers.

> **Hinweis:**
>
> Wenn bereits ein Export ausgeführt wird, können Sie auf einer Registerkarte des Knotens **Suchen** keinen weiteren Export ausführen.

## Maschinenaktionen und Spalten

June 27, 2024

In diesem Artikel werden Maschinenaktionen und Spalten mit Beschreibungen als Referenz aufgeführt.

### Aktionen

Sehen Sie sich die Aktionen an, die Sie an Maschinen ausführen können, und deren Beschreibungen.

| Aktion | Beschreibung | Gilt für |
|---|---|---|
| Aus Bereitstellungsgruppe entfernen | Eine Maschine aus der Bereitstellungsgruppe entfernen. | Einzelsitzung und Multisitzung |
| Zu Bereitstellungsgruppe hinzufügen | Fügen Sie einer Bereitstellungsgruppe eine Maschine hinzu. | Einzelsitzung und Multisitzung |
| Sitzungen anzeigen | Sehen Sie sich die Sitzungen an, die auf einer Maschine ausgeführt werden | Einzelsitzung und Multisitzung |
| Tags verwalten | Fügen Sie Tags für eine Maschine hinzu und verwalten Sie sie. Weitere Informationen zu typischen Anwendungsfällen von Tags finden Sie unter Tags. | Einzelsitzung und Multisitzung |

| Aktion | Beschreibung | Gilt für |
| --- | --- | --- |
| Wartungsmodus einschalten | Es kann nötig sein, eine Maschine in den Wartungsmodus zu versetzen, bevor ein Patch angewendet oder ein Problem behandelt wird.<br>Dieser Modus verhindert, dass neue Verbindungen zu dieser Maschine hergestellt werden. Die Benutzer können sich mit Sitzungen auf der Maschine verbinden, auf ihr aber keine neuen Sitzungen starten. | Einzelsitzung und Multisitzung |
| Wartungsmodus ausschalten | Schalten Sie den Wartungsmodus für eine Maschine aus. | Einzelsitzung und Multisitzung |
| VDA aktualisieren | Aktualisieren Sie den VDA für eine Maschine. | Maschinen mit Einzelsitzungs- oder Multisitzungs-OS, die bestimmte Anforderungen erfüllen: Weitere Informationen. |
| Abmelden | Abmelden einer Maschine erzwingen | Einzelsitzung und Multisitzung |
| Löschen | Eine VM aus einem Maschinenkatalog löschen, während Sie sie auf dem Hypervisor oder Clouddienst intakt lassen. | Einzelsitzung und Multisitzung |
| Benutzer ändern | Weisen Sie eine Maschine einem bestimmten Benutzer zu. | *Statische* Einzelsitzungs-OS-Maschinen. |
| Starten | Eine Maschine starten. | Einzelsitzung und Multisitzung |
| Herunterfahren | Eine Maschine herunterfahren. | Einzelsitzung und Multisitzung |
| Neu starten | Maschine neu starten | Einzelsitzung und Multisitzung |

| Aktion | Beschreibung | Gilt für |
| --- | --- | --- |
| Anhalten | Eine Maschine in den Ruhe- oder Anhaltezustand versetzen. Wenn Sie eine Maschine anhalten, speichern Delivery Controller den Speicherinhalt der Maschine in einer Datei und fahren die Maschine dann herunter. | Maschinen mit Einzelsitzungs-OS |
| Fortsetzen | Eine angehaltene Maschine fortsetzen. Wenn Sie eine angehaltene Maschine fortsetzen, starten Delivery Controller die Maschine und setzen sie in den vorherigen Zustand zurück. | Maschinen mit Einzelsitzungs-OS |
| Neustart erzwingen | Erzwingen Sie einen Neustart einer Maschine. | Maschinen mit Einzelsitzungs-OS |
| Herunterfahren erzwingen | Damit können Sie das Herunterfahren einer Maschine erzwingen. | Maschinen mit Einzelsitzungs-OS |

## Spalten

Alle Maschinenspalten und ihre Beschreibungen nach Typ anzeigen:

- Maschine
- Maschinendetails
- Anwendungen
- Hosting
- Verbindung
- Registrierung
- Sitzungsdetails
- Sitzung

### Maschine

Spalten in der Kategorie **Maschine**.

| Spalte | Beschreibung | Gilt für |
| --- | --- | --- |
| Name | Der DNS-Hostname der Maschine. | Einzelsitzung und Multisitzung |
| Maschinenkatalog | Der Name des Katalogs, zu dem die Maschine gehört. | Einzelsitzung und Multisitzung |
| Bereitstellungsgruppe | Der Name der Bereitstellungsgruppe, zu der die Maschine gehört. | Einzelsitzung und Multisitzung |
| Anzeigename für Benutzer | Die vollständigen Namen der Benutzer, die der Maschine zugewiesen sind (normalerweise in der Form `Firstname Lastname`). Zugewiesene Benutzer sind die aktuellen Benutzer für freigegebene Maschinen und die zugewiesenen Benutzer für dedizierte Maschinen. | Einzelsitzung und Multisitzung |
| Benutzer | Die Benutzernamen der Benutzer, die der Maschine zugewiesen sind (in der Form “domain\user”). Zugewiesene Benutzer sind die aktuellen Benutzer für freigegebene Maschinen und die zugewiesenen Benutzer für dedizierte Maschinen. | Einzelsitzung und Multisitzung |
| Benutzerprinzipalname | Die Benutzerprinzipalnamen der Benutzer, die der Maschine zugewiesen sind (in der Form “Benutzer@Domäne”). Zugewiesene Benutzer sind die aktuellen Benutzer für freigegebene Maschinen und die zugewiesenen Benutzer für dedizierte Maschinen. | Einzelsitzung und Multisitzung |

| Spalte | Beschreibung | Gilt für |
| --- | --- | --- |
| Desktopanzeigename | Der veröffentlichte Name der Maschine, die ursprünglich zum Starten der Sitzung verwendet wurde. Dieser Name wird in der Citrix Workspace-App oder in StoreFront angezeigt.<br>**Hinweis:** Um die Anzeige eines Desktops zu ändern, benötigen Sie die Berechtigung **Maschinenupdate ausführen**, da das Ändern des Anzeigenamens eine Aktualisierung der Maschineneigenschaft mit sich bringt. | Nur Einzelsitzung |
| Desktopbedingungen | Die Liste der ausstehenden Desktopbedingungen für die Maschine. Mögliche Werte: Unknown, CPU, ICALatency und UPMLogonTime. | Einzelsitzung und Multisitzung |
| Zuteilungstyp | Der Zuteilungstyp der Maschine: **Permanent**, wenn sie einem Benutzer dauerhaft zugeteilt ist. **Zufällig**, wenn zufällig zugeteilt. | Einzelsitzung und Multisitzung |
| Wartungsmodus | Zeigt an, ob sich die Maschine im Wartungsmodus befindet. | Einzelsitzung und Multisitzung |
| Windows-Verbindungseinstellung | Von Windows gemeldeter Anmeldemodus.<br>Mögliche Werte: LogonEnabled, Draining, DrainingUntilRestart und LogonDisabled. | Nur Multisitzung |

| Spalte | Beschreibung | Gilt für |
| --- | --- | --- |
| Ist zugewiesen | Gibt an, ob einem Benutzer oder einem Client ein dedizierter Desktop zugewiesen wurde (Name/Adresse). Benutzer können explizit oder durch Zuweisung bei der ersten Verwendung der Maschine zugewiesen werden. | Einzelsitzung und Multisitzung |
| Ist physisch | Zeigt an, ob es sich bei der Maschine um eine physische Maschine handelt. `True` gibt an, dass es sich um eine physische Maschine ohne Energieverwaltung durch Delivery Controller handelt. `False` gibt an, dass dies nicht der Fall ist. | Einzelsitzung und Multisitzung |
| Provisioningtyp | Wie die Maschine bereitgestellt wurde. Mögliche Werte<br>Manuell: Wird nicht mit PVS oder MCS bereitgestellt.<br>PVS: Mit PVS bereitgestellt (physische, Blade- und virtuelle Maschinen)<br>MCS: Mit MCS bereitgestellt (nur VMs) | Einzelsitzung und Multisitzung |
| Geplanter Neustart | Der Status aller geplanten Neustartvorgänge für die Maschine. Mögliche Werte<br>Keiner: Es ist kein Neustart geplant.<br>Ausstehend: Wartet auf den Neustart, kann aber verwendet werden.<br>Deaktiviert: Wartet auf den Neustart, ist aber für neue Sitzungen nicht verfügbar. Wiederverbindungen zu bestehenden Verbindungen sind jedoch weiterhin zulässig.<br>In Bearbeitung: Es wird gerade ein geplanter Neustart durchgeführt.<br>Natürlich: Natürlicher Neustart ist im Gange. Die Maschine wartet auf einen Neustart. | Einzelsitzung und Multisitzung |
| Zone | Der Name der Zone, in der sich die Maschine befindet. | Einzelsitzung und Multisitzung |

| Spalte | Beschreibung | Gilt für |
| --- | --- | --- |
| Status | Der Gesamtstatus des mit der Maschine verbundenen Desktops, der aus verschiedenen spezifischen Zuständen wie Sitzungsstatus, Registrierungszustand und Energiezustand abgeleitet wird. Mögliche Status: Aus, Nicht registriert, Verfügbar, Getrennt, InUse und In Vorbereitung. | Einzelsitzung und Multisitzung |
| Tags | Die Liste der Tags, die der Maschine zugeordnet sind. | Einzelsitzung und Multisitzung |
| VDA-Upgrade | Der Maschinenstatus für VDA-Paket-Upgrade-Aktionen. Mögliche Werte: MissingUpgradeType, UpgradeScheduled, UpgradeAvailable, UpToDate und Unknown. | Einzelsitzung und Multisitzung |
| Anhalten-fähig | Zeigt an, ob die Maschine Stromversorgungsaktionen unterstützt (Anhalten und Fortfahren). | Einzelsitzung und Multisitzung |
| Lastindex | Der aktuelle Lastindex. Weitere Informationen finden Sie unter Weitere Informationen. | Nur Multisitzung |
| Drainingzustand | Zeigt an, ob sich die Maschine im Draining befindet und heruntergefahren wird, nachdem alle ihre Sitzungen beendet sind. True wird nur für energieverwaltete Maschinen mit mehreren Sitzungen angezeigt. | Nur Multisitzung |

| Spalte | Beschreibung | Gilt für |
| --- | --- | --- |
| | **Hinweis:** Die Maschine wird nicht heruntergefahren, wenn sie sich im Wartungsmodus befindet. Sie wird erst heruntergefahren, wenn der Wartungsmodus ausgeschaltet ist. | |

#### Maschinendetails

Spalten in der Kategorie **Maschinendetails**.

| Spalte | Beschreibung | Gilt für |
| --- | --- | --- |
| Agentversion | Die Version von Citrix Virtual Delivery Agent (VDA), die auf der Maschine installiert ist. | Einzelsitzung und Multisitzung |
| IP-Adresse | Die IP-Adresse der Maschine. | Einzelsitzung und Multisitzung |
| Ist zugewiesen | Gibt an, ob einem Benutzer oder einem Client ein dedizierter Desktop zugewiesen wurde (Name/Adresse). Benutzer können explizit oder durch Zuweisung bei der ersten Verwendung der Maschine zugewiesen werden. | Einzelsitzung und Multisitzung |
| Betriebssystemtyp | Der Typ des Betriebssystems, das auf der Maschine ausgeführt wird. | Nur Einzelsitzung |

#### Anwendungen

Spalten in der Kategorie **Anwendungen**.

| Spalte | Beschreibung | Gilt für |
| --- | --- | --- |
| Anwendung wird verwendet | Die Liste der auf der Maschine verwendeten Anwendungen (als Browsernamen angezeigt). | Einzelsitzung und Multisitzung |
| Veröffentlichte Anwendungen | Die Liste der von der Maschine veröffentlichten Anwendungen (als Browsernamen angezeigt). | Einzelsitzung und Multisitzung |

**Verbindungen**

Spalten in der Kategorie **Verbindungen**.

| Spalte | Beschreibung | Gilt für |
| --- | --- | --- |
| Client (IP) | Die IP-Adresse des Clients, der mit der Maschine verbunden ist. | Nur Einzelsitzung |
| Client | Der Hostname des Clients, der mit der Maschine verbunden ist. | Nur Einzelsitzung |
| Plug-In-Version | Die Version der Citrix Workspace-App auf dem verbundenen Client. | Nur Einzelsitzung |
| Verbunden durch | Der Hostname der eingehenden Verbindung, in der Regel ein Gateway, Router oder Client. | Nur Einzelsitzung |
| Verbunden durch (IP) | Die IP-Adresse der eingehenden Verbindung, in der Regel ein Gateway, Router oder Client. | Nur Einzelsitzung |
| Verbindungstyp | Das für die Sitzung verwendete Protokoll. Mögliche Werte: HDX, RDP und Console. Hinweis: Das Feld bleibt für Konsolensitzungen auf XenDesktop 5 VDAs leer. | Nur Einzelsitzung |

| Spalte | Beschreibung | Gilt für |
| --- | --- | --- |
| Uhrzeit der letzten Verbindung (UTC) | Die Uhrzeit des letzten erkannten Verbindungsversuchs, der entweder fehlgeschlagen oder erfolgreich war. | Einzelsitzung und Multisitzung |
| Letzter Verbindungsbenutzer | Der SAM-Name (in der Form "DOMAIN\user") des Benutzers, der zuletzt versucht hat, eine Verbindung mit der Maschine herzustellen. Wenn der SAM-Name nicht verfügbar ist, wird die SID verwendet. | Einzelsitzung und Multisitzung |
| Secure ICA aktiv | Gibt an, ob SecureICA in der aktuellen Sitzung aktiv ist. Immer Null für Maschinen mit mehreren Sitzungen. | Einzelsitzung und Multisitzung |

**Hosting**

Spalten in der Kategorie **Hosting**.

| Spalte | Beschreibung | Gilt für |
| --- | --- | --- |
| VM | Der vom Hypervisor verwendete Anzeigename einer gehosteten Maschine, auf der die Sitzung ausgeführt wird. Er stimmt nicht unbedingt mit dem DNS- oder AD-Namen der Maschine überein. | Einzelsitzung und Multisitzung |
| Hostingservername | Der DNS-Name des Hypervisors, der die Maschine hostet, sofern sie verwaltet wird. | Einzelsitzung und Multisitzung |
| Verbindung | Der Name der Hostverbindung, die der Maschine zugewiesen ist, die die Sitzung hostet. | Einzelsitzung und Multisitzung |

| Spalte | Beschreibung | Gilt für |
| --- | --- | --- |
| Ausstehendes Update | Gibt an, ob das VM-Image für eine gehostete Maschine veraltet ist und beim nächsten Neustart der Maschine auf ein neues Image aktualisiert werden muss. | Einzelsitzung und Multisitzung |
| Benutzeränderungspersistenz | Wie Benutzeränderungen behandelt werden, wobei angegeben wird, ob die Änderungen persistent sind<br>OnLocal: Persistent. Benutzeränderungen werden lokal gespeichert.<br>Verworfen: Nicht persistent. Benutzeränderungen werden verworfen. | Einzelsitzung und Multisitzung |
| Ausstehende Energieaktion | Zeigt an, ob Energieaktionen für die Maschine ausstehen. | Einzelsitzung und Multisitzung |
| Energiezustand | Der Energiezustand der Maschine. Mögliche Werte: Nicht verwaltet, Unbekannt, Nicht verfügbar, Aus, Ein, Angehalten, Wird eingeschaltet, Wird ausgeschaltet, Wird angehalten und Wird fortgesetzt. | Einzelsitzung und Multisitzung |
| Wird nach Verwendung heruntergefahren | Gilt nur für Maschinen mit Energieverwaltung und Einzelsitzung. Zeigt an, ob die Maschine unsauber ist und heruntergefahren wird, wenn alle Sitzungen beendet sind.<br>**Hinweis:** Die Maschine wird nicht heruntergefahren, wenn sie sich im Wartungsmodus befindet. Sie wird erst heruntergefahren, nachdem sie den Wartungsmodus verlassen hat. | Nur Einzelsitzung |

**Registrierung**

Spalten in der Kategorie **Registrierung**.

| Spalte | Beschreibung | Gilt für |
| --- | --- | --- |
| Letzter Registrierungsfehler | Der Grund für die letzte Abmeldung der Maschine beim Broker.<br>Mögliche Werte sind: AgentShutdown, AgentSuspended, AgentRequested, IncompatibleVersion, AgentAddressResolutionFailed, AgentNotContactable, AgentWrongActiveDirectoryOU, EmptyRegistrationRequest, MissingRegistrationCapabilities, MissingAgentVersion, InconsistentRegistrationCapabilities, NotLicensedForFeature, UnsupportedCredentialSecurityVersion, InvalidRegistrationRequest, SingleMultiSessionMismatch, FunctionalLevelTooLowForCatalog, FunctionalLevelTooLowForDesktopGroup, PowerOff, DesktopRestart, DesktopRemoved, AgentRejectedSettingsUpdate, SendSettingsFailure, SessionAuditFailure, SessionPrepareFailure, ContactLost, SettingsCreationFailure, UnknownError und BrokerRegistrationLimitReached. | Einzelsitzung und Multisitzung |
| Zeitpunkt des letzten Registrierungsfehlers (UTC) | Der Zeitpunkt der letzten Registrierungsaufhebung der Maschine. | Einzelsitzung und Multisitzung |

| Spalte | Beschreibung | Gilt für |
| --- | --- | --- |
| Registrierungszustand | Der Registrierungszustand der Maschine. Mögliche Werte: Unregistered, Initializing, Registered und AgentError. | Einzelsitzung und Multisitzung |
| Fehlerzustand | Der zusammenfassende Status aller aktuellen Fehlerzustände der Maschine. Mögliche Werte Keiner: Kein Fehler. Die Maschine ist fehlerfrei. FailedToStart: Der letzte Einschaltvorgang für die Maschine ist fehlgeschlagen. StuckOnBoot: Die Maschine konnte nach dem Einschalten nicht gestartet werden. Nicht registriert. Die Maschine konnte nicht innerhalb des erwarteten Zeitraums registriert werden oder ihre Registrierung wurde abgelehnt. Max. Kapazität. Die Maschine meldet sich selbst mit maximaler Kapazität. | Einzelsitzung und Multisitzung |

**Sitzungsdetails**

Spalten in der Kategorie **Sitzungsdetails**.

| **Spalte** | **Beschreibung** | **Gilt für** |
| --- | --- | --- |
| Gestartet über | Der Hostname des StoreFront-Servers, der zum Starten der aktuellen Brokersitzung verwendet wird. Immer Null für Maschinen mit mehreren Sitzungen. | Einzelsitzung und Multisitzung |
| Gestartet über (IP) | Die IP-Adresse des StoreFront-Servers, der zum Starten der aktuellen Brokersitzung verwendet wird. Immer Null für Maschinen mit mehreren Sitzungen. | Einzelsitzung und Multisitzung |
| Uhrzeit der Sitzungsänderung (UTC) | Die Uhrzeit der letzten Statusänderung der aktuellen Sitzung. | Nur Einzelsitzung |

| Spalte | Beschreibung | Gilt für |
| --- | --- | --- |
| SmartAccess-Filter | Smart Access-Tags für die aktuelle Sitzung. Immer Null für Maschinen mit mehreren Sitzungen. | Einzelsitzung und Multisitzung |

#### Sitzung

Spalten in der Kategorie **Sitzung**.

| Spalte | Beschreibung | Gilt für |
| --- | --- | --- |
| Sitzungszustand | Der Status der aktuellen Sitzung. Mögliche Werte: Other, PreparingSession, Connected, Active, Disconnected, Reconnecting, NonBrokeredSession und Unknown. | Nur Einzelsitzung |
| Aktueller Benutzer | Der Name des Benutzers der aktuellen Sitzung (in der Form “DOMAIN\user”). | Nur Einzelsitzung |
| Startzeit (UTC) | Die Startzeit der aktuellen Sitzung. | Nur Einzelsitzung |
| Sitzungsanzahl | Die Anzahl der Sitzungen auf der Maschine. | Nur Multisitzung |

## Sitzungsaktionen und Spalten

June 27, 2024

In diesem Artikel werden Maschinenaktionen und Spalten mit Beschreibungen als Referenz aufgeführt.

### Aktionen

Sehen Sie sich die Aktionen an, die Sie an Sitzungen ausführen können, und deren Beschreibungen.

| Aktion | Beschreibung | Gilt für Sitzungen auf |
|---|---|---|
| Abmelden | Einen Benutzer von einer Sitzung abmelden. | Maschinen mit Einzelsitzungs-OS oder mit Multisitzungs-OS |
| Nachricht senden | Eine Nachricht an den Benutzer einer Sitzung senden. | Maschinen mit Einzelsitzungs-OS oder mit Multisitzungs-OS |
| Maschinen anzeigen | Hostingmaschine für eine Sitzung anzeigen. | Maschinen mit Einzelsitzungs-OS oder mit Multisitzungs-OS |
| Trennen | Sitzung trennen. Wenn eine Sitzung getrennt wird, bleibt sie aktiv und die Anwendungen werden weiter ausgeführt, das Benutzergerät kommuniziert jedoch nicht mehr mit den Delivery Controllern. | Maschinen mit Einzelsitzungs-OS oder mit Multisitzungs-OS |
| Maschine herunterfahren | Die mit einer Sitzung verbundene Maschine herunterfahren. | Maschinen mit Einzelsitzungs-OS |
| Maschine neu starten | Neustart einer Maschine durchführen, die einer Sitzung zugeteilt ist. | Maschinen mit Einzelsitzungs-OS |

### Spalten

Sitzungsspalten und ihre Beschreibungen anzeigen.

| Spalte | Beschreibung |
|---|---|
| Aktueller Benutzer | Der Name des Benutzers; der Benutzerprinzipalname (User Principal Name, UPN). |

| Spalte | Beschreibung |
| --- | --- |
| Name | Der DNS-Hostname der Maschine, die die Sitzung hostet. |
| Bereitstellungsgruppe | Der Name der Bereitstellungsgruppe, die die Hostmaschine der Sitzung enthält. |
| Maschinenkatalog | Der Name des Maschinenkatalogs, der die Hostmaschine der Sitzung enthält. |
| Agentversion | Die Version des Citrix Virtual Delivery Agent (VDA), die auf der Maschine installiert ist, auf der die Sitzung gehostet wird. |
| Anwendung wird verwendet | Die Liste der in der Sitzung verwendeten Anwendungen, identifiziert durch ihre Administratornamen. |
| Autonom vermittelt | Ob es sich um eine HDX-Sitzung handelt, die über eine direkte Verbindung ohne Vermittlung eingerichtet wurde. |
| Brokerzeit (UTC) | Der Zeitpunkt, zu dem die Sitzung vermittelt wurde. |
| Vermittlungsbenutzername | Der Name des Vermittlungsbenutzers. |
| Client (IP) | Die IP-Adresse des Clients, der mit der Sitzung verbunden ist. |
| Client | Der Hostname des Clients, der mit der Sitzung verbunden ist. |
| Plug-In-Version | Die Version der Citrix Workspace-App, die auf dem mit der Sitzung verbundenen Client ausgeführt wird. |
| Verbunden durch | Der Hostname der eingehenden Verbindungen, in der Regel ein Gateway, Router oder Client. |
| Verbunden durch (IP) | Die IP-Adresse der eingehenden Verbindung, in der Regel ein Gateway, Router oder Client. |
| Zuteilungstyp | Ob die Sitzung geteilt oder dediziert ist. |
| Ausgeblendet | Ob die Sitzung vor dem Benutzer verborgen ist und nicht erneut verbunden werden soll. |
| VM | Der vom Hypervisor verwendete Anzeigename der VM, die die Sitzung hostet. Er stimmt nicht unbedingt mit dem DNS- oder AD-Namen der Maschine überein. |

| Spalte | Beschreibung |
| --- | --- |
| Hostingservername | Der DNS-Name des Hypervisors, der die Hostmaschine der Sitzung hostet. |
| Verbindung | Der Name der Hostverbindung, die der Maschine zugewiesen ist, die die Sitzung hostet. |
| Ausstehendes Update | Ob das VM-Image für eine gehostete Maschine veraltet ist und beim nächsten Neustart der Maschine auf ein neues Image aktualisiert werden muss. |
| Wartungsmodus | Ob sich die Maschine, die die Sitzung hostet, im Wartungsmodus befindet. |
| IP-Adresse | Die IP-Adresse der Maschine, die die Sitzung hostet. |
| Ist physisch | Zeigt an, ob es sich bei der Maschine, die die Sitzung hostet, um eine physische Maschine handelt. `True` gibt an, dass es sich um eine physische Maschine ohne Energieverwaltung durch Delivery Controller handelt. `False` gibt an, dass dies nicht der Fall ist. |
| Gestartet über | Der Hostname des StoreFront-Servers, der zum Starten der Sitzung verwendet wird. Leer, wenn die Sitzung über Workspace gestartet wurde. |
| Gestartet über (IP) | Die IP-Adresse des StoreFront-Servers, der zum Starten der Sitzung verwendet wurde. Leer, wenn die Sitzung über Workspace gestartet wurde. |
| Betriebssystemtyp | Die Identifikationszeichenfolge des Betriebssystems, das die Sitzung hostet. |
| Benutzeränderungspersistenz | Wie Benutzeränderungen behandelt werden, wobei angegeben wird, ob die Änderungen persistent sind<br>OnLocal: Persistent. Benutzeränderungen werden lokal gespeichert.<br>Verwerfen: Nicht persistent. Benutzeränderungen werden verworfen. |
| Verbindungstyp | Das für die Sitzung verwendete Protokoll, z. B. HDX, RDP oder Console.<br>**Hinweis:** Das Feld ist leer für Konsolensitzungen auf XenDesktop 5 VDAs. |
| Provisioningtyp | Wie die Maschine, die die Sitzung hostet, bereitgestellt wurde<br>Manuell: Wird nicht mit PVS oder MCS bereitgestellt.<br>PVS: Wird von PVS bereitgestellt (physische Maschinen, Blade-Maschinen und virtuelle Maschinen)<br>MCS: Von MCS bereitgestellt (nur VMs). |

| Spalte | Beschreibung |
| --- | --- |
| Secure ICA aktiv | Ob SecureICA in der Sitzung aktiv ist. |
| Sitzungszustand | Der Status der Sitzung. Mögliche Werte: Verbunden, Aktiv oder Getrennt. Andere Zustände können für Sitzungen auf Maschinen mit Funktionsebenen vor L7 auftreten, z. B. PreparingSession, Reconnecting, NonBrokeredSession, Other und Unknown. |
| Uhrzeit der Sitzungsänderung | Die Uhrzeit der letzten Statusänderung für die Sitzung. |
| Anwendungszustand | Der Status der Anwendungen in der Sitzung. Mögliche Werte: PreLogon, PreLaunched, Active, Desktop, Lingering und NoApps. |
| Sitzungsunterstützung | Ob die Maschine, die die Sitzung hostet, mehrere oder einzelne Sitzungen unterstützt. |
| Zone | Name der Zone, in der sich die Maschine befindet, die die Sitzung hostet. |
| SmartAccess-Filter | Smart Access-Tags für die Sitzung. |
| Startzeit (UTC) | Wann die Sitzung gestartet wurde. |
| Status | Der zusammenfassende Status der Maschine. Mögliche Werte: Unregistered, Disconnected oder InUse. |
| Zeit in Zustand (UTC) | Wie lange sich die Sitzung in ihrem aktuellen Zustand befindet. |
| Delivery Controller | Der DNS-Hostname des Controllers, bei dem die Hostmaschine der Sitzung registriert ist. |
| Anzeigename für Benutzer | Der vollständige Name des Benutzers. |

| Spalte | Beschreibung |
| --- | --- |
| Desktopanzeigename | Der veröffentlichte Name der Maschine, die ursprünglich zum Starten der Sitzung verwendet wurde. Dieser Name wird in der Citrix Workspace-App oder in StoreFront angezeigt. Bei Anwendungssitzungen ist dies der Name der ersten Anwendung, die in der Sitzung gestartet wurde, auch wenn diese Anwendung inzwischen beendet wurde. Der Name bleibt unverändert, auch wenn die Ressource später umbenannt oder entfernt wird. |

## Sicherheitsschlüssel verwalten

June 27, 2024

> **Wichtig:**
>
> - Sie müssen dieses Feature in Kombination mit StoreFront 1912 LTSR CU2 oder höher verwenden.
> - Secure XML wird nur von Citrix ADC und Citrix Gateway ab Version 12.1 unterstützt.
>
> **Hinweis:**
>
> Sie können Ihre Citrix Virtual Apps and Desktops-Bereitstellung mithilfe von zwei Verwaltungskonsolen verwalten: Web Studio (webbasiert) und Citrix Studio (Windows-basiert). Dieser Artikel behandelt nur Web Studio. Informationen zu Citrix Studio finden Sie im entsprechenden Artikel in Citrix Virtual Apps and Desktops 7 2212 oder früher.

Mit diesem Feature können nur genehmigte StoreFront- und Citrix Gateway-Maschinen mit 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 Web Studio, um die Feature-Einstellungen anzuzeigen.
2. Konfigurieren Sie die Einstellungen für Ihre Site.

3. Konfigurieren Sie die Einstellungen für StoreFront.
4. Konfigurieren Sie die Einstellungen für Citrix ADC.

### Web Studio aktivieren, um die Feature-Einstellungen anzuzeigen

Standardmäßig sind die Einstellungen für Sicherheitsschlüssel in Web Studio ausgeblendet. Verwenden Sie das PowerShell-SDK wie folgt, damit Web Studio sie anzeigen kann:

1. Führen Sie das Citrix Virtual Apps and Desktops 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 PowerShell SDK finden Sie unter SDKs und APIs.

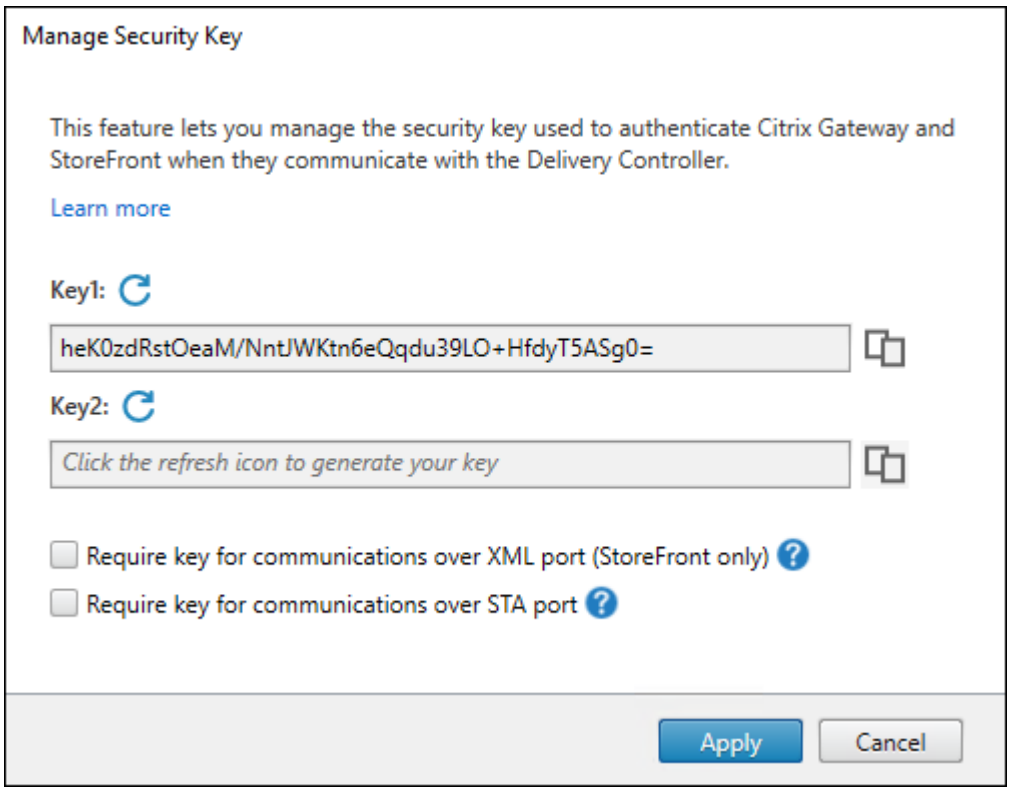
### Einstellungen für die Site konfigurieren

Sie können die Sicherheitsschlüsseleinstellungen für Ihre Site mit Web Studio oder PowerShell konfigurieren.

#### Web Studio verwenden

1. Melden Sie sich bei Web Studio an und wählen Sie im linken Bereich **Einstellungen**.
2. Suchen Sie die Kachel **Sicherheitsschlüssel verwalten** und klicken Sie auf **Bearbeiten**. Die Seite **Sicherheitsschlüssel verwalten** wird angezeigt.




3. Klicken Sie auf das Aktualisierungssymbol, um die Schlüssel zu generieren.

> **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.

4. Wählen Sie aus, wo ein Schlüssel für die Kommunikation erforderlich ist:

   - **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.

5. Klicken Sie auf **Speichern**, um die Änderungen anzuwenden und das Fenster zu schließen.

#### PowerShell verwenden

Nachfolgend sind die den Web 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.

### Einstellungen für StoreFront konfigurieren

Nach Abschluss der Konfiguration für Ihre Site müssen Sie relevante Einstellungen für 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 |

```
$store = Get-STFStoreService -VirtualPath [Path to store]
$farm = Get-STFStoreFarm -StoreService $store -FarmName [Resource feed
    name]
Set-STFStoreFarm -Farm $farm -XMLValidationEnabled $true -
    XMLValidationSecret [secret]
<!--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:

```
$gateway = Get-STFRoamingGateway -Name [Gateway name]
$sta1 = New-STFSecureTicketAuthority -StaUrl [STA1 URL] -
    StaValidationEnabled $true -StaValidationSecret [secret]
$sta2 = New-STFSecureTicketAuthority -StaUrl [STA2 URL] -
    StaValidationEnabled $true -StaValidationSecret [secret]
Set-STFRoamingGateway -Gateway $gateway -SecureTicketAuthorityObjs
    $sta1,$sta2
<!--NeedCopy-->
```

Geben Sie die entsprechenden Werte für die folgenden Parameter ein:

- `Gateway name`
- `STA URL`
- `Secret`

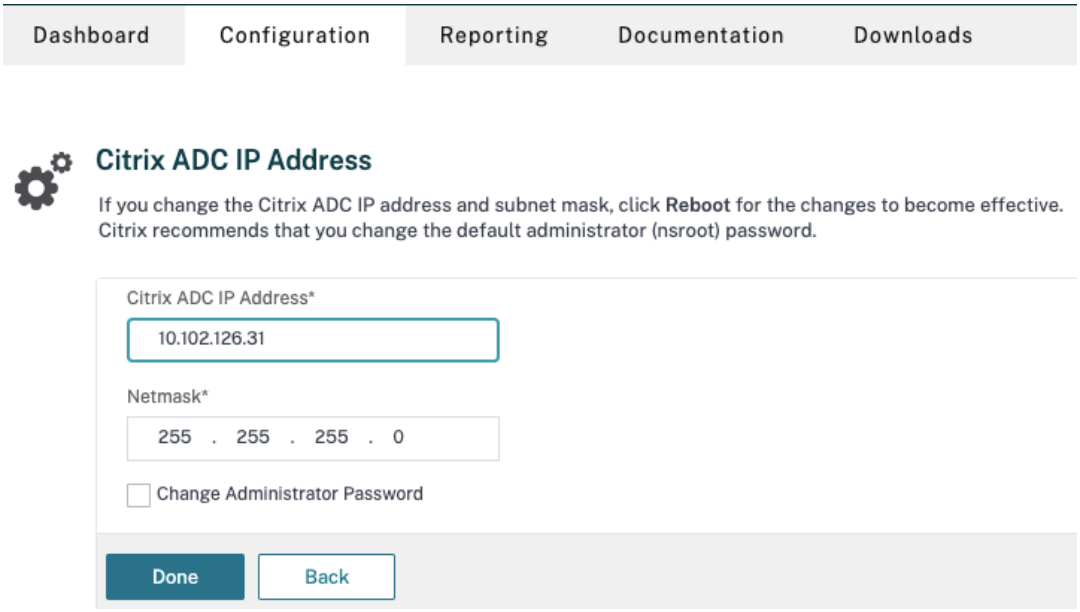
Anleitungen und Informationen zur Syntax finden Sie in der Hilfe zu PowerShell-Befehlen.

### Einstellungen für Citrix ADC konfigurieren

> **Hinweis:**
>
> Die Konfiguration dieses Features für Citrix ADC ist nur erforderlich, wenn Sie Citrix ADC als Gateway verwenden. Führen Sie folgende Schritte aus, wenn Sie Citrix ADC verwenden:

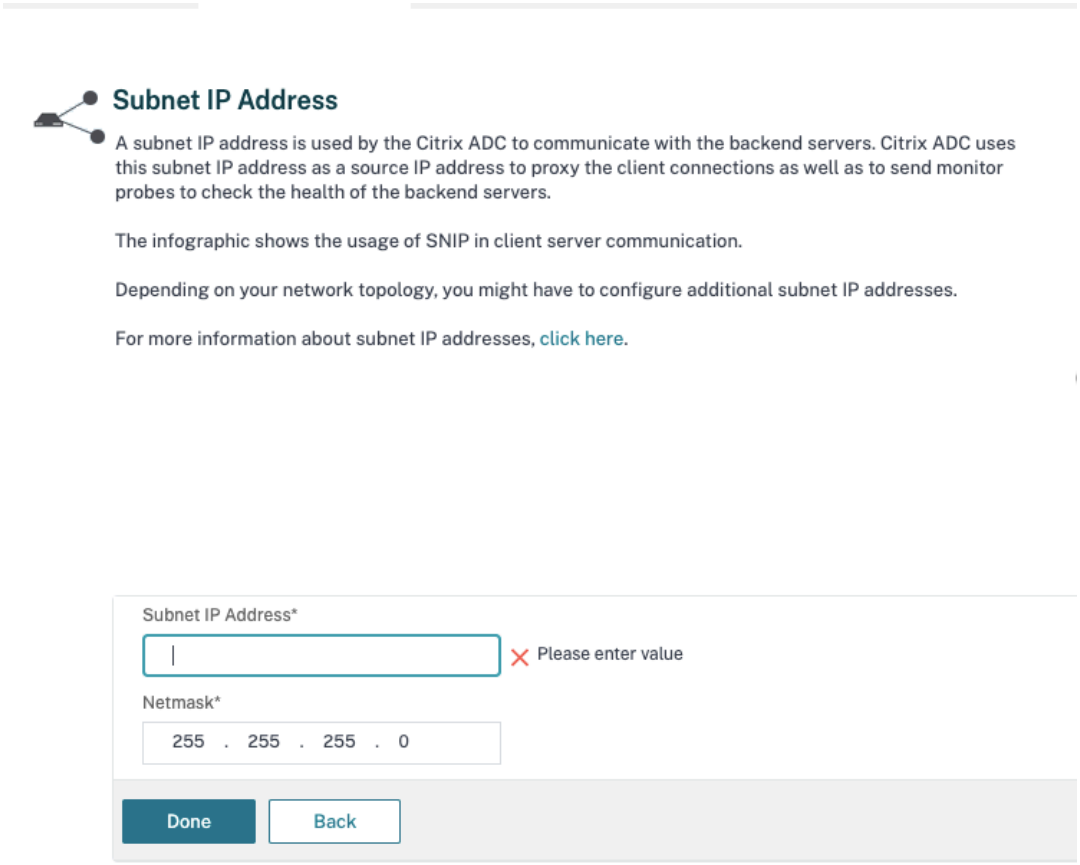
1. Vergewissern Sie sich, dass die erforderliche Konfiguration ausgeführt wurde:
    - Die folgenden IP-Adressen im Zusammenhang mit Citrix ADC wurden konfiguriert.
        - Citrix ADC Management-IP-Adresse (NSIP) für den Zugriff auf die Citrix ADC-Konsole. Weitere Informationen finden Sie unter Konfigurieren der NSIP-Adresse.



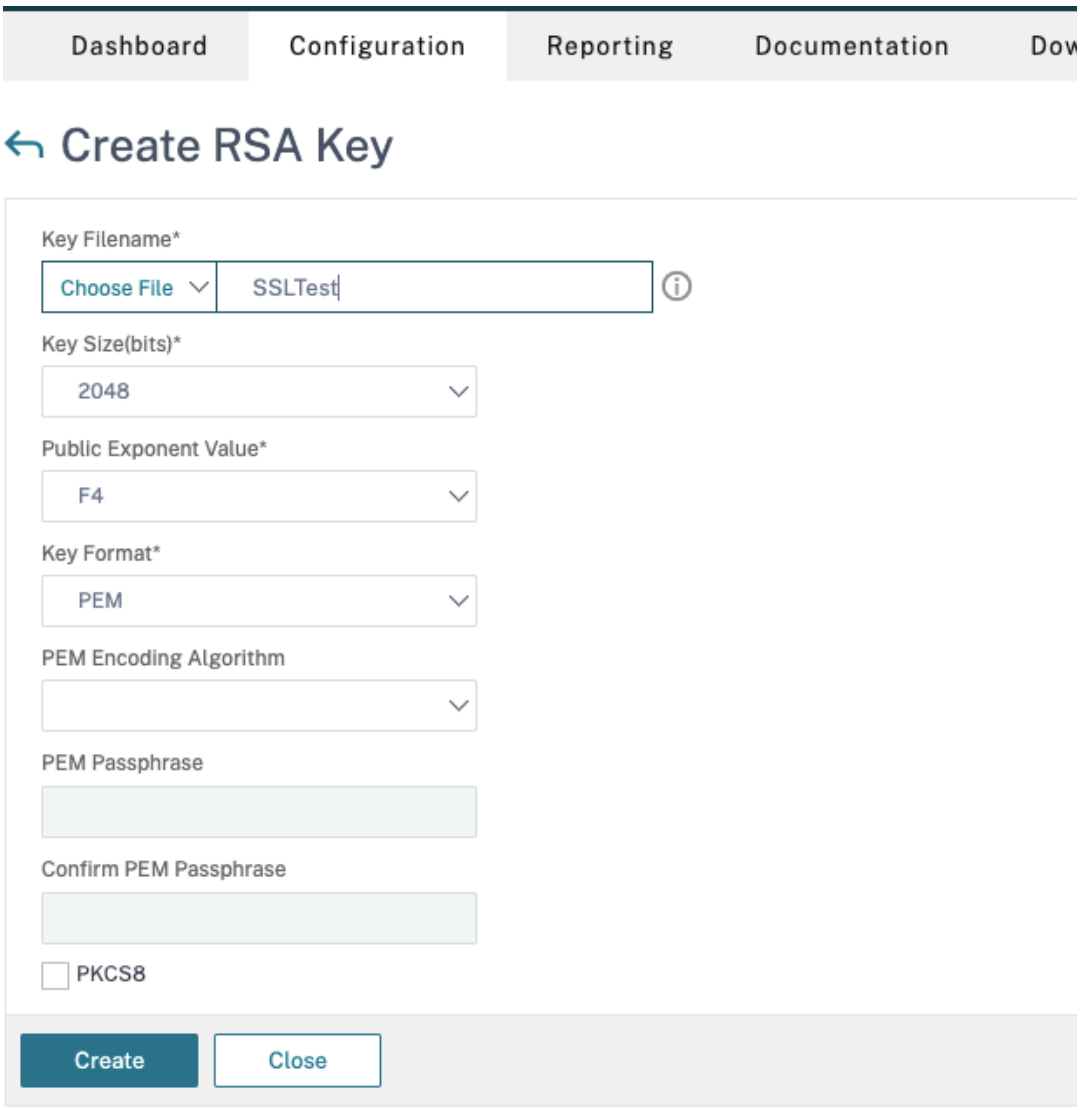

- Subnetz-IP-Adresse (SNIP) zur Kommunikation zwischen der Citrix ADC Appliance und den Back-End-Servern. Weitere Informationen finden Sie unter Konfigurieren von Subnetz-IP-Adressen.
- Virtuelle IP-Adresse von Citrix Gateway und des Load Balancers zur Anmeldung bei der ADC Appliance für den Sitzungsstart. Weitere Informationen finden Sie unter Erstellen eines virtuellen Servers.



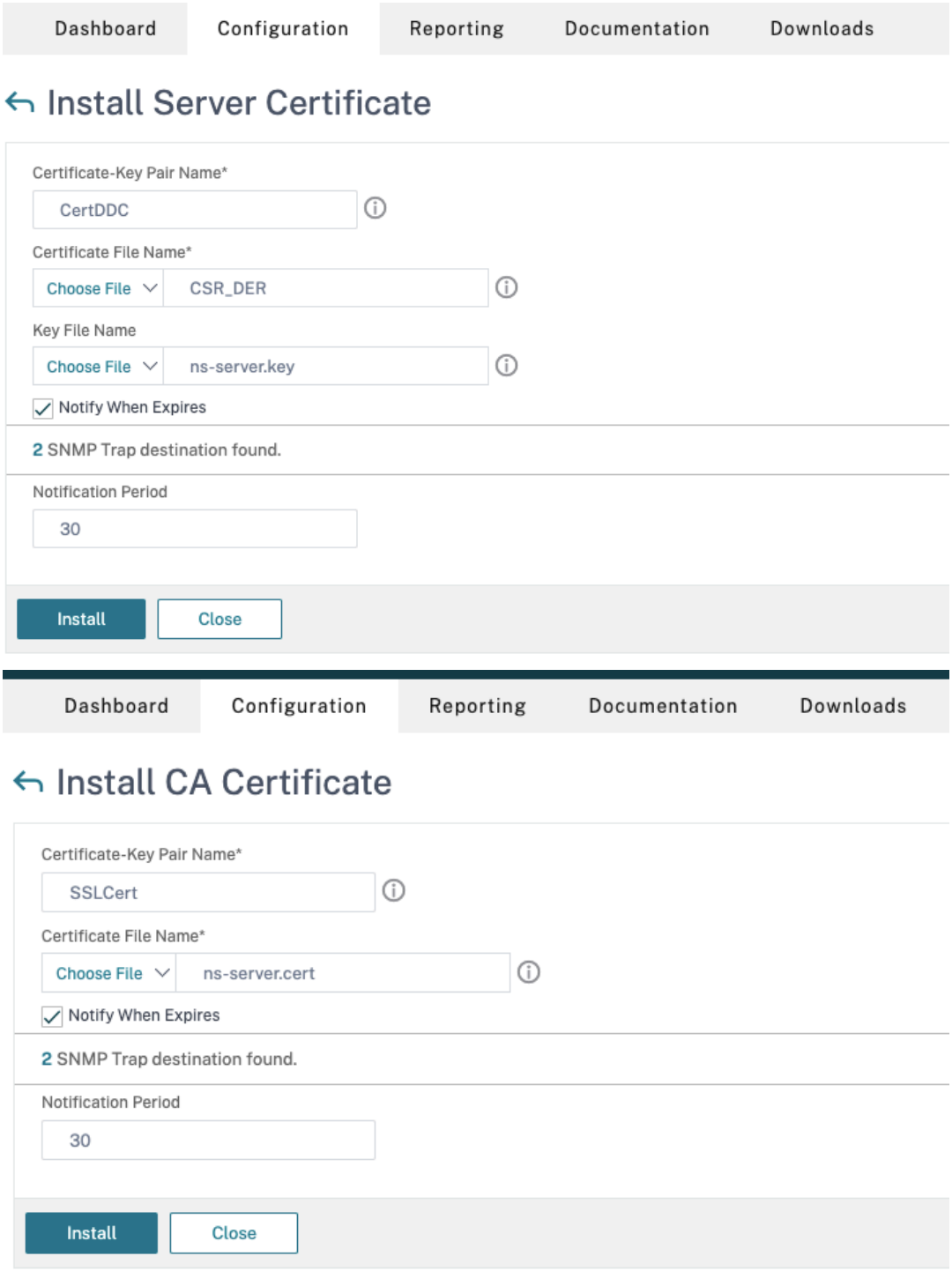

- Die erforderlichen Modi und Features in der Citrix ADC Appliance sind aktiviert.
  - Um die Modi zu aktivieren, gehen Sie in Citrix ADC zu **System > Settings > Configure Mode**.
  - Um die Features zu aktivieren, gehen Sie in Citrix ADC zu **System > Settings > Configure Basic Features**.
- Die Konfiguration für Zertifikate wurde ausgeführt.
  - Die Zertifikatsignieranforderung (CSR) wurde erstellt. Weitere Informationen finden Sie unter Erstellen eines Zertifikats.



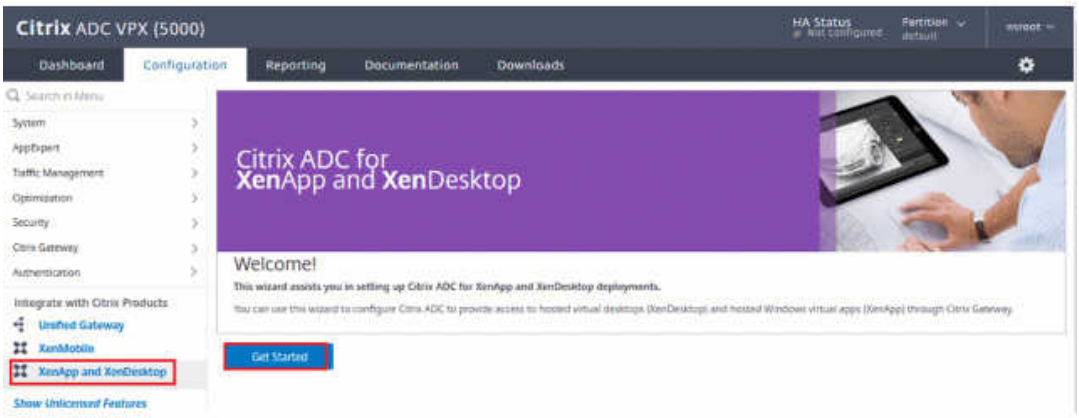

- Das Serverzertifikat, das ZS-Zertifikat und das Stammzertifikat wurden installiert. Weitere Informationen finden Sie unter Installieren, Links und Updates.




- Für Citrix Virtual Desktops wurde ein Citrix Gateway erstellt. Testen Sie die Verbindung durch Klicken auf die Schaltfläche **Test STA Connectivity**, um sicherzustellen, dass die virtuellen Server online sind. Weitere Informationen finden Sie unter Einrichten von Citrix ADC für Citrix Virtual Apps and Desktops.

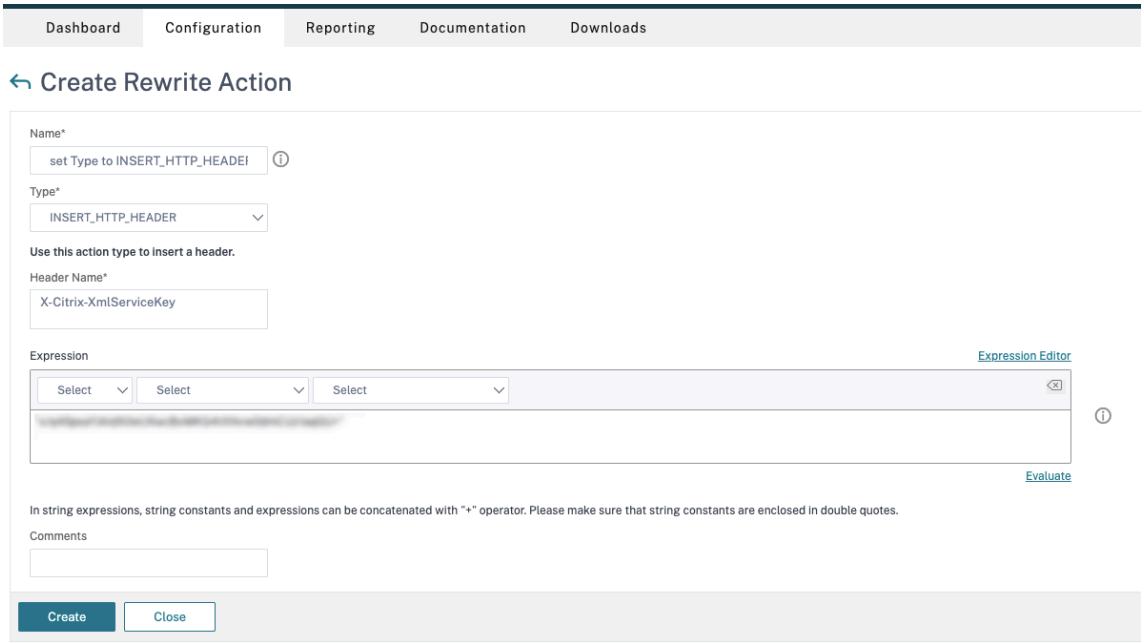
 




2. Fügen Sie eine Rewrite-Aktion hinzu. Weitere Informationen finden Sie unter Konfigurieren einer Rewrite-Aktion.

   a) Gehen Sie zu **AppExpert > Rewrite > Actions**.

   b) Klicken Sie auf **Hinzufügen**, um eine neue Rewrite-Aktion hinzuzufügen. Sie können die Aktion “set Type to INSERT_HTTP_HEADER”nennen.



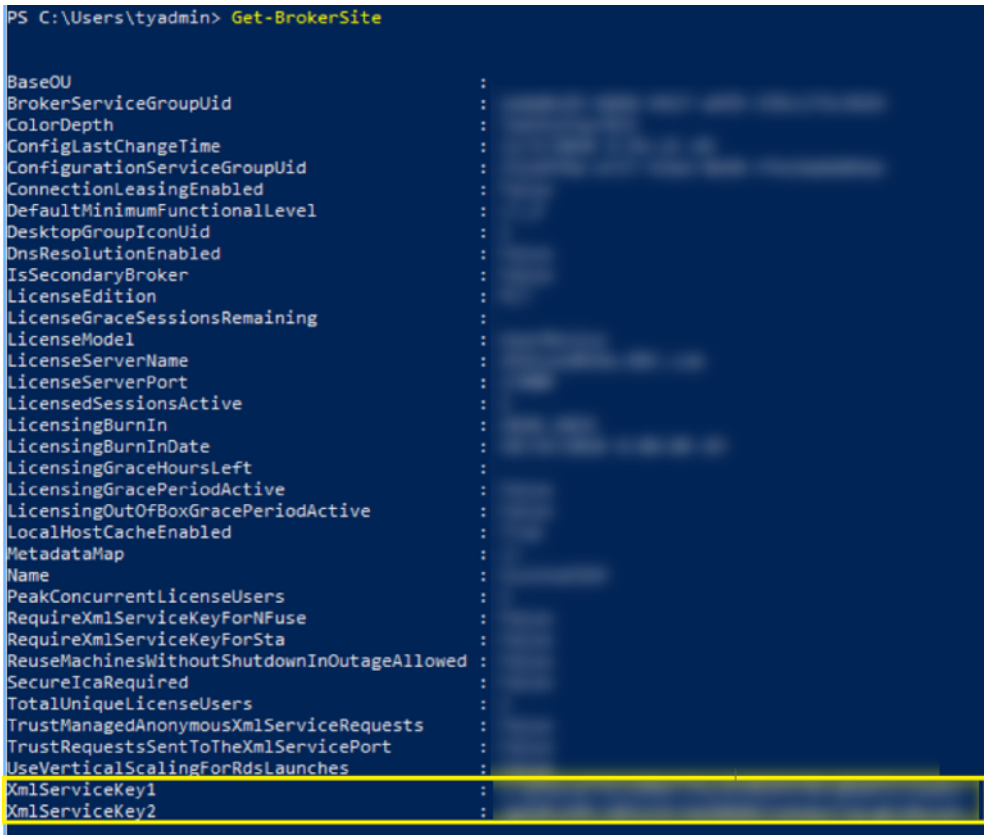

   a) Wählen Sie unter **Type** die Option **INSERT_HTTP_HEADER**.

   b) Geben Sie im Feld **Header Name** “X-Citrix-XmlServiceKey”ein.

   c) Fügen Sie unter **Ausdruck** <`XmlServiceKey1 value`> mit Anführungszeichen hinzu.

Sie können den XmlServiceKey1-Wert aus der Desktop Delivery Controller-Konfiguration kopieren.

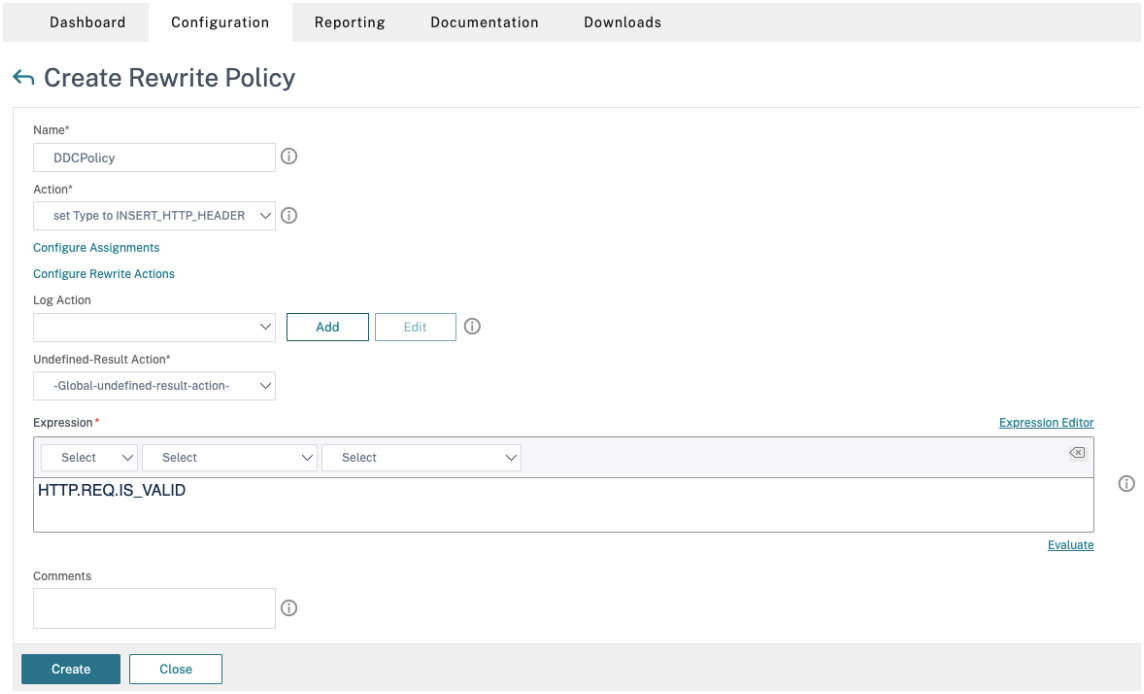



3. Fügen Sie eine Rewrite-Richtlinie hinzu. Weitere Informationen finden Sie unter Konfigurieren einer Rewrite-Richtlinie.

   a) Gehen Sie zu **AppExpert > Rewrite > Policies**.

   b) Klicken Sie auf **Add**, um eine neue Richtlinie hinzuzufügen.




a) Wählen Sie unter **Action** die im vorherigen Schritt erstellte Aktion aus.
b) Fügen Sie unter **Expression** “HTTP.REQ.IS_VALID”hinzu.
c) Klicken Sie auf **OK**.

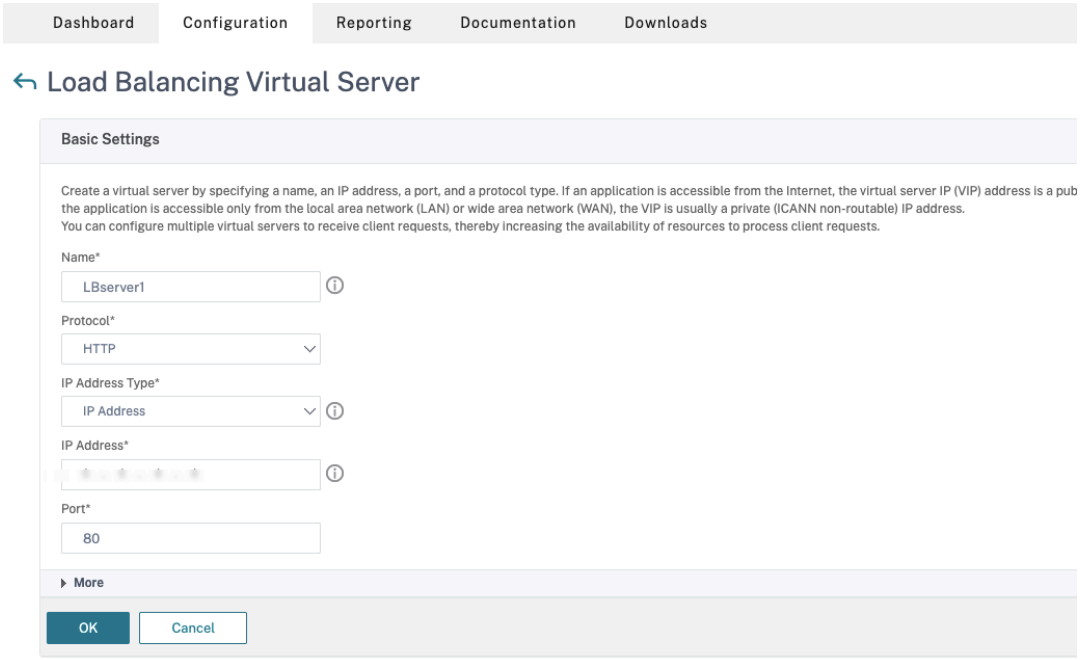
4. Richten Sie den Lastenausgleich ein. Sie müssen einen virtuellen Lastausgleichsserver pro STA-Server konfigurieren. Ansonsten können die Sitzungen nicht gestartet werden.

   Weitere Informationen finden Sie unter Einrichten des einfachen Lastenausgleichs.

   a) Erstellen Sie einen virtuellen Lastausgleichsserver.

      - Gehen Sie zu **Traffic Management > Load Balancing > Servers**.
      - Klicken Sie auf der Seite **Virtual Servers** auf **Add**.

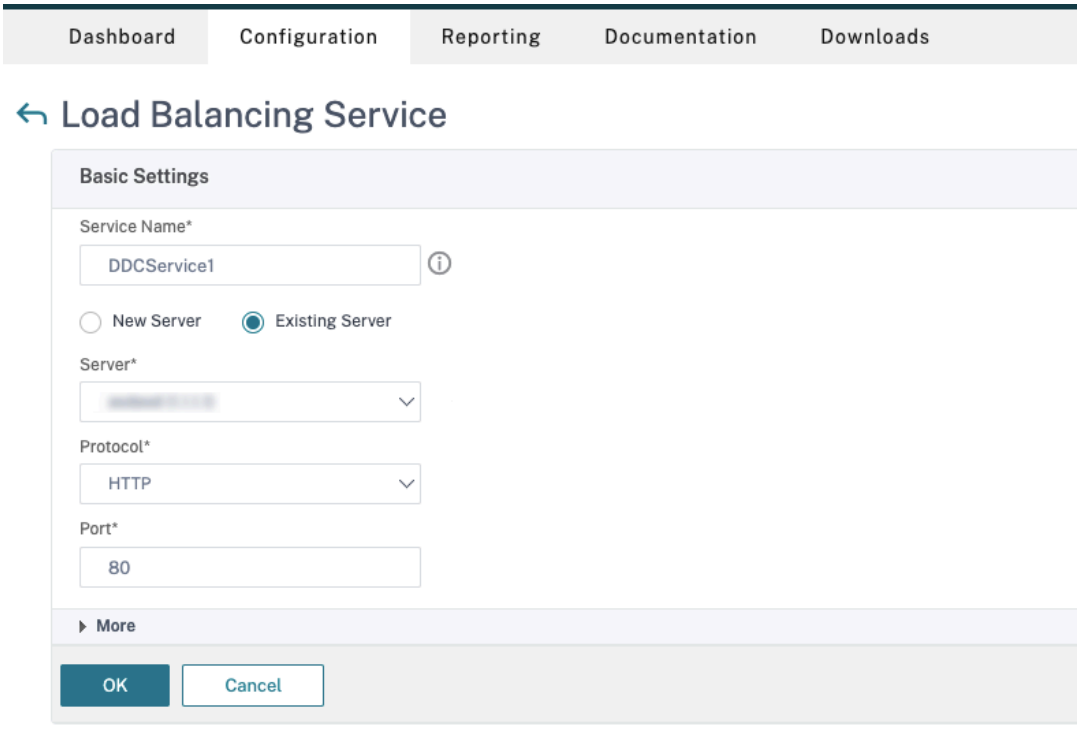
 




- Wählen Sie unter **Protocol** die Option **HTTP**.
- Geben Sie die IP-Adresse des virtuellen Lastausgleichsserver ein und wählen Sie für **Port** die Option **80**.
- Klicken Sie auf **OK**.

b) Erstellen Sie einen Lastausgleichsdienst.

- Gehen Sie zu **Traffic Management > Load Balancing > Services**.

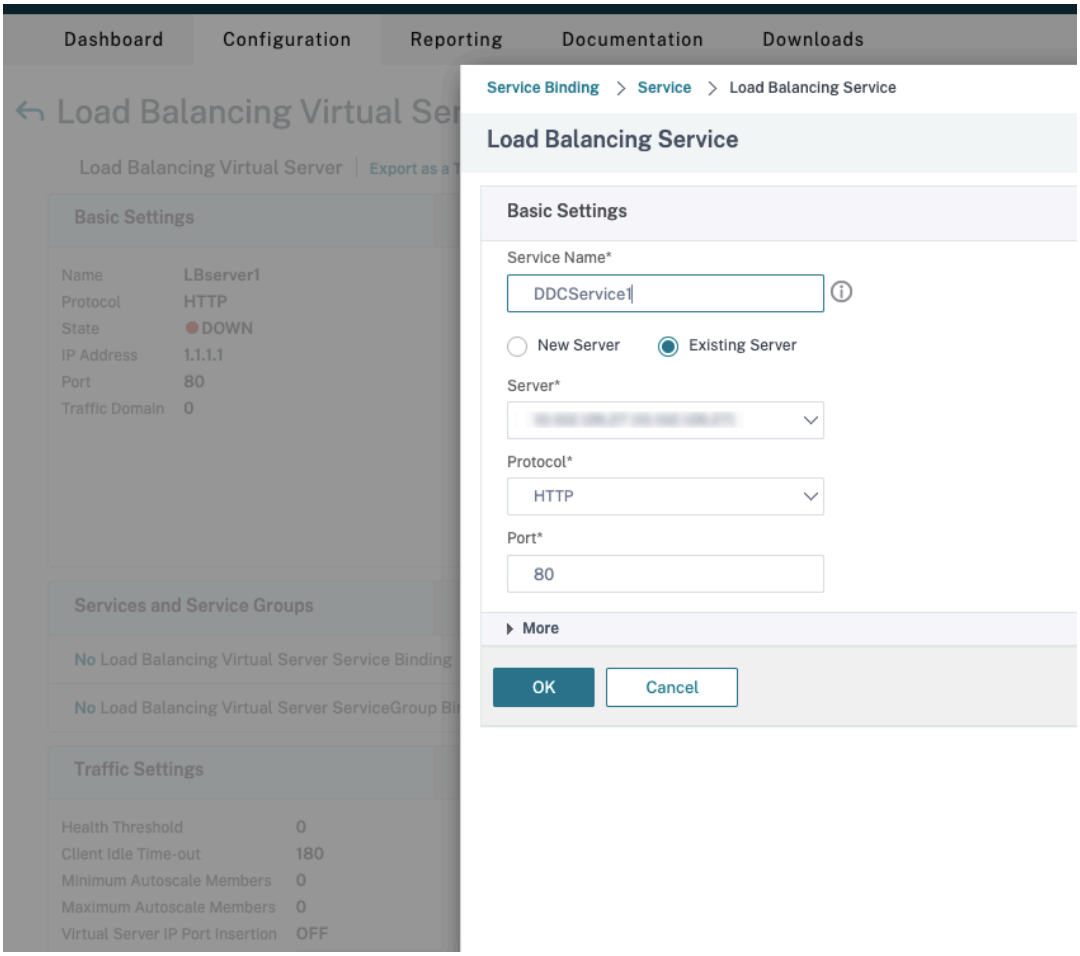


- Wählen Sie unter **Existing Server** den im vorherigen Schritt erstellten virtuellen Server aus.
- Wählen Sie für **Protocol** die Option **HTTP** und für **Port** die Option **80**.
- Klicken Sie auf **OK** und dann auf **Done**.

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**.

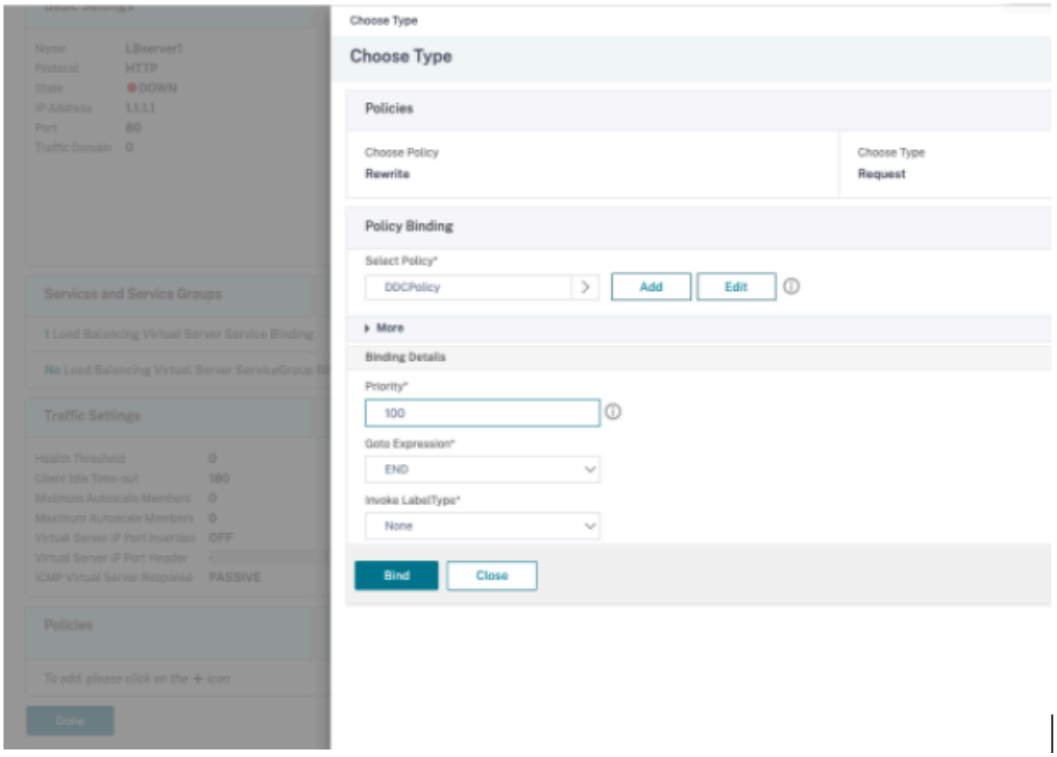



- Wählen Sie unter **Service Binding** den zuvor erstellten Dienst aus.
- Klicken Sie auf **Bind**.

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 **+**.

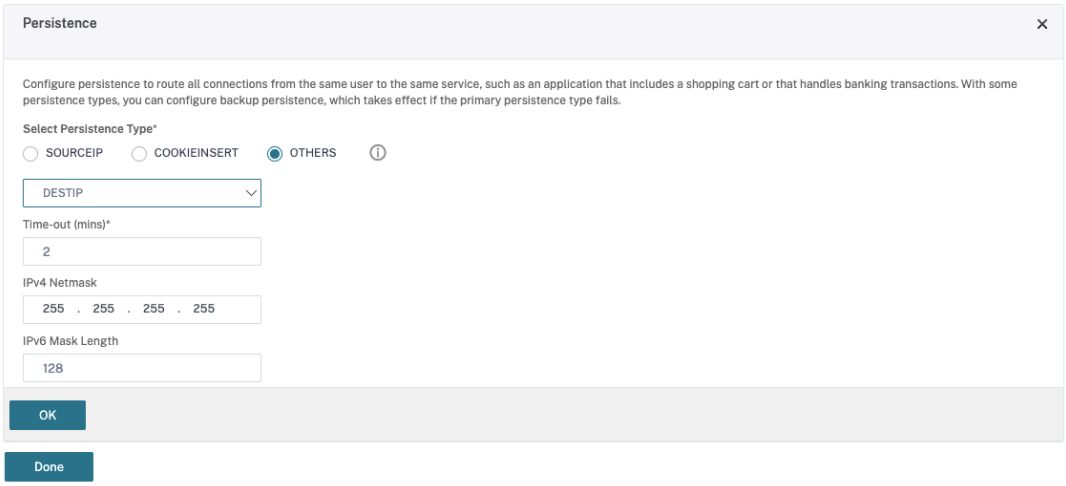
 




- Wählen Sie unter **Choose Policy** die Option **Rewrite** und für **Choose Type**, die Option **Request**.
- Klicken Sie auf **Continue**.
- Wählen Sie unter **Select Policy** die zuvor erstellte Rewrite-Richtlinie aus.
- Klicken Sie auf **Bind**.
- Klicken Sie auf **Fertig**.

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**.

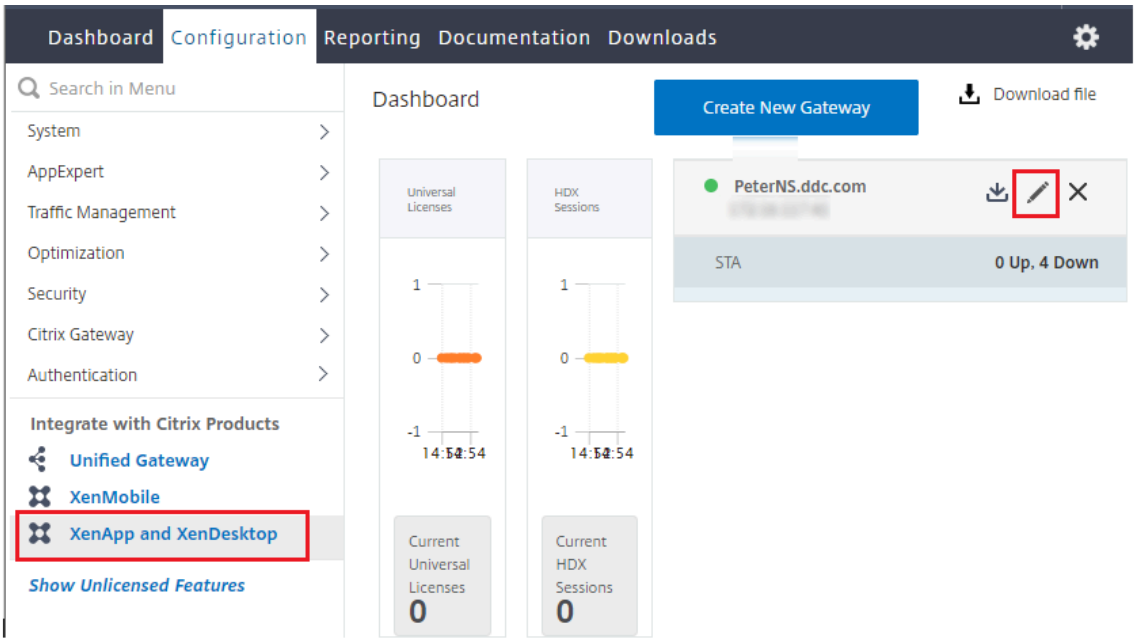
f) Wiederholen Sie diese Schritte für den anderen virtuellen Server.

### 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.

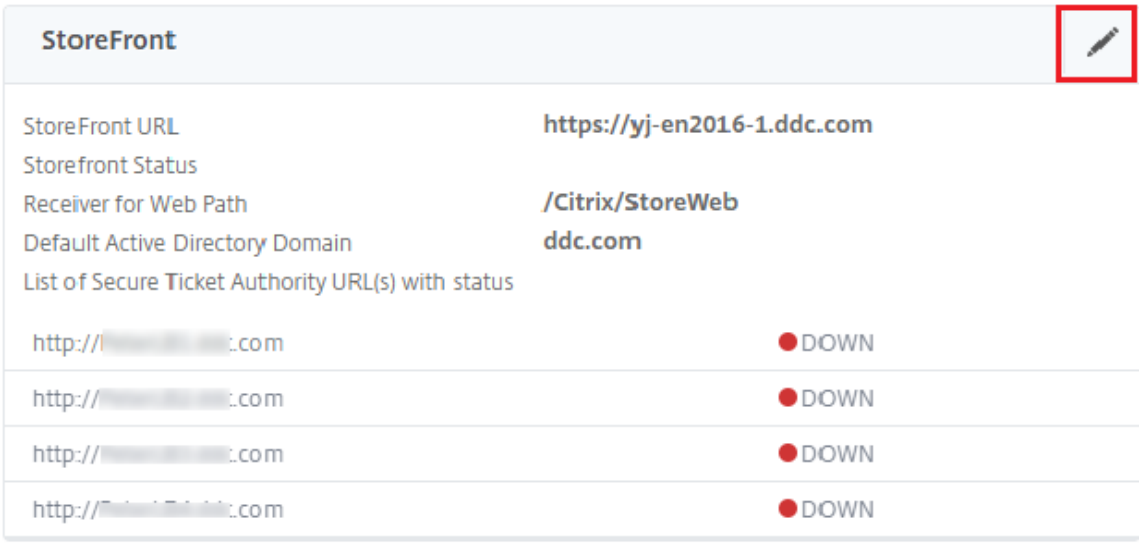
- Ändern Sie vor dem Start der Sitzung die **Secure Ticket Authority-URL** des Gateways, um die FQDNs der virtuellen Lastausgleichsserver zu verwenden.
- Stellen Sie sicher, dass der Parameter `TrustRequestsSentToTheXmlServicePort` auf "False"festgelegt ist. Standardmäßig ist der Parameter `TrustRequestsSentToTheXmlServicePort` 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.

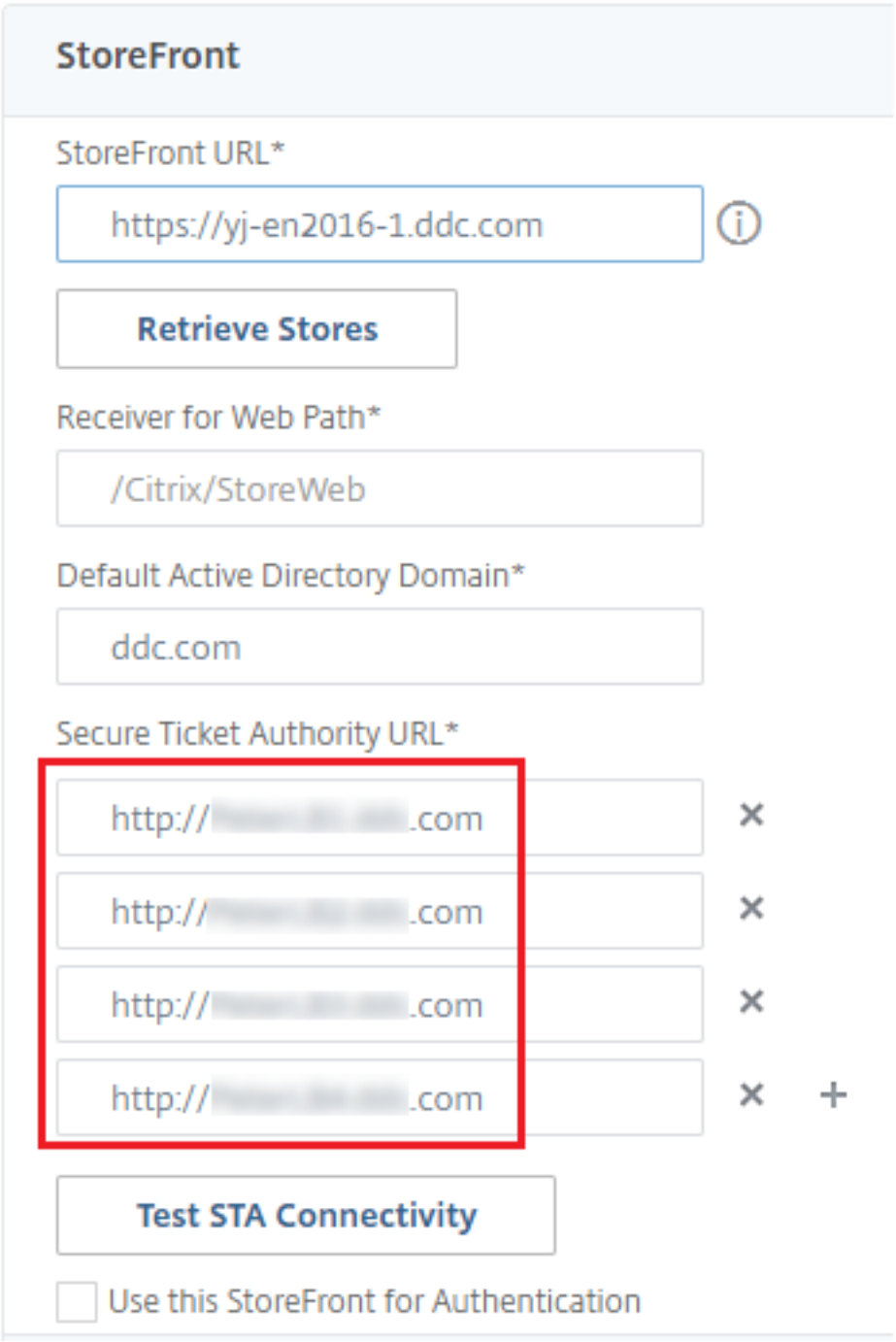
 




4. Fügen Sie die **Secure Ticket Authority-URL**hinzu.

   - 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.




## Resilienzeinstellungen für Sitzungen

June 27, 2024

Aufrechterhalten der Sitzungsaktivität ist wichtig für die beste Benutzererfahrung. Eine Unter-

brechung der Verbindung aufgrund von unzuverlässigen Netzwerken, stark variierender Netzwerklatenz oder Bereichseinschränkungen von drahtlosen Geräten kann zu Frustrationen bei den Benutzern führen. Der schnelle Wechsel von Geräten und Zugriff auf dieselben Anwendungen bei jeder Anmeldung ist wichtig für viele mobile Mitarbeiter, etwa im Gesundheitswesen.

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.

### Sitzungszuverlässigkeit

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.

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). Sie können den Zeitraum vergrößern, den die Sitzungszuverlässigkeit eine Sitzung offen lässt, diese Funktion dient jedoch zum Erhöhen des Bedienungskomforts. Daher wird der Benutzer nicht zur erneuten Authentifizierung aufgefordert. Je länger eine Sitzung offen gelassen wird, desto höher ist das Risiko, dass der Benutzer abgelenkt wird und das Benutzergerät verlässt. Es besteht dann das Risiko, dass unbefugte Benutzer Zugang zu der Sitzung erhalten.
- 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 ohne Neuauthentifizierung nicht 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 diesen Zeitraum zu ändern, bearbeiten Sie die folgende Registrierungseinstellung auf dem Benutzergerät (wobei `seconds` die Zeit in Sekunden angibt, nach der keine weiteren Wiederverbindungsversuche unternommen werden).

```
HKLM\Software\Citrix\ICA Client\TransportReconnectRetryMaxTimeSeconds
; DWORD;<seconds>
```

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 Informationen über Wiederverbindungsereignisse in seinem eigenen Systemprotokoll. Die Site stellt kein kombiniertes Protokoll zu Wiederverbindungsereignissen auf allen Servern zur Verfügung.

> **Hinweis:**
>
> Das automatische Wiederverbinden von Clients ohne erneute Authentifizierung wird nur für die Kennwortauthentifizierung unterstützt. Wenn Sie den Verbundauthentifizierungsdienst oder die Smartcardauthentifizierung verwenden, wird die automatische Wiederverbindung von Clients ohne erneute Authentifizierung nicht unterstützt. In solchen Fällen werden Benutzer zum Anmeldebildschirm weitergeleitet.

Bei der automatischen Wiederverbindung von Clients findet eine Authentifizierung mit verschlüsselten Anmeldeinformationen statt. Wenn sich ein Benutzer erstmals anmeldet, verschlüsselt der Server seine Anmeldeinformationen und speichert sie im Speicher. Der Server erstellt und sendet außerdem 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, startet der Wiederverbindungsversuch eine neue Sitzung. 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 feststellt, verhindert dieses Feature, sofern aktiviert, dass die Sitzung durch die Remotedesktopdienste getrennt wird. Beispiele für fehlende Aktivität sind die Abwesenheit von Mausbewegungen und Bildschirmaktualisierungen. 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 in der Windows-Gruppenrichtlinie 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 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 bei der Sitzung angemeldet ist. Beispielsweise meldet sich ein Mitarbeiter im Gesundheitswesen von einem Gerät in der Notaufnahme ab und meldet sich dann an einer Arbeitsstation im Röntgenlabor an. Die Richtlinien, Druckerzuordnungen und Clientlaufwerkzuordnungen, die für die Sitzung im Röntgenlabor geeignet sind, werden bei Sitzungsstart wirksam.

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

> **Hinweis:**
>
> Die folgende Anleitung zeigt Ihnen, wie Sie das Sitzungsroaming mit PowerShell konfigurieren. Sie können stattdessen Web Studio verwenden. Weitere Informationen finden Sie unter Bereitstellungsgruppen verwalten.

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. Oft 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
```

Für `value` sind folgende Optionen möglich:

- **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.

# Einstellungen

June 27, 2024

> **Hinweis:**
>
> Sie können Ihre Citrix Virtual Apps and Desktops-Bereitstellung mithilfe von zwei Verwaltungskonsolen verwalten: Web Studio (webbasiert) und Citrix Studio (Windows-basiert). Dieser Artikel behandelt nur Web Studio. Informationen zu Citrix Studio finden Sie im entsprechenden Artikel in Citrix Virtual Apps and Desktops 7 2212 oder früher.

Sie können diese Einstellungen in Web Studio verwalten:

- Authentifizierung verwalten
- Citrix Programm zur Verbesserung der Benutzerfreundlichkeit
- Delivery Controller entfernen
- Protokollierungsdatenbank ändern
- Datum und Uhrzeit einstellen
- Site zentral verwalten
- Automatische Zuweisung mehrerer Benutzer für Remote-PC-Zugriff aktivieren
- DNS-Auflösung aktivieren
- XML-Vertrauen aktivieren
- Sicherheitsschlüssel verwalten
- Inaktivitätstimeout für die Studio-Konsole festlegen

## Authentifizierung verwalten

Standardmäßig authentifizieren sich Benutzer mit ihren Domänenanmeldeinformationen (Benutzername und Kennwort) bei Web Studio. Sie können die integrierte Windows-Authentifizierung aktivieren, sodass Benutzer mit ihren Windows-Anmeldeinformationen über Kerberos oder NTLM auf Studio zugreifen können. Das Deaktivieren der Anmeldung mit Domänenanmeldeinformationen wird nicht unterstützt.

> **Wichtig**
>
> Die integrierte Windows-Authentifizierung funktioniert nicht, wenn Web Studio als Proxy für Delivery Controller konfiguriert ist.

Wenn Sie die Option **Integrierte Windows-Authentifizierung** aktiviert haben, werden Ihre Benutzer bei der nächsten Anmeldung automatisch angemeldet. Wenn Sie als Benutzer nicht automatisch angemeldet werden, gehen Sie wie folgt vor, um Ihren Webbrowser für die integrierte Windows-Authentifizierung zu konfigurieren.

Google Chrome:

1. Wählen Sie in der Systemsteuerung "Internetoptionen"aus.
2. Wählen Sie die Registerkarte **Erweitert**.
3. Wählen Sie **Integrierte Windows-Authentifizierung aktivieren**.
4. Klicken Sie auf die Registerkarte **Sicherheit**.
5. Wählen Sie **Lokales Intranet > Websites > Erweitert**.
6. Führen Sie im Feld **Diese Website zur Zone hinzufügen** folgenden Schritt aus:
    - Wenn sich Web Studio und der Delivery Controller auf demselben Server befinden, geben Sie die URL des Hosts ein, auf dem Web Studio ausgeführt wird.
    - Wenn nicht, geben Sie eine Platzhalterdomäne ein. Beispiel: Wenn der Delivery Controller in `ddc.domain.com` ist, geben Sie `*.domain.com` ein.
7. Klicken Sie auf **Hinzufügen > Schließen**.

Mozilla Firefox:

1. Geben Sie `about:config` im Browser-URL-Feld ein.
2. Geben Sie im **Suchfeld** `network negotiate` ein.
3. Klicken Sie mit der rechten Maustaste auf **network.negotiate-auth.trusted-uris** und wählen Sie **Modify**.
4. Führen Sie im Feld **Enter string value** folgenden Schritt aus:
    - Wenn sich Web Studio und der Delivery Controller auf demselben Server befinden, fügen Sie eine durch Kommas getrennte Liste der URLs und/oder Aliasnamen hinzu, die auf den Namen des Servers verweisen, auf dem Web Studio gehostet wird.
    - Wenn nicht, fügen Sie die URLs auf diese Weise hinzu. Beispiel: Wenn der Delivery Controller in `ddc.domain.com` ist, geben Sie `*.domain.com` ein.

Nachdem Sie den Browser konfiguriert haben, können Sie auf der Anmeldeseite auf **Integrierte Windows-Anmeldung** klicken, um es erneut zu versuchen.

Wenn Web Studio und der Delivery Controller auf verschiedenen Maschinen installiert sind, müssen Sie den **ursprungsübergreifenden Zugriff** aktivieren, damit die integrierte Windows-Authentifizierung funktioniert.

Gehen Sie wie folgt vor, um den **ursprungsübergreifenden Zugriff** zu aktivieren:

1. Aktivieren Sie das Kontrollkästchen **Allow cross-origin access**.
2. Fügen Sie die URL des Web Studio-Servers zur Positivliste hinzu.
3. Geben Sie im Feld **Enter URL** die URL ein. Klicken Sie auf **Hinzufügen**, um bei Bedarf weitere hinzuzufügen.

   > **Hinweis**
   >
   > - Die URL muss das richtige Format haben:`<scheme>://<hostname>`. Vergewissern Sie sich, dass sie keine Pfade oder abschließende Schrägstriche enthält.
   > - IP-Adressen und FQDNs werden unterstützt. Stellen Sie beim Hinzufügen einer URL sicher, dass sie der Art und Weise entspricht, wie Sie auf Web Studio zugreifen. Wenn Sie beispielsweise über eine IP-Adresse auf Web Studio zugreifen, fügen Sie die auf der IP-Adresse basierende URL zur Liste hinzu.
   > - Wenn Sie einen nicht standardmäßigen Port verwenden, geben Sie die Portnummer an.

4. Klicken Sie auf **Hinzufügen**, um bei Bedarf weitere hinzuzufügen.
5. Wenn Sie fertig sind, klicken Sie auf **Fertig**, um die Konfiguration zu speichern und zu beenden.

### Zeitzone einrichten

Führen Sie folgende Schritte aus, um das Datums- und Uhrzeitformat an Ihre Präferenzen anzupassen:

1. Melden Sie sich bei Web Studio an und wählen Sie im linken Bereich **Einstellungen**.
2. Suchen Sie die Kachel für **Datum und Uhrzeit** und klicken Sie auf **Bearbeiten**, um die folgenden Optionen zu konfigurieren:

   - **Zeitformat:**
     - Wählen Sie diese Option, um die Uhrzeit im 12-Stunden-Format (z. B. 09:00 PM) oder im 24-Stunden-Format (z. B. 21:00 Uhr) anzuzeigen.
   - **Datumsformat:**
     - Konfigurieren Sie das Datumsformat so, dass es Ihren Präferenzen entspricht, z. B. JJJJ/MM/TT.
   - **Zeitzone:**
     - **UTC:** UTC für die Anzeige von Datum und Uhrzeit in der gesamten Benutzeroberfläche verwenden. Beim Zeigen mit der Maus auf Datum und Uhrzeit werden diese Informationen in der lokalen Zeitzone angezeigt.

- **Lokale Zeitzone:** Lokale Zeitzone für Datum und Uhrzeit in der gesamten Benutzeroberfläche verwenden. Beim Zeigen mit der Maus auf Datum und Uhrzeit werden diese Informationen in UTC angezeigt.

> **Hinweis:**
>
> Diese Einstellungen sind für jedes Benutzerkonto spezifisch.

### DNS-Auflösung aktivieren

Führen Sie folgende Schritte aus, um in der ICA-Datei keine IP-Adressen, sondern DNS-Namen anzuzeigen:

1. Melden Sie sich bei Web Studio an und wählen Sie im linken Bereich **Einstellungen**.
2. Aktivieren Sie die Einstellung **DNS-Auflösung aktivieren**.

### Inaktivitätstimeout für die Studio-Konsole festlegen

Sie können die Dauer der Inaktivität festlegen, nach der Administratoren automatisch von der Studio-Konsole abgemeldet werden.

1. Melden Sie sich bei Web Studio an und wählen Sie im linken Bereich **Einstellungen**.
2. Geben Sie eine Dauer zwischen 10 Minuten und 24 Stunden ein.
3. Um die Einstellung anzuwenden, aktualisieren Sie die Seite oder melden Sie sich ab und wieder an.

### Site zentral verwalten

Mit dieser Funktion können Sie mit einer Web Studio-Konsole mehrere Citrix Virtual Apps and Desktops-Sites verwalten. Weitere Informationen finden Sie unter Verwalten mehrerer Sites aktivieren.

## Tags

June 27, 2024

> **Hinweis:**
>
> Sie können Ihre Citrix Virtual Apps and Desktops-Bereitstellung mithilfe von zwei Verwaltungskonsolen verwalten: Web Studio (webbasiert) und Citrix Studio (Windows-basiert). Dieser

> Artikel behandelt nur Web Studio. Informationen zu Citrix Studio finden Sie im entsprechenden Artikel in Citrix Virtual Apps and Desktops 7 2212 oder früher.

## 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 Web 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 Web 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 eine Teilmenge von Maschinen in Bereitstellungsgruppen, Bereitstellungsgruppentypen oder Organisationseinheiten, die ein bestimmtes Tag haben oder nicht haben

  Wenn Sie beispielsweise eine Citrix Richtlinie nur auf leistungsstarke Arbeitsstationen anwenden möchten, fügen Sie diesen Maschinen ein Tag mit dem Namen "Hohe Leistung"

hinzu. Wählen Sie dann auf der Seite **Richtlinie zuweisen** des Assistenten zum Erstellen von Richtlinien dieses Tag und das Kontrollkästchen **Aktivieren**. Sie können auch einer Bereitstellungsgruppe ein Tag hinzufügen und eine Citrix Richtlinie auf die Gruppe anwenden. 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 Web Studio konfigurieren:

- Desktops in einer freigegebenen Bereitstellungsgruppe
- Anwendungsgruppen

## Tagbeschränkungen für Desktops oder Anwendungsgruppen

Das Erstellen von Tagbeschränkungen umfasst mehrere Schritte:

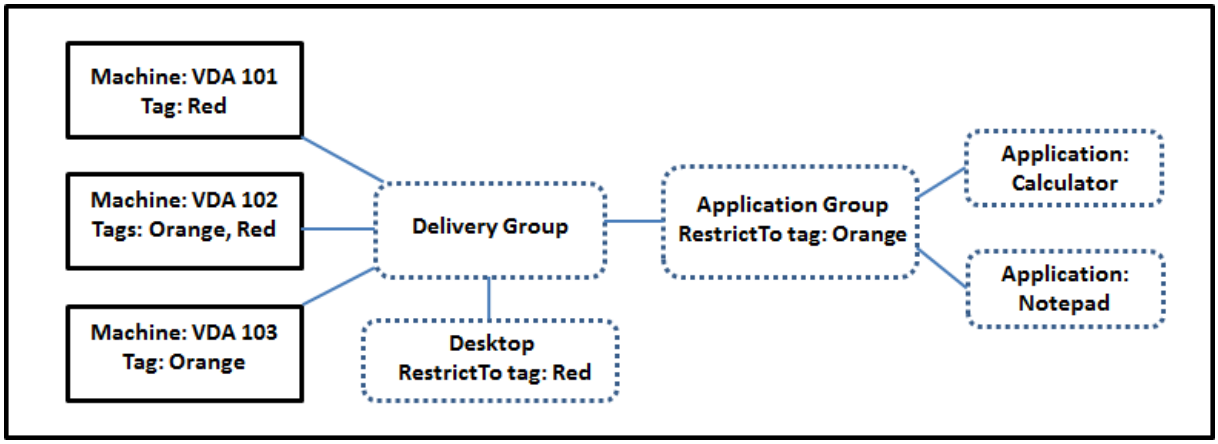
- Erstellen Sie das Tag und fügen Sie es Maschinen hinzu.
- Erstellen oder bearbeiten Sie eine Gruppe mit der Tagbeschränkung (d. h. beschränken Sie Starts auf Maschinen mit Tag "x").

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 freigegebenen Bereitstellungsgruppe wurde mit der Tagbeschränkung "Red" erstellt. Ein Desktop kann nur auf Maschinen in dieser Bereitstellungsgruppe mit dem Tag "Red" (VDA 101 und 102) gestartet werden.
- 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.

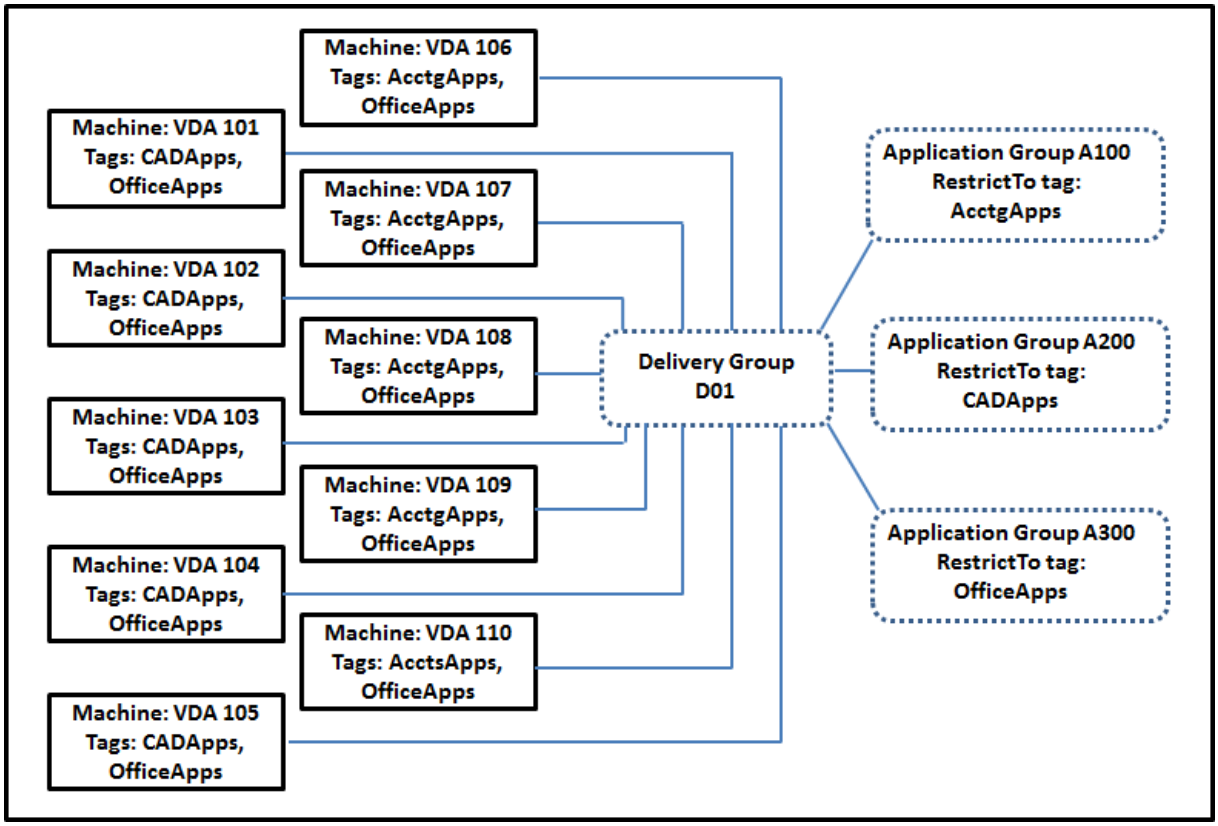
Maschine VDA 102 hat beide Tags (Rot und Orange) und kann daher für das Starten von Anwendungen und Desktops verwendet werden.

#### 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, Hinzufügen (Anwenden), Bearbeiten und Löschen von Tags für ausgewählte Elemente wird die Aktion **Tags verwalten** in Web Studio verwendet.

(Ausnahme: Tags für Richtlinienzuweisungen werden über die Aktion **Tags verwalten** in Web Studio erstellt, bearbeitet und gelöscht. Die Tags werden jedoch beim Erstellen der Richtlinie angewendet (zugewiesen). Weitere Informationen finden Sie unter Erstellen von Richtlinien.)

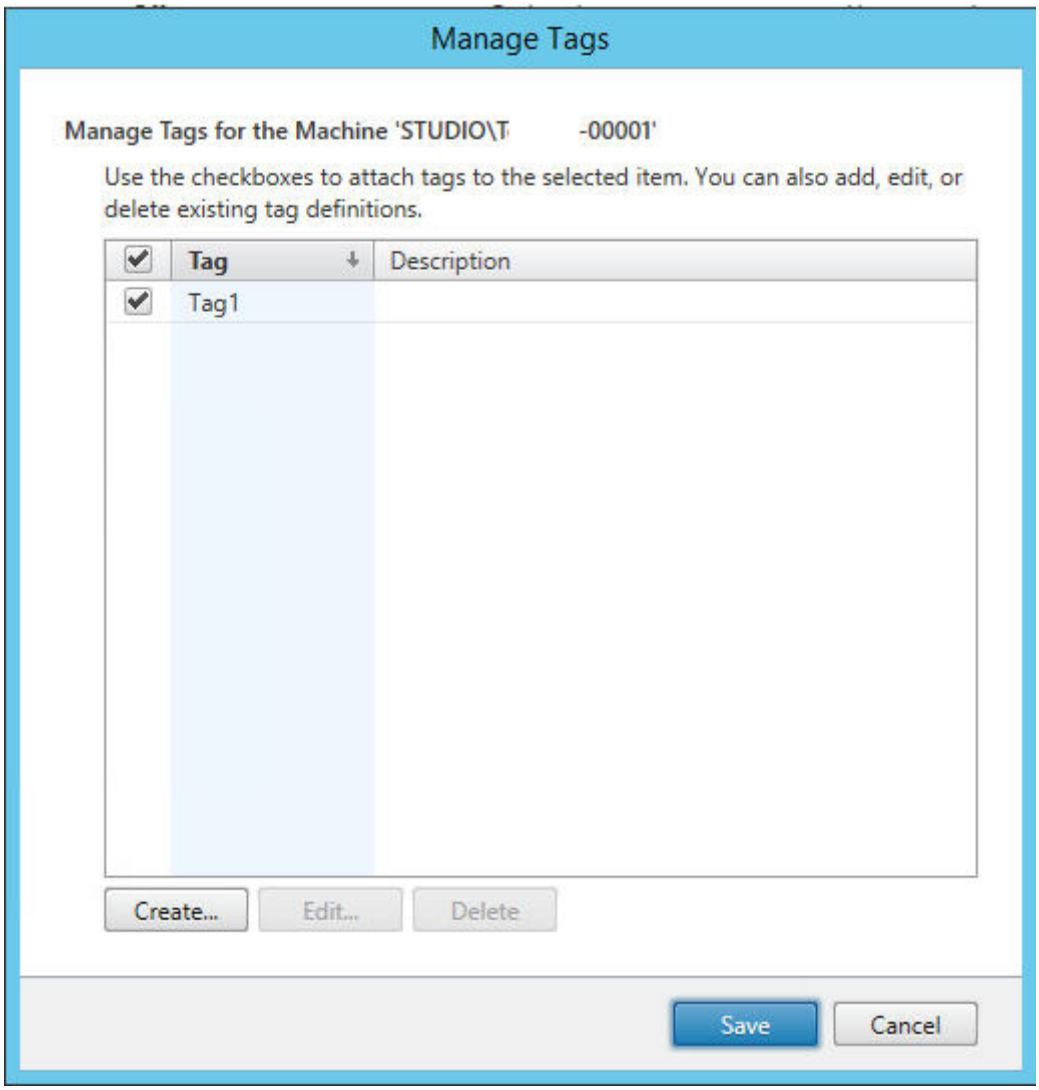
Tagbeschränkungen konfigurieren Sie beim Erstellen oder Bearbeiten von Desktops in Bereitstellungsgruppen und beim Erstellen und Bearbeiten von Anwendungsgruppen.

#### Dialogfelder “Tags verwalten”in Web Studio verwenden

Wählen Sie in Web Studio die Elemente aus, auf die Sie ein Tag anwenden möchten (eine oder mehrere Maschinen oder Anwendungen, einen Desktop, eine Bereitstellungsgruppe oder eine Anwendungsgruppe), und wählen Sie dann in der Aktionsleiste **Tags verwalten**. Das Dialogfeld enthält alle in der Site erstellten Tags und nicht nur diejenigen, die für die ausgewählten Elemente erstellt wurden.

- Ein Kontrollkästchen mit Häkchen kennzeichnet Tags, die den ausgewählten Elementen bereits hinzugefügt wurden. (In der Abbildung unten hat die ausgewählte Maschine das Tag “Tag1”.)
- Wenn Sie mehrere Elemente auswählen, wird durch ein Kontrollkästchen mit einem Strich angezeigt, wenn das Tag einigen (aber nicht allen) Elementen hinzugefügt wurde.




Die folgenden Aktionen stehen im Dialogfeld **Tags verwalten** zur Verfügung. Lesen Sie in diesem Zusammenhang unbedingt den Abschnitt Hinweise zum Arbeiten mit Tags.

- **Tags erstellen:**

  Klicken Sie auf **Erstellen**. Geben Sie einen Namen und eine Beschreibung ein. Tagnamen müssen eindeutig sein, die Groß- und Kleinschreibung spielt keine Rolle. Klicken Sie dann auf **OK**. (Durch das Erstellen eines Tags wird es nicht automatisch auf Elemente angewendet, die Sie ausgewählt haben. Verwenden Sie zum Anwenden die Kontrollkästchen.)

- **Hinzufügen von Tags:**

  Aktivieren Sie die Kontrollkästchen neben den Tagnamen. Wenn Sie mehrere Elemente ausgewählt haben, das Kontrollkästchen neben einem Tag einen Strich enthält (d. h. das Tag wurde bereits auf einige, jedoch nicht alle ausgewählten Elemente angewendet) und Sie das Kontrollkästchen mit einem Häkchen versehen, wirkt sich dies auf alle ausgewählten Maschinen aus.

Wenn Sie versuchen, ein als Einschränkung in einer Anwendungsgruppe verwendetes Tag einer oder mehreren Maschinen hinzuzufügen, werden Sie gewarnt, dass die Aktion dazu führen kann, dass die Maschinen für Starts verfügbar gemacht werden. Wenn dies beabsichtigt ist, fahren Sie fort.

- **Entfernen von Tags:**

  Deaktivieren Sie die Kontrollkästchen neben den entsprechenden Tagnamen. Wenn Sie mehrere Elemente ausgewählt haben, das Kontrollkästchen neben einem Tag einen Strich enthält (d. h. das Tag wurde bereits auf einige, jedoch nicht alle ausgewählten Elemente angewendet), und Sie das Kontrollkästchen deaktivieren, wird das Tag von allen ausgewählten Maschinen entfernt.

  Wenn Sie versuchen, ein Tag von einer Maschine zu entfernen, für die es als Einschränkung verwendet wird, werden Sie 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 Web 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 linken Bereich **Bereitstellungsgruppen**. Wählen Sie im mittleren Bereich eine Bereitstellungsgruppe und dann in der Aktionsleiste **Maschinen anzeigen**. Wählen Sie im mittleren Bereich eine Maschine und dann im Bereich **Details** die Registerkarte **Tags**.

#### Tagbeschränkungen verwalten

Das Verfahren zum Konfigurieren von Tagbeschränkungen besteht aus mehreren Schritten. Zunächst erstellen das Tag und wenden es auf Maschinen an. Anschließend fügen Sie der Anwendungsgruppe oder dem Desktop die Einschränkung hinzu.

- **Tag erstellen und anwenden:**

  Erstellen Sie mithilfe des Dialogfelds **Tags verwalten** das Tag und wenden Sie es dann auf die Maschinen an, für die die Beschränkung gelten soll (siehe weiter oben).

- **Tagbeschränkung einer Anwendungsgruppe hinzufügen:**

  Erstellen oder bearbeiten Sie die Anwendungsgruppe. Wählen Sie auf der Seite **Bereitstellungsgruppen** 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 vollständig durch Deaktivieren der Option **Starts auf Maschinen mit Tag beschränken**.

- **Tagbeschränkung einem Desktop hinzufügen:**

  Erstellen oder bearbeiten Sie eine Bereitstellungsgruppe. Klicken Sie auf der Seite **Desktops** auf **Hinzufügen** oder **Bearbeiten**. Wählen Sie 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 den Listen oder entfernen Sie die Tagbeschränkung vollständig 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 Web Studio-Suchfeld zu sortieren. Sie können dasselbe Tag beim Konfigurieren einer Anwendungsgruppe oder eines Desktops als Einschränkung verwenden. Das Tag beschränkt die Startauswahl auf Maschinen in den Bereitstellungsgruppen, die das Tag haben.

Wenn Sie versuchen, Maschinen ein Tag hinzuzufügen, nachdem dieses als Tagbeschränkung für eine Desktop- oder Anwendungsgruppe konfiguriert wurde, wird 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, können Sie den Vorgang abbrechen.

Angenommen, Sie erstellen eine Anwendungsgruppe mit der Tagbeschränkung "Rot". Später fügen Sie der von der Anwendungsgruppe verwendeten Bereitstellungsgruppe mehrere Maschinen hinzu.

Wenn Sie versuchen, das Tag "Rot"den Maschinen hinzuzufügen, zeigt Web 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 Web 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 Web Studio die Bereitstellungsgruppe D01 und in der Aktionsleiste **Maschinen anzeigen**.
2. Wählen Sie die Maschinen VDA 101–105 und dann in der Aktionsleiste **Tags verwalten**.
3. Klicken Sie im Dialogfeld "Tags verwalten"auf **Erstellen** und erstellen Sie ein Tag mit dem Namen `CADApps`. Klicken Sie auf **OK**.
4. Klicken Sie erneut auf **Erstellen** und erstellen Sie ein Tag namens "OfficeApps". Klicken Sie auf **OK**.
5. Fügen Sie im Dialogfeld **Tags verwalten** die neu erstellten Tags den ausgewählten Maschinen hinzu, indem Sie die Kontrollkästchen neben den Tagnamen (`CADApps` und `OfficeApps`) aktivieren. Wenn Sie fertig sind, schließen Sie das Dialogfeld.
6. Wählen Sie die Bereitstellungsgruppe "D01"und dann in der Aktionsleiste **Maschinen anzeigen**.
7. Wählen Sie die Maschinen VDA 106–110 und dann in der Aktionsleiste **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, und schließen Sie das Dialogfeld.

Anwendungsgruppen mit Tagbeschränkungen erstellen

1. Wählen Sie in Web Studio im linken Bereich **Anwendungen**, wählen Sie dann die Registerkarte **Anwendungsgruppen** und zum Schluss in der Aktionsleiste die Option **Anwendungsgruppe erstellen**. Der Assistent zum Erstellen einer Anwendungsgruppe wird angezeigt.
2. Wählen Sie auf der Seite **Bereitstellungsgruppen** des Assistenten die Bereitstellungsgruppe "D01". Wählen Sie **Starts auf Maschinen mit Tag beschränken** und wählen Sie dann das Tag `AcctgApps` aus der 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 Web Studio können Sie Tags nicht auf einen Katalog anwenden oder daraus entfernen. Die Kataloganzeigen in Web Studio lassen nicht erkennen, ob ein Tag angewendet wurde.

Zusammenfassung: Sie können Web 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 Web Studio oder PowerShell erstellt.)

Weitere Anleitungen und Informationen zur Syntax finden Sie in der Hilfe zu PowerShell-Cmdlets.

### Automatische Tags (Preview)

Mit Auto-Tagging können Administratoren für verschiedene Citrix Virtual Apps and Desktops-Objekte automatische Tags benutzerdefiniert festlegen und entfernen. Dadurch entfällt die Notwendigkeit, periodisch verschiedene Skripts zur Umgebungsoptimierung auszuführen und zu verwalten.

### Anwendungsfälle

Mit Auto-Tagging können Sie Regeln implementieren, die Ihren Geschäftsfaktoren entsprechen: z. B. Kostensenkung, Optimierung der Infrastruktur oder Verbrauchssteigerung. Im Folgenden sind einige der Anwendungsfälle aufgeführt:

- **Ungenutzte VDIs zurückfordern**: Freigabe dedizierter Workloads, die länger als eine vorkonfigurierte Anzahl von Tagen nicht genutzt wurden.
- **Übersichtlichere App-Anzeige**: Identifizieren von Anwendungen, die länger als eine vorkonfigurierte Anzahl von Tagen nicht verwendet wurden.
- **Bereitstellungsgruppen mit weniger als Funktionsebene X**: Anzeige von Bereitstellungsgruppen, die unter einer bestimmten Funktionsebene liegen.
- **Inaktive Benutzer**. Rückforderung der Ressourcen von Benutzern, die länger als eine vorkonfigurierte Anzahl von Tagen nicht angemeldet waren.

### PowerShell-Befehle

Sie können automatische Tags mithilfe von PowerShell-Befehlen erstellen. Nachdem eine Autotag-Regel erstellt wurde, wird sie alle 600 Sekunden ausgewertet. Weitere Informationen finden Sie unter New-BrokerAutoTagRule.

**Beispiele** `New-BrokerAutoTagRule` verwendet denselben Objekttyp und dieselben Filterparameter wie das Cmdlet `Get-BrokerMachine`. Weitere Informationen finden Sie unter GetBrokerMachine.

1. Taggen Sie dedizierte VDIs, die länger als 30 Tage nicht verwendet wurden, mit der ID 123:

    a) Definieren Sie ein Tag zum Kennzeichnen ungenutzter VDIs, zum Beispiel **Unused-VDI**.

    - Tagname: Unused-VDI
    - Tag-ID : 123

    b) Erstellen Sie die Autotag-Regel zum Kennzeichnen ungenutzter Maschinen. Definieren Sie die Regelparameter:

    - Name: Allgemeiner Name für die Regel.
    - Objekttyp: Maschine.
    - Regeltext: Statische, zugewiesene Maschinen, deren letzte Verbindungszeit länger als 30 Tage zurückliegt, oder keine Wertangabe.
    - Tag-UID: Die Tag-ID, die Sie zuordnen möchten: 123.

```
New-BrokerAutoTagRule -Name 'UnusedVdi' -ObjectType 'Machine'
 -RuleText "-AllocationType Static -IsAssigned $true -Filter
 { SummaryState -ne `"InUse`" -and ( LastConnectionTime -lt
'-30' -or LastConnectionTime -eq `$null )} " -TagUid 123<!--
NeedCopy-->
```

c) Überprüfen Sie die mit dem Tag **Unused-VDI** markierten Maschinen und geben Sie sie frei.

2. Kennzeichnen von Bereitstellungsgruppen, die unter Funktionsebene X liegen (mit **L7_20** als Schwellenwert für Funktionsebene):

```
New-BrokerAutoTagRule -Name 'LowFL'-ObjectType 'DesktopGroup'-RuleText
 "-Filter { MinimumFunctionalLevel -lt 'L7_20' } "-TagUid 123
```

1. Kennzeichnen von für Benutzer sichtbare Apps, die ohne Ordner veröffentlicht wurden:

```
New-BrokerAutoTagRule -Name 'NoFolder'-ObjectType 'Application'-
RuleText "-Enabled $true -Filter { ClientFolder -eq $null )} "-TagUid
 123
```

#### Weitere Informationen

Blogbeitrag: How to assign desktops to specific servers.

## Benutzerprofile

June 27, 2024

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.

### 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 folgenden Tabelle 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 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. Sie werden als permanent eingestuft.

Zusammen definieren diese beiden Faktoren die folgenden Maschinentypen:

- **Persistent und dediziert**. Beispiele sind Maschinen mit Einzelsitzungs-OS mit statischen Zuweisungen und persistentem lokalen Speicher, die mit den Maschinenerstellungsdiensten erstellt wurden, physische Arbeitsstationen und Laptops
- **Persistent und freigegeben**. Beispiele sind Maschinen mit Multisitzungs-OS, die mit den Maschinenerstellungsdiensten erstellt wurden, und Citrix Virtual Apps-Server
- **Provisioning und dediziert**. Beispiele sind Maschinen mit Einzelsitzungs-OS mit statischer Zuweisung, aber ohne persistenten Speicher, die mit Citrix Provisioning Service (in Citrix Virtual Desktops) erstellt wurden.
- **Provisioning and freigegeben**. Beispiele sind Maschinen mit Einzelsitzungs-OS mit einer zufälligen Zuweisung, die mit Citrix Provisioning Service (in Citrix Virtual Desktops) und Citrix Virtual Apps-Servern 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 Abmeldung löschen | Deaktiviert | Aktiviert |
| Profilstreaming | Deaktiviert | Aktiviert |
| Immer zwischenspeichern | Aktiviert (Hinweis 1) | Deaktiviert (Hinweis 2) |
| Aktiv zurückschreiben | Deaktiviert | Deaktiviert (Hinweis 3) |
| Anmeldungen lokaler Administratoren verarbeiten | Aktiviert | Deaktiviert (Hinweis 4) |

**Bereitgestellte Maschinen**

| Richtlinie | Bereitgestellt und dediziert | Bereitgestellt and freigegeben |
|---|---|---|
| Lokal zwischengespeicherte Profile nach Abmeldung löschen | Deaktiviert (Hinweis 5) | Aktiviert |
| Profilstreaming | Aktiviert | Aktiviert |
| Immer zwischenspeichern | Deaktiviert (Hinweis 6) | Deaktiviert |
| Aktiv 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**. Mit dieser Einstellung 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. Die Ordnerumleitung 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 Betriebssystem verwendet werden. Um sicherzustellen, dass die Benutzererfahrung für alle Betriebssysteme konsistent ist, benötigen Sie für jedes Betriebssystem eine andere Konfiguration, also eine 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. Durch diese Vorgehensweise 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. Eine falsch angewendete Ordnerumleitung kann zu unvorhersehbarem Verhalten führen.

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 10-Desktops ausgeführt werden, und Anwendungen, einschließlich andere Versionen von Outlook und Internet Explorer, die von Windows Server 2019 bereitgestellt werden. Sie haben 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 verschiedenen 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 10? | Umleitung in Windows Server 2019? |
|---|---|---|
| Eigene Dateien | Ja | Ja |
| Anwendungsdaten | Nein | Nein |
| Kontakte | Ja | Ja |
| Desktop | Ja | Nein |
| Downloads | Nein | Nein |
| Favoriten | Ja | Ja |
| Verknüpfungen | Ja | Nein |
| Eigene Musik | Ja | Ja |
| Eigene Bilder | Ja | Ja |
| Eigene Videos | Ja | Ja |

| Ordner | Umleitung in Windows 10? | Umleitung in Windows Server 2019? |
|---|---|---|
| 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 10-Bereitstellungsgruppe um. Windows 10 wird häufiger von Benutzern in ihrer täglichen Arbeit verwendet. Benutzer greifen nur gelegentlich auf die vom Windows Server bereitgestellten Anwendungen zu. 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 10-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 über die Ordnerumleitung finden Sie unter Überblick über die Ordnerumleitung, Offlinedateien und Roamingbenutzerprofile.

### 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 Ausschlussfunktionen arbeiten zusammen. Wenn Sie 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.

## VDA-Registrierung

June 27, 2024

### Einführung

> **Hinweis:**
>
> In einer On-Premises-Umgebung registrieren sich VDAs bei einem Delivery Controller. In einer Citrix Cloud-Umgebung registrieren sich VDAs bei einem Cloud Connector. In einer Hybridumgebung registrieren sich einige VDAs bei einem Delivery Controller und andere bei einem Cloud Connector.

VDAs können erst verwendet werden, wenn sie bei mindestens einem Controller oder einem Cloud Connector der Site registriert wurden (Herstellen der Kommunikation). Zur Suche eines Controllers bzw. Connectors überprüft der VDA die 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 bzw. Cloud Connectors zur Site hinzufügen und entfernen und ein VDA keine präzisen und aktuellen Controller-/Connectorinformationen hat, kann er Sitzungsstarts ablehnen, die von einem nicht aufgelisteten Controller bzw. Cloud Connector vermittelt werden. 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 bzw. Cloud Connector 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.

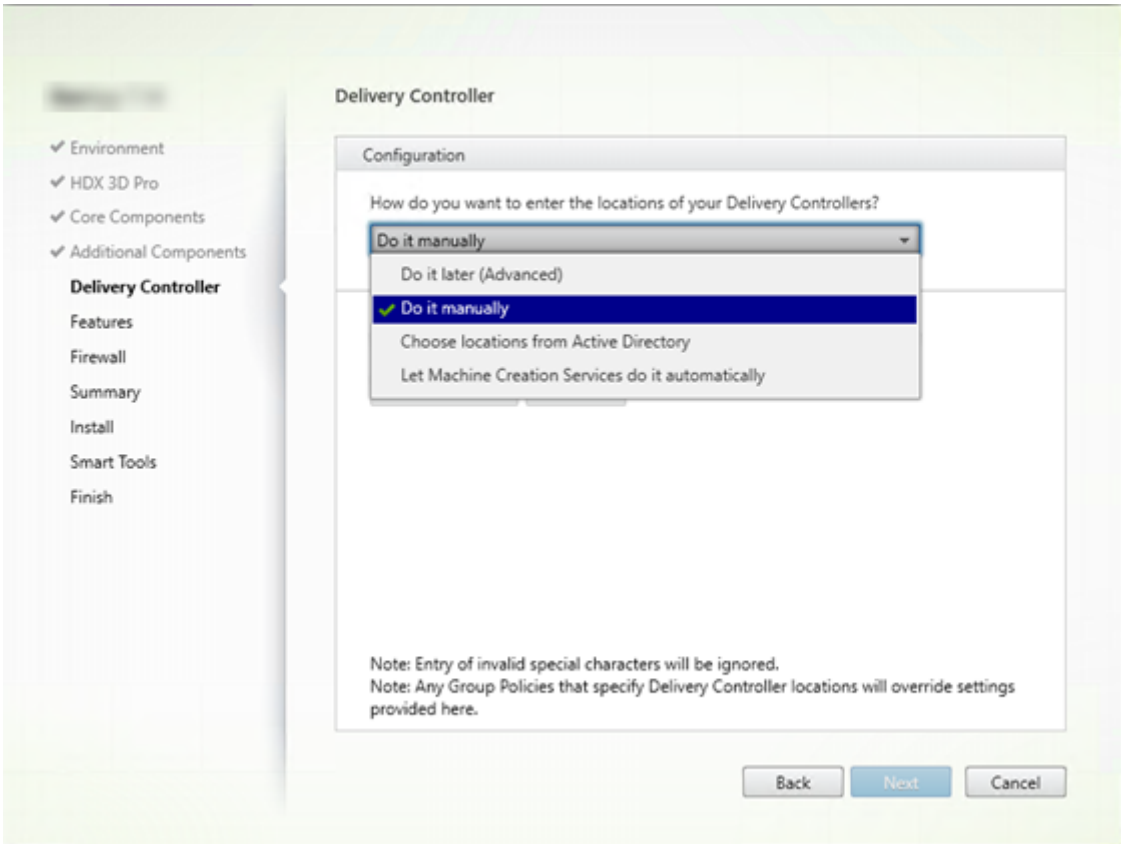
Es gibt verschiedene Methoden zum Konfigurieren von Controller-/Cloud Connector-Adressen auf einem VDA.

- Über Richtlinien (LGPO oder GPO)
- Über die Registrierung (Gruppenrichtlinieneinstellungen (GPP), 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 "/controller"und geben Sie die FQDNs der installierten Controller bzw. Cloud Connectors an.

Diese Informationen werden 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 dies Vorrang vor den bei der VDA-Installation angegebenen Konfigurationseinstellungen, da es eine höhere Methodenpriorität hat.

#### Konfiguration über Active Directory-Organisationseinheit

Diese Methode wird hauptsächlich zum Zweck der Abwärtskompatibilität unterstützt und wird nicht empfohlen. Wenn Sie sie noch immer verwenden, empfiehlt Citrix den Wechsel zu einer anderen Methode.

Zum Angeben dieser Methode führen Sie die folgenden Schritte aus:

- Wählen Sie auf der Seite **Delivery Controller** des VDA-Installationsassistenten **Standorte aus Active Directory auswählen**.
- Verwenden Sie das Skript `Set-ADControllerDiscovery.ps1` (steht auf jedem Controller zur Verfügung). Konfigurieren Sie außerdem den Registrierungseintrag `FarmGuid` auf jedem VDA mit der korrekten Organisationseinheit. Diese Einstellung kann mit der Gruppenrichtlinie konfiguriert werden.

#### 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 oder Kommata 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)
<!--NeedCopy-->
```

- 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 Liste `ListofDDCs` herunter und speichert sie in einem persistenten Cache auf dem VDA. Dieser Schritt wird für jeden VDA durchgeführt. Im 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. Ein serverseitiger Cache ist jedoch kein übliches Verfahren, da es keinen persistenten Cache zur Speicherung automatischer Aktualisierungen gibt.

Gehen Sie zum Angeben dieser Methode folgendermaßen vor:

- Aktivieren oder deaktivieren Sie die automatische Aktualisierung über eine Citrix Richtlinie, die die Einstellung `Virtual Delivery Agent Settings > Enable auto update of Controllers` enthält. Diese Einstellung ist standardmäßig aktiviert.

Funktionsweise:

- Bei jeder erneuten Registrierung eines VDAs (z. B. nach einem Neustart der Maschine) wird der Cache aktualisiert. Außerdem überprüft jeder Controller bzw. Cloud Connector alle 90 Minuten

die Sitedatenbank. Wenn seit der letzten Überprüfung ein Controller bzw. Cloud Connector hinzugefügt oder entfernt wurde oder bei einer Änderung der Richtlinie, die sich auf die VDA-Registrierung auswirkt, sendet der Controller bzw. Cloud Connector eine aktualisierte Liste an die bei ihm registrierten VDAS und der Cache wird aktualisiert. Der VDA nimmt alle Verbindungen von allen Controllern bzw. Cloud Connectors in der aktuellen Liste im Cache an.

- Geht eine Liste ein, die den Controller bzw. Cloud Connector, bei dem der VDA registriert ist, nicht enthält (d. h. der Controller/Cloud Connector wurde aus der Site entfernt), nimmt der VDA eine neue Registrierung bei einem der Controller bzw. Cloud Connectors aus der Liste `ListofDDCs` vor.

Beispiel:

- Die Bereitstellung hat die drei Controller A, B und C. Ein VDA wird bei Controller B registriert (dies wurde bei der Installation des VDAs festgelegt).
- Anschließend werden der Site zwei Controller (D und E) hinzugefügt. Innerhalb von 90 Minuten erhalten die VDAs aktualisierte Listen und akzeptieren Verbindungen von den Controllern A, B, C, D und E. Die Lastverteilung auf alle Controller erfolgt erst nach einem Neustart der VDAs.
- Controller B wird später in eine andere Site verschoben. Innerhalb von 90 Minuten erhalten die VDAs der ursprünglichen Site aktualisierte Listen, da seit der letzten Überprüfung eine Controlleränderung stattfand. Der ursprünglich bei (dem nun nicht mehr vorhandenen) Controller B registrierte VDA wird bei einem der anderen Controller der Liste (A, C, D oder E) registriert.

In einer Bereitstellung mit mehreren Zonen speichert die automatische Aktualisierung in einer Satellitenzone automatisch zuerst alle lokalen Controller. Alle Controller in der primären Zone werden in einer 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.


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. Dieser Prozess kann hilfreich sein, wenn Sie einen VDA in eine andere Site verschieben (zum Beispiel bei einer Notfallwiederherstellung).

### Überlegungen zur Konfiguration

Hier wird eine gebräuchliche VDA-Registrierungskonfiguration vorgestellt.

Dies ist ein eingebettetes Video. Klicken Sie auf den Link, um das Video anzusehen

Das folgende Video zeigt die Schritte zur VDA-Registrierung.

Dies ist ein eingebettetes Video. Klicken Sie auf den Link, um das Video anzusehen

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/Cloud Connector und Controller/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 bestimmten Szenarien 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 zusätzlichen Schritt ausführen. Sie müssen die Richtlinie **Automatische Aktualisierung von Controllern** in Studio auf **Nicht zulassen** festlegen.

### ListOfSIDs

`ListofDDCs` ist die Liste der Controller, die ein VDA zur Registrierung ansprechen kann. Ein VDA muss außerdem "wissen", welche Controller vertrauenswürdig sind. VDAS vertrauen nicht automatisch den Controllern in der Liste `ListofDDCs`. Die Liste der Sicherheits-IDs (`ListofSIDs`) enthält die vertrauenswürdigen Controller. VDAs versuchen eine Registrierung nur mit vertrauenswürdigen Controllern.

In den meisten Umgebungen wird die Liste `ListofSIDs` automatisch aus der Liste `ListofDDCs` generiert. Sie können die Liste `ListofSIDs` mit einer CDF-Ablaufverfolgung lesen.

Im Allgemeinen besteht keine Notwendigkeit einer manuellen Änderung der Liste `ListofSIDs`. Es müssen allerdings einige Ausnahmen berücksichtigt werden. Die ersten beiden Ausnahmen sind nicht mehr relevant, da neuere Technologien zur Verfügung stehen.

- **Getrennte Rollen für Controller:** Vor der Einführung von Zonen in XenApp und XenDesktop 7.7 wurde die Liste `ListofSIDs` manuell konfiguriert, wenn nur eine Teilgruppe von Controllern für die Registrierung verwendet wurde. Wenn beispielsweise XDC-001 und XDC-002 als XML-Broker verwendet wurden und XDC-003 und XDC-004 für die VDA-Registrierung, wurden alle Controller in der Liste `ListofSIDs` sowie die Controller XDC-003 und XDC-004 in der Liste `ListofDDCs` angegeben. Dies ist keine typische oder empfohlene Konfiguration. Verwenden Sie sie nicht in neueren Umgebungen. 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.

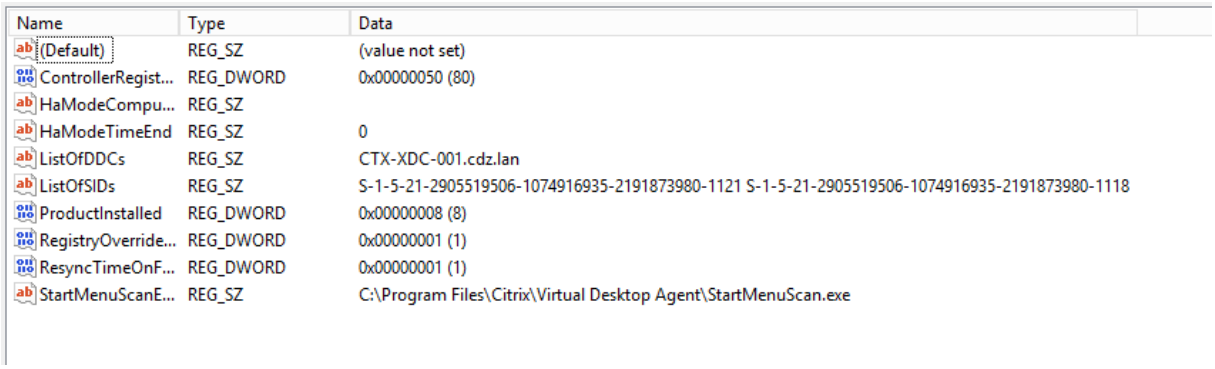
 

- **Sicherheit:** In manchen hochsicheren Umgebungen wurden die SIDs vertrauenswürdiger Controller manuell konfiguriert, um mögliche Sicherheitsbedrohungen durch beeinträchtigte DNS-Server zu vermeiden. Hierfür müssen Sie jedoch auch die automatische Aktualisierung deaktivieren. Andernfalls wird die 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 (ListOfSIDs) verwendet.



| Name | Type | Data |
|---|---|---|
| (Default) | REG_SZ | (value not set) |
| ControllerRegist... | REG_DWORD | 0x00000050 (80) |
| HaModeCompu... | REG_SZ | |
| HaModeTimeEnd | REG_SZ | 0 |
| ListOfDDCs | REG_SZ | CTX-XDC-001.cdz.lan |
| ListOfSIDs | REG_SZ | S-1-5-21-2905519506-1074916935-2191873980-1121 S-1-5-21-2905519506-1074916935-2191873980-1118 |
| ProductInstalled | REG_DWORD | 0x00000008 (8) |
| RegistryOverride... | REG_DWORD | 0x00000001 (1) |
| ResyncTimeOnF... | REG_DWORD | 0x00000001 (1) |
| StartMenuScanE... | REG_SZ | C:\Program Files\Citrix\Virtual Desktop Agent\StartMenuScan.exe |

### Controllersuche während der VDA-Registrierung

Wenn ein VDA versucht, sich zu registrieren, führt der Broker-Agent zunächst eine DNS-Suche in der lokalen Domäne durch, um sicherzustellen, dass der angegebene Controller erreicht werden kann.

Wenn der Controller dabei nicht gefunden wird, kann der Broker-Agent eine Top-Down-Fallbacksuche in AD starten. Diese Abfrage durchsucht alle Domänen und wird mehrfach wiederholt. Wenn die Controlleradresse ungültig ist (z. B. weil der Administrator bei der Installation des VDA einen falschen FQDN eingegeben hat), kann die Abfrage zu einem verteilten Denial-of-Service (DDoS) auf dem Domänencontroller führen.

Der folgende Registrierungsschlüssel legt fest, ob der Broker-Agent die Top-Down-Fallbacksuche verwendet, wenn er bei der ersten Suche keinen Controller findet.

`HKEY_LOCAL_MACHINE\Software\Policies\Citrix\VirtualDesktopAgent`

- Name:`DisableDdcWildcardNameLookup`
- Typ: `DWORD`
- Wert: `1` (Standard) oder `0`

Bei Auswahl von `1` ist die Fallbacksuche deaktiviert. Wenn die erste Suche nach dem Controller fehlschlägt, sucht der Broker-Agent nicht weiter. Dies ist die Standardeinstellung.
Bei Auswahl von `0` ist die Fallbacksuche aktiviert. Wenn die erste Suche nach dem Controller fehlschlägt, wird die Top-Down-Fallbacksuche gestartet.

### LDAP-Bindungssequenzdurchlauf während der VDA-Registrierung mit einem schreibgeschützten Domänencontroller

Wenn ein VDA sich bei einem schreibgeschützten Domänencontroller (RODC) registriert, muss der Broker Agent die LDAP-Bindungen auswählen, die ignoriert werden sollen. Um diese Auswahl zu treffen, benötigt der Broker Agent einen geeigneten Registrierungsschlüssel.

Wenn kein Registrierungsschlüssel bereitgestellt wird oder wenn das Feld für den Registrierungsschlüssel leer ist, dauert die VDA-Registrierung beim RODC länger, da zunächst die ursprüngliche LDAP-Bindungssequenz durchlaufen wird.

Um die LDAP-Bindungssequenz zu ändern, wurde unter `HKEY_LOCAL_MACHINE\Software\Policies\Citrix\VirtualDesktopAgent` der Registrierungsschlüssel `ListofIgnoredBindings` hinzugefügt. Mithilfe von `ListofIgnoredBindings` können Sie die LDAP-Bindungssequenz nach Bedarf ändern und dadurch die VDA-Registrierung bei einem RODC beschleunigen.

- Name:`ListofIgnoredBindings`
- Typ: `REG_SZ`
- Werte: `DefaultPath`, `DomainPath`, `PDCPath`

Der Wert ist eine Liste von Bindungspfadoptionen, die jeweils durch ein Komma getrennt sind. Der Registrierungsschlüssel ignoriert alle Werte, die nicht als gültig erkannt werden.

### Problembehandlung bei der VDA-Registrierung

Wie bereits erwähnt, muss ein VDA bei einem Delivery Controller oder Cloud Connector 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 wurde (z. B. weil die Maschine nie 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. Um Features zu verwenden, 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.
- Probleme bei der VDA-Registrierung und beim Sitzungsstart lassen sich auch durch Integritätsprüfungen mit Citrix Scout beheben. Weitere Informationen finden Sie unter Informationen zu Integritätsprüfungen.

## Virtuelle IP und virtuelles Loopback

June 27, 2024

> **Wichtig:**
>
> - Windows 10 Enterprise-Multisitzungs-OS unterstützt keine IP-Virtualisierung (virtuelle IP) für Remotedesktops und Citrix unterstützt weder Remotedesktop-IP-Virtualisierung noch virtuelles Loopback für Windows 10-Multisitzungs-OS.
> - Remotedesktop-IP-Virtualisierung (Virtual IP) wird auf in der Cloud gehosteten Maschinen nicht unterstützt.
>
>   Informationen hierzu finden Sie in der Dokumentation von Microsoft.

Die Features Remotedesktop-IP-Virtualisierung und virtuelles Loopback werden auf Maschinen unter Windows Server 2016, Windows Server 2019 und Windows Server 2022 unterstützt. Die Features gelten nicht für Windows-Desktopbetriebssystemmaschinen.

Das Feature IP-Virtualisierungsadresse von Microsoft-Remotedesktop stellt einer veröffentlichten Anwendung eine eindeutige dynamisch zugewiesene IP-Adresse für jede Sitzung bereit. Mit dem Citrix Feature für virtuelles Loopback 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 Loopbackadresse. Andere Anwendungen binden sich möglicherweise an einen statischen Port an, sodass das Starten weitere Instanzen einer Anwendung in Mehrbenutzerumgebungen fehlschlägt, da der Port verwendet wird. Damit solche Anwendungen in einer Citrix Virtual Apps-Umgebung richtig ausgeführt werden können, benötigen Sie für jedes Gerät eine eindeutige IP-Adresse.

Remotedesktop-IP-Virtualisierung und virtuelles Loopback sind voneinander unabhängige Features. Sie können ein Feature oder beide wählen.

Zusammenfassung der Administratoraktion:

- Zur Verwendung von IP-Virtualisierung von Microsoft-Remotedesktop 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.

### Remotedesktop-IP-Virtualisierung (virtuelle IP)

Wenn Remotedesktop-IP-Virtualisierung 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 Remotedesktop-IP-Virtualisierung 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

So ermitteln Sie, ob eine Anwendung Remotedesktop-IP-Virtualisierungsadressen verwenden muss:

1. Beziehen Sie das **TCPView-Tool** von Microsoft. Das Programm zeigt alle Anwendungen an, die an spezifische IP-Adressen und Ports binden. Weitere Informationen zu TCPView finden Sie in der Dokumentation von Microsoft.
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 weitere 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 zur Konfiguration der Remotedesktop-IP-Virtualisierung 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 Feature der **Remotedesktop-IP-Virtualisierung** 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 korrekte IP-Adresse, die sie verwenden soll. Jeder Versuch der Anwendung, auf TCP- oder UDP-Kommunikation zu lauschen, wird automatisch an die zugewiesene virtuelle IP-Adresse (oder Loopbackadresse) gebunden. Alle von der Anwendung geöffneten ursprünglichen Verbindungen stammen von der an die Anwendung gebundenen IP-Adresse.

In Funktionen, die eine Adresse ausgeben, (wie z. B. `GetAddrInfo()`, über eine Windows–Richtlinie gesteuert), untersucht die Remotedektop-IP-Virtualisierung beim Abrufen der IP-Adresse des lokalen Hosts die zurückgegebene IP-Adresse und ändert sie in die Remotedesktop-IP-Virtualisierungsadresse der Sitzung. Anwendungen, die mit solchen Namensfunktionen versuchen, die IP-Adresse des lokalen Servers zu ermitteln, erhalten nur die eindeutige Remotedesktop-IP-Virtualisierungsadresse, 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 Feature Remotedesktop-IP-Virtualisierungsadresse sucht in diesen Aufruftypen auch nach 0.0.0.0. Es ändert den Aufruf so, dass er die spezifische Remotedesktop-IP-Virtualisierungsadresse abhört, wodurch mehr als eine Anwendung denselben Port auf demselben Computer abhören kann, da sie alle an unterschiedlichen Adressen lauschen. Der Aufruf wird nur geändert, wenn er in einer ICA-Sitzung erfolgt und das Feature Remotedesktop-IP-Virtualisierungsadresse aktiviert ist. 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

Wenn die Einstellungen der **Citrix Richtlinie für Remotedesktop-IP-Virtualisierung-Loopback** aktiviert sind, 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. Dieses Feature 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. Andernfalls kommt es evtl. zu unerwünschten Ergebnissen.
- 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.

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>

## Zonen

June 27, 2024

> **Hinweis:**
>
> Sie können Ihre Citrix Virtual Apps and Desktops-Bereitstellung mithilfe von zwei Verwaltungskonsolen verwalten: Web Studio (webbasiert) und Citrix Studio (Windows-basiert). Dieser Artikel behandelt nur Web Studio. Informationen zu Citrix Studio finden Sie im entsprechenden Artikel in Citrix Virtual Apps and Desktops 7 2212 oder früher.

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 Web 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". Diese Zone umfasst SQL Server-Sitedatenbank (sowie ggf. hoch verfügbare SQL Server-Computer), Web Studio, Director, Citrix StoreFront, Citrix Lizenzserver und Citrix Gateway. Die Sitedatenbank muss immer in der primären Zone sein.

Die primäre Zone muss mindestens zwei Controller für Redundanzzwecke haben. Die primäre Zone kann VDAs mit Anwendungen enthalten, die eng an die Datenbank und Infrastruktur gekoppelt sind.

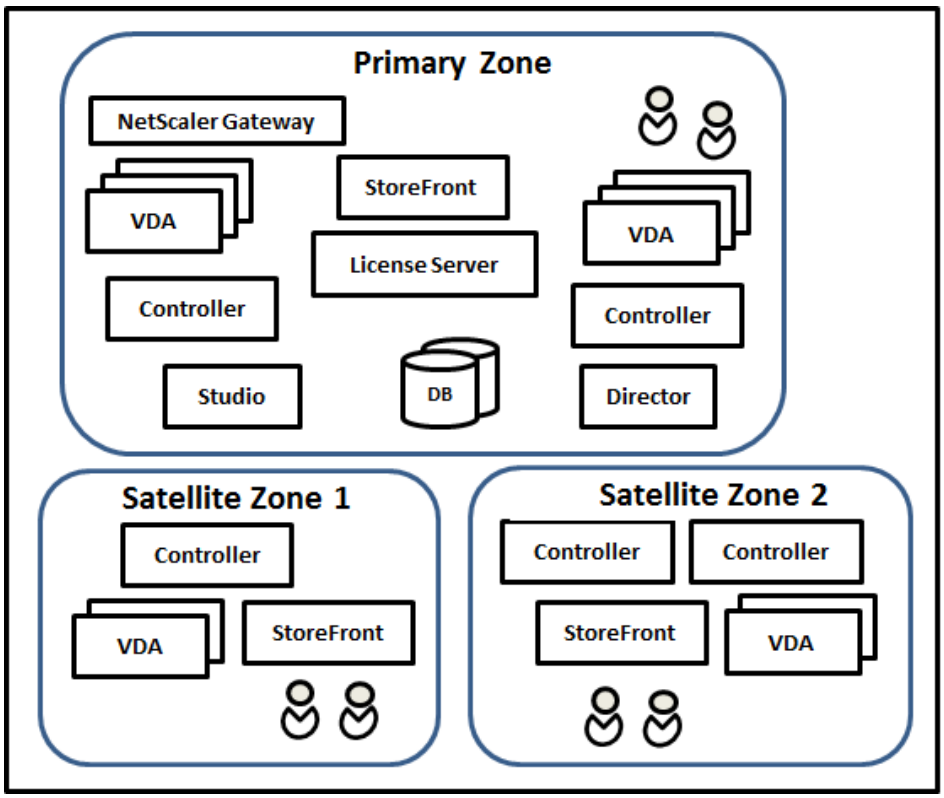
**Satellitenzonen:**

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 Speicherung von Maschinen enthalten. Beim Konfigurieren einer Satellitenzone können Sie dieser eine Verbindung zu einem Hypervisor oder zu einem anderen Service zuweisen. Alle Kataloge, 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, Web 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.
- **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 einer 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 Katalog 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 Web 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.

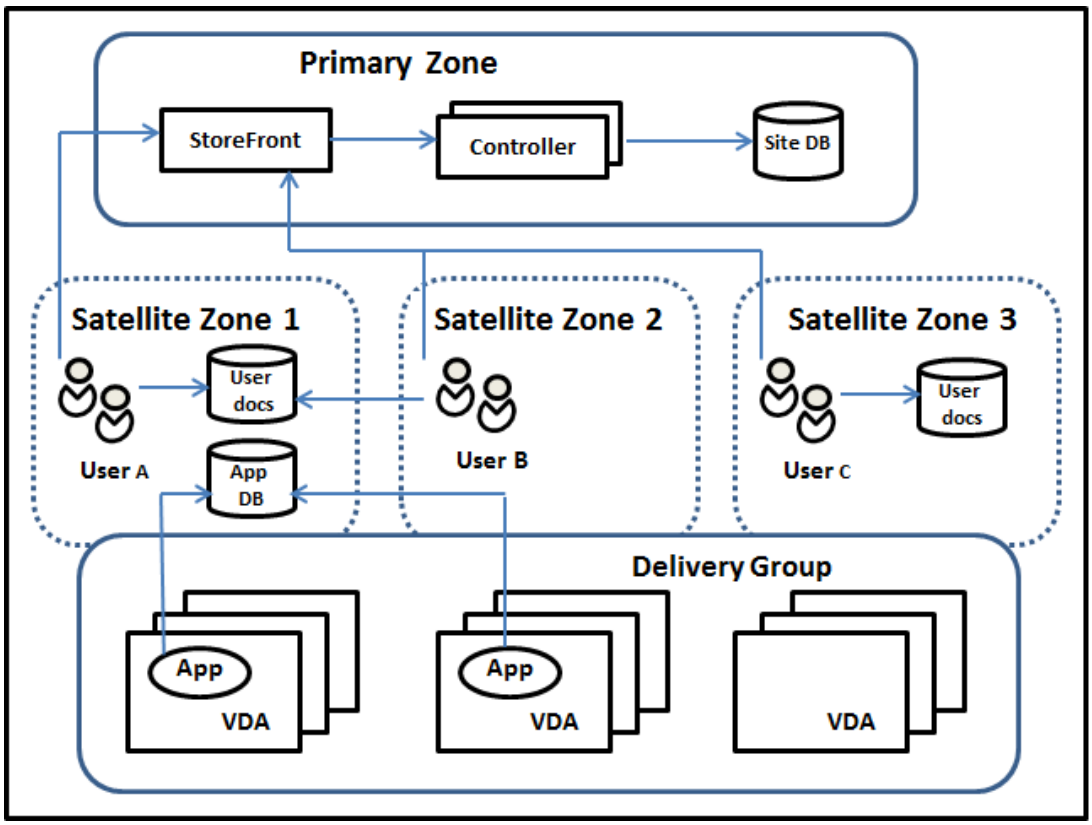
### Funktionsweise der Zonenpräferenz

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. Dieses Beispiel veranschaulicht, dass Benutzer ihre Citrix Workspace-App-Endpunkte an verschiedenen Standorten ausführen können.

- Benutzer A verwendet ein Gerät mit Citrix Workspace-App in Satellitenzone 1.
- Benutzer B verwendet ein Gerät in Satellitenzone 2.
- Die Dokumente eines Benutzers können an verschiedenen Orten gespeichert sein.
  - Benutzer A und B verwenden eine Freigabe in Satellitenzone 1.
  - Benutzer C verwendet 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 konfiguriert ist) 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 Anwendung auf einem VDA erzwungen wird, der sich in der Nähe des Geräts 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 Katalog eine Hostverbindung verwendet, müssen Katalog und Verbindung in der gleichen Satellitenzone 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 Controller in einer Satellitenzone platziert werden, wird angenommen, dass sie eine gute (lokale) Verbindung mit Hypervisors und VDAs in derselben Zone 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 Katalogs 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 Katalogs 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 Web 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. Dadurch können Sie Elemente trennen, die am besten in unmittelbarer Nähe funktionieren. Das Verschieben eines Katalogs 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 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 Web Studio und Director nur in der primären Zone. Sie können auf Web Studio und Director über eine Satellitenzone zugreifen (beispielsweise eine Satellitenzone mit Controllern, die für ein Failover bei Ausfall der primären Zone verwendet werden), da dies Webanwendungen sind.
- Im Idealfall wird Citrix Gateway in einer Satellitenzone für Benutzerverbindungen aus anderen Zonen oder externen Orten verwendet, 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 Katalogs von einer Zone in eine andere brauchen Sie beispielsweise die Berechtigung zum Bearbeiten des Maschinenkatalogs. Weitere Informationen finden Sie unter Delegierte Administration.

**Mit Citrix Provisioning:** Die bereitgestellte Citrix Provisioning Console erkennt keine Zonen. Wir empfehlen daher, Web Studio zum Erstellen von Katalogen für Satellitenzonen zu verwenden. Erstellen Sie den Katalog in Web Studio 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 der primären Zone platziert. Sie müssen ihn mithilfe von Web Studio in die Satellitenzone verschieben.)

#### Erstellen von Zonen

1. Melden Sie sich bei Web Studio an.
2. Wählen Sie im linken Bereich **Zonen**.
3. Wählen Sie in der Aktionsleiste **Zone erstellen**.
4. Geben Sie einen Namen für die Zone und optional eine Beschreibung ein. Der Name muss innerhalb der Site eindeutig sein.
5. 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.
6. Klicken Sie auf **Speichern**.

Alternativ können Sie ein oder mehrere Elemente in Web Studio auswählen und dann in der Aktionsleiste die Option **Zone erstellen** wählen.

#### Ändern des Namen oder der Beschreibung einer Zone

1. Melden Sie sich bei Web Studio an.
2. Wählen Sie im linken Bereich **Zonen**.
3. Wählen Sie im mittleren Bereich eine Zone und dann in der Aktionsleiste **Zone bearbeiten**.
4. Ändern Sie den Namen und/oder die Beschreibung der Zone. Wenn Sie den Namen der primären Zone ändern, stellen Sie sicher, dass sie weiterhin eindeutig als primäre Zone identifiziert werden kann.
5. Klicken Sie auf **Speichern** oder **Anwenden**.

#### Verschieben von Elementen zwischen Zonen

1. Melden Sie sich bei Web Studio an.
2. Wählen Sie im linken Bereich **Zonen**.
3. Wählen Sie im mittleren Bereich eine Zone und dann ein oder mehrere Elemente.
4. Ziehen Sie entweder das Element in die Zielzone oder wählen Sie in der Aktionsleiste **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 Katalog eine Hostverbindung zu einem Hypervisor oder anderen Service 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. Melden Sie sich bei Web Studio an.
2. Wählen Sie im linken Bereich **Zonen**.
3. Wählen Sie eine Zone im mittleren Bereich.
4. Wählen Sie in der Aktionsleiste **Zone löschen**. Wenn die Zone nicht leer ist, werden Sie aufgefordert, die Zone auszuwählen, in die die enthaltenen Elemente verschoben werden sollen.
5. 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. Melden Sie sich bei Web Studio an.
2. Wählen Sie im linken Bereich **Zonen** und wählen Sie dann im mittleren Bereich eine Zone aus.
3. Wählen Sie in der Aktionsleiste **Benutzer zur Zone hinzufügen**.
4. 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.
5. 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. Melden Sie sich bei Web Studio an.
2. Wählen Sie im linken Bereich **Zonen** und wählen Sie dann im mittleren Bereich eine Zone aus.
3. Wählen Sie in der Aktionsleiste **Benutzer aus Zone entfernen**.
4. 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.
5. 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 zu einem späteren Zeitpunkt.

- Wählen Sie beim Erstellen einer Bereitstellungsgruppe, Erstellen einer Anwendungsgruppe oder Hinzufügen von Anwendungen zu vorhandenen Gruppen auf der Seite **Anwendungen** des Assistenten **Eigenschaften**.
- Um die Eigenschaften einer Anwendung nach dem Hinzufügen zu ändern, wählen Sie im linken Bereich **Anwendungen**. Wählen Sie die Anwendung und dann in der Aktionsleiste **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.
  - 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

Nach dem Erstellen von mindestens einer Satellitenzone können Sie beim Hinzufügen einer Hostverbindung oder beim Erstellen eines Katalogs eine Zone angeben.

Normalerweise ist die primäre Zone die Standardeinstellung. Wenn Sie einen Katalog 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.

# Überwachung

June 27, 2024

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
- Fehlerhafte Einzelsitzungsmaschinen

- Fehlerhafte Multisitzungsmaschinen

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 werden zur Überwachung und Problembehandlung verwendet.

Weitere Informationen finden Sie unter Ereignisprotokolle. Artikel zu einzelnen Features enthalten auch Informationen zu Ereignissen.

## Konfigurationsprotokollierung

June 27, 2024

Die Konfigurationsprotokollierung dient zum Erfassen der Sitekonfigurationsänderungen und Administratoraktivitäten in einer Datenbank. Das Feature ist in der Standardeinstellung aktiviert. Sie können den protokollierten Inhalt folgendermaßen verwenden:

- Diagnose und Behandlung von Problemen nach 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. Melden Sie sich bei Web Studio an und wählen Sie im linken Bereich **Protokollierung**.
2. Wählen Sie in der Aktionsleiste **Einstellungen**. 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. Melden Sie sich bei Web Studio an und wählen Sie im linken Bereich **Protokollierung**.
3. Wählen Sie in der Aktionsleiste **Einstellungen**.
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 in der Aktionsleiste**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 Sie den Bericht speichern möchten.

### 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 ein Backup der Konfigurationsprotokolldaten vor dem Löschen anlegen 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 mehr 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. Melden Sie sich bei Web Studio an und wählen Sie im linken Bereich **Protokollierung**.
2. Wählen Sie in der Aktionsleiste **Protokolle löschen**.
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.

### API- und PowerShell-Protokolle anzeigen

Um API-Anfragen zu überwachen, die während Ihrer aktuellen Sitzung gestellt wurden, klicken Sie auf die Registerkarte **APIs**. API-Protokolle werden gelöscht, nachdem Sie sich von Web Studio abmelden.

Um PowerShell-Befehle anzuzeigen, die den von Ihnen im Tagesverlauf ausgeführten Benutzeroberflächenaktionen entsprechen, klicken Sie auf die Registerkarte **PowerShell**.

### Metadaten zu Konfigurationsprotokollen zuordnen

Sie können Metadaten Konfigurationsprotokolle anfügen, indem Sie den Protokolldatensätzen das `MetadataMap`-Paar `name-value` zuordnen.

> **Hinweis:**
>
> - Sie können Metadaten nur High-Level-Operation-Objekten anfügen.
> - Die Metadaten werden den vorhandenen Datensätzen zum Zeitpunkt der Ausführung zugeordnet.

#### Metadaten festlegen

Führen Sie den PowerShell-Befehl `Set-LogHighLevelOperationMetadata` aus, um einem Protokolldatensatz `MetadataMap` anzufügen.

`Set-LogHighLevelOperationMetadata` hat folgende Parameter:

- **Id**: ID der High-Level-Operation.
- **InputObject**: High-Level-Operationen, zu denen Sie die Metadaten hinzufügen. Dies ist eine Alternative zu Parameter `Id`, mit dem ein High-Level-Operationsobjekt (bzw. eine Objektliste) an den PowerShell-Befehl übergeben wird.

---

**Name**: Eigenschaftsname der Metadaten, die hinzugefügt werden sollen. Die Eigenschaft muss für die angegebene High-Level-Operation eindeutig sein. Die Eigenschaft darf keines der folgenden Zeichen enthalten: ()/;:#.*?=<> []'".

---

- 
- **Value**: Wert der Eigenschaft.
- **Map**: Wörterbuch von name-value-Paaren für die Eigenschaften. Dies ist eine Alternative zum Festlegen der Metadaten mithilfe der Parameter `-Name` und `-Value`.

Führen Sie beispielsweise den folgenden PowerShell-Befehl aus, um die Metadaten an alle High-Level-Protokolldatensätze mit der ID 40 anzufügen:

```
Get-LogHighLevelOperation – Id 40 | Set-LogHighLevelOperationMetadata
 -Name A -Value B
```

Führen Sie den folgenden PowerShell-Befehl aus, um die Metadaten an den High-Level-Datensatz mit dem Benutzer `abc@example.com` anzufügen:

```
Get-LogHighLevelOperation – User `abc@example.com` | Set-LogHighLevelOperation
 -Name C -Value D
```

#### Anhand von Metadaten abrufen

Führen Sie die folgenden PowerShell-Befehle aus, um Protokolldatensätze anhand der zugehörigen Metadaten abzurufen:

- Suche nach Schlüssel und Wert:

  ```
  Get-LogHighLevelOperation -Metadata "Key:Value"
  ```

- Suche nach Wert eines beliebigen Schlüssels:

  ```
  Get-LogHighLevelOperation -Metadata "*:Value"
  ```

- Suche nach Schlüssel und einem beliebigen Wert:

  ```
  Get-LogHighLevelOperation -Metadata "Key:*"
  ```

#### Metadaten entfernen

Führen Sie den PowerShell-Befehl `Remove-LogHighLevelOperationMetadata` aus, um zugeordnete Metadaten zu entfernen.
`Remove-LogHighLevelOperationMetadata` hat folgende Parameter:

- **Id**: ID der High-Level-Operation.
- **InputObject**: High-Level-Operationen, zu denen Sie die Metadaten hinzufügen. Dies ist eine Alternative zu Parameter `Id`‘, mit dem ein High-Level-Operationsobjekt (bzw. eine Objektliste) an den PowerShell-Befehl übergeben wird.
- **Name**: Eigenschaftsname der Metadaten, die entfernt werden sollen. $null entfernt alle Metadaten aus dem angegebenen Objekt.
- **Map**: Wörterbuch von name-value-Paaren für die Eigenschaften. Dies kann entweder eine Hashtabelle sein (erstellt mit @{“name1”= “val1”; “name2”= “val2”}) oder ein Zeichenkettenwörterbuch (erstellt mit new-object “System.Collections.Generic.Dictionary[String, String]”). Die Eigenschaften, deren Namen mit den Schlüsseln in Map übereinstimmen, werden entfernt.

## Ereignisprotokolle

June 27, 2024

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.

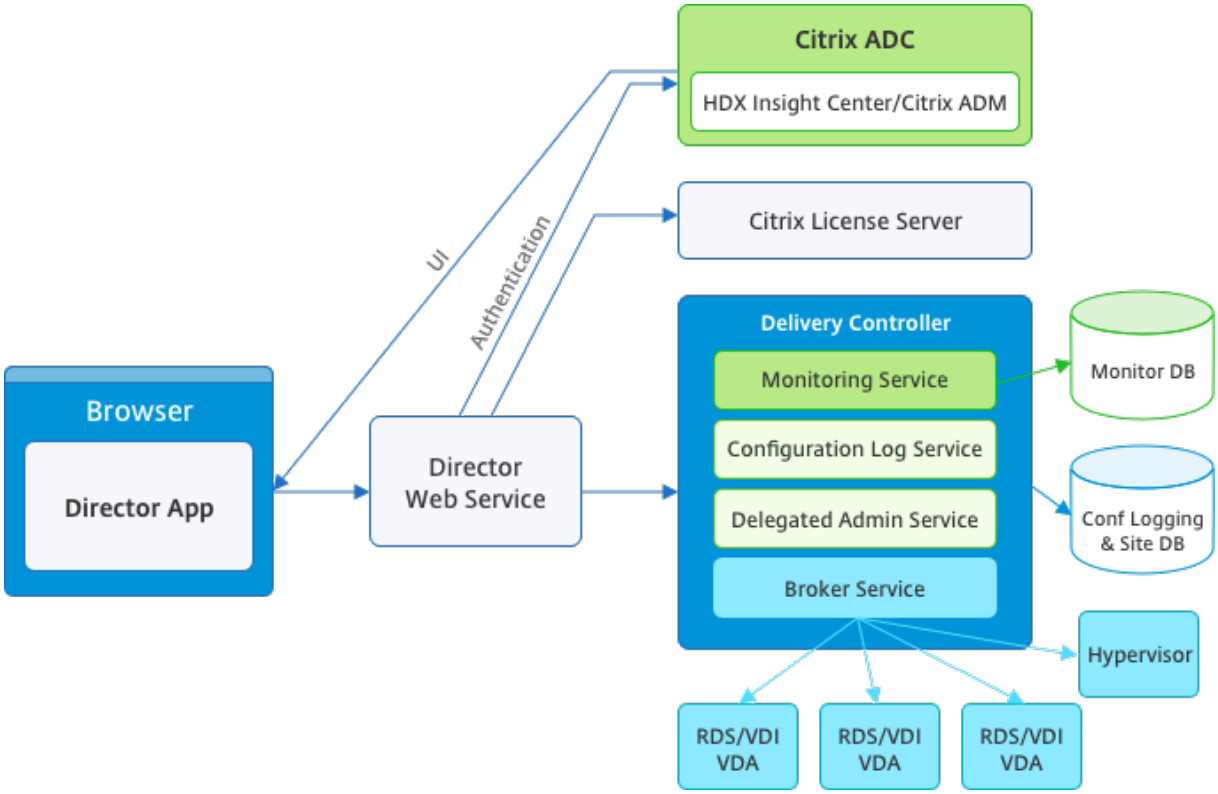
- Citrix Brokerdienstereignisse
- Citrix FMA Service SDK-Ereignisse
- Citrix Konfigurationsdienstereignisse
- Citrix Delegated Administration Service-Ereignisse

# Director

June 27, 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. Die folgenden Analysen über Citrix ADM helfen, durch das Netzwerk verursachte Engpässe in einer Citrix Virtual Apps- oder Desktops-Umgebung zu erkennen:
  - Leistungsmanagement zur Gewährleistung von Integrität und Kapazität
  - Analyse historischer Trend- und Netzwerkdaten
- 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 etwas länger, während Verbindungsversuche mit dieser Site laufen.

### Verwenden von Director mit PIV-Smartcardauthentifizierung

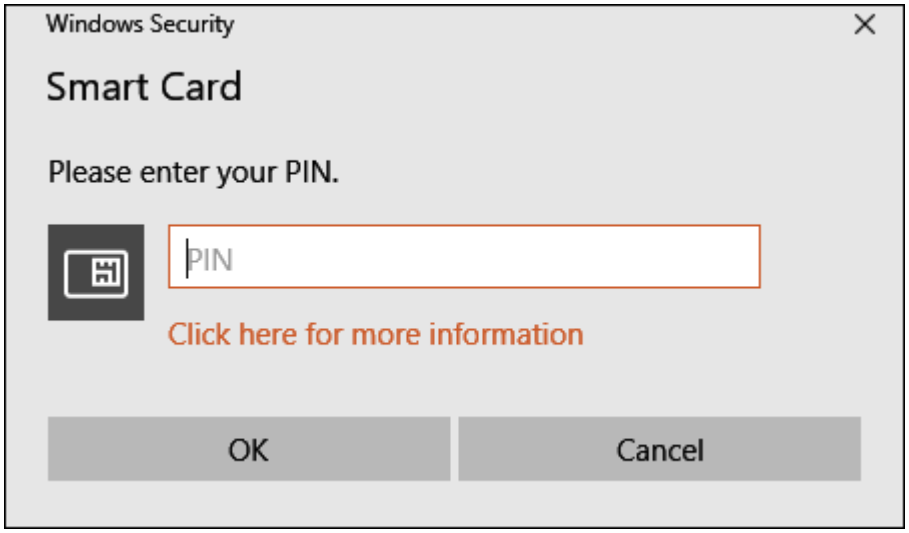
Director unterstützt jetzt die Smartcardauthentifizierung auf PIV-Basis (Personal Identity Verification). Das Feature ist für Unternehmen und Behörden nützlich, die eine Authentifizierung per Smartcard für die Zugriffssteuerung verwenden.
Die Smartcardauthentifizierung erfordert eine spezifische Konfiguration 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

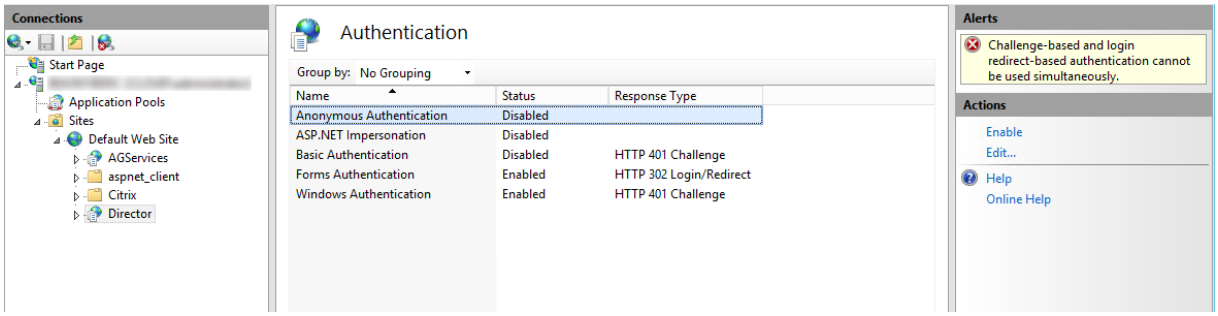
Mit der integrierten Windows-Authentifizierung (IWA) erhalten in die Domäne eingebundene Benutzer direkten Zugriff auf Director, ohne ihre Anmeldeinformationen auf der Director-Anmeldeseite erneut eingeben zu müssen. Für die Verwendung der integrierten Windows-Authentifizierung mit Director gelten folgende 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 Unterstützung 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. Dazu gehören der 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 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 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:

```
New-Item HKLM:\SOFTWARE\Citrix -Name Director

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 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:

```
New-Item HKLM:\SOFTWARE\Citrix -Name Director

New-ItemProperty HKLM:\SOFTWARE\Citrix\Director -Name DisableGuidedHelp
    -PropertyType DWORD -Value 1
```

# Installation

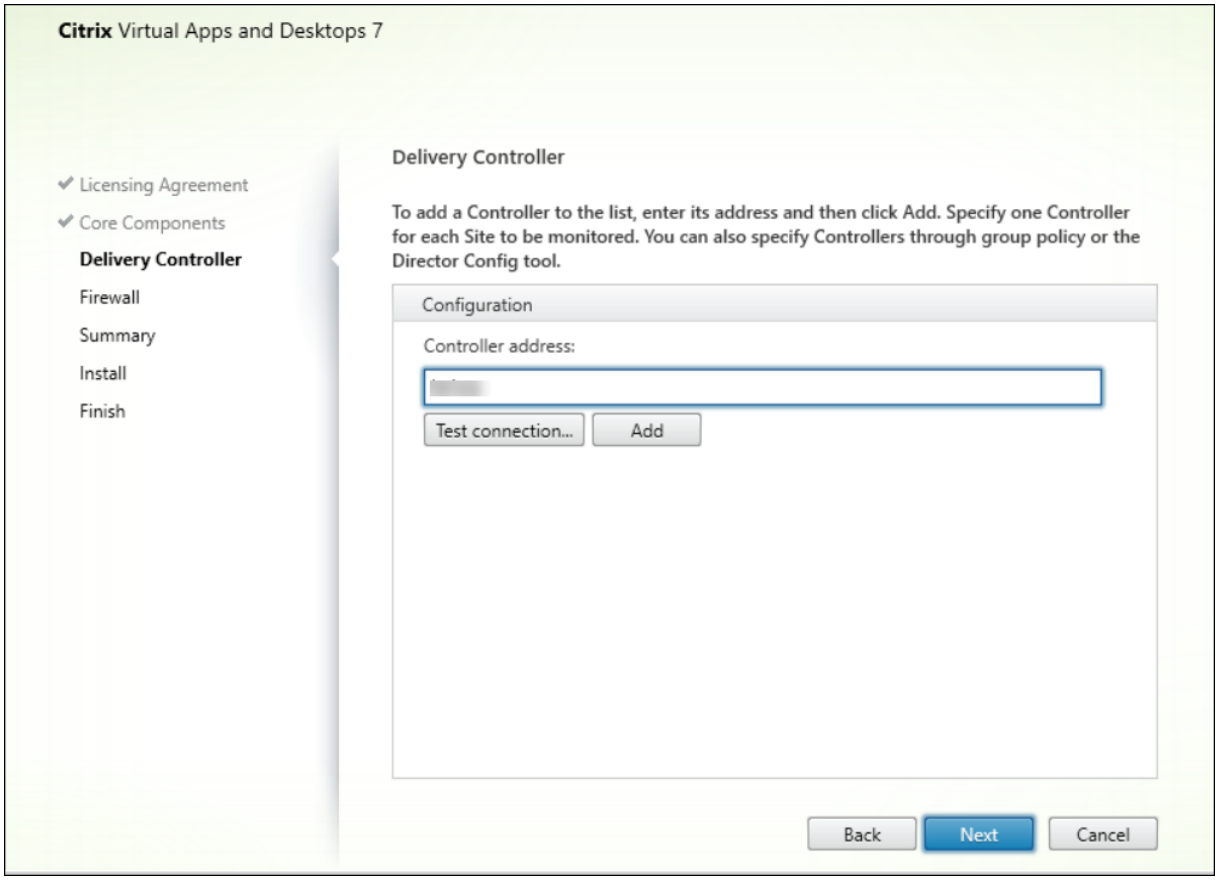
June 27, 2024

## 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 lassen Sie nur Director-Verbindungen mit HTTPS und nicht mit HTTP zu. 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

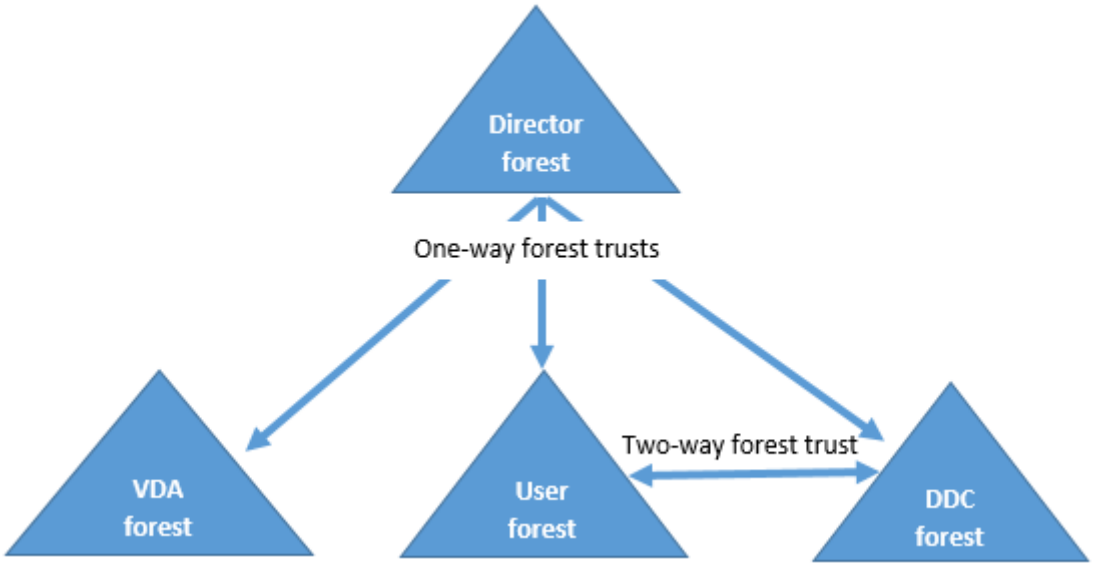
June 27, 2024

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 weiteren 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:

```
1 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 weiteren Domäne oder Gesamtstruktur zu ermöglichen, fügen Sie, wie in diesem Beispiel gezeigt, den Namen der Domäne der Liste hinzu:

```
1 Connector.ActiveDirectory.Domains = (user),(server),\<domain1\>,\<
    domain2\>
```

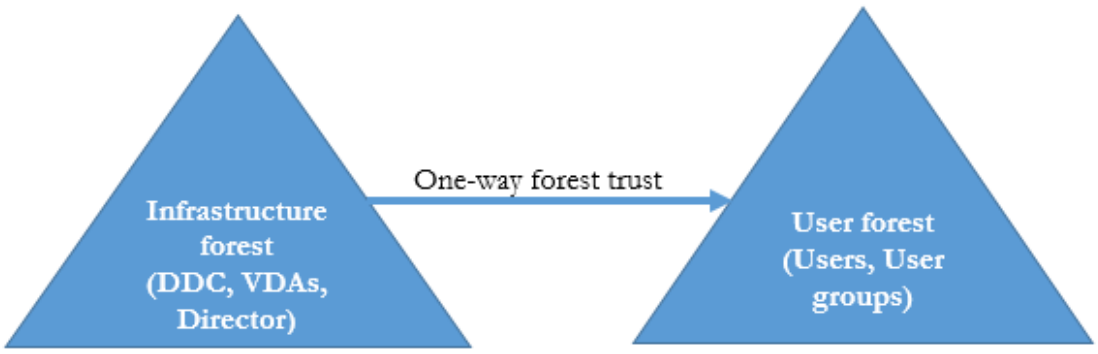
Director versucht, Suchen für jede Domäne in der Liste auf der Gesamtstrukturebene durchzuführen. Wenn Sie keine Berechtigungen zum Suchen auf der Gesamtstrukturebene haben, wird nur die Domäne durchsucht.

### Konfiguration einer domänenlokalen Gruppe

Die meisten Citrix Service Provider (CSPs) haben ähnliche Umgebungen, bei denen VDAs, Delivery Controller und Director in einer Infrastruktur-Gesamtstruktur sind. Die Benutzer-/Gruppeneinträge sind 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

   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 Web 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 Arbeit mit mehreren Sites ein. Verwenden Sie zum Konfigurieren die IIS-Manager-Konsole auf jedem Director-Server, um die Liste der Serveradressen in den Anwendungseinstellungen zu aktualisieren.

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. Erstellen 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 führen sie beide Änderungen durch, damit die Daten im Aktivitätsmanager nicht angezeigt werden.

## PIV-Smartcardauthentifizierung konfigurieren

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:

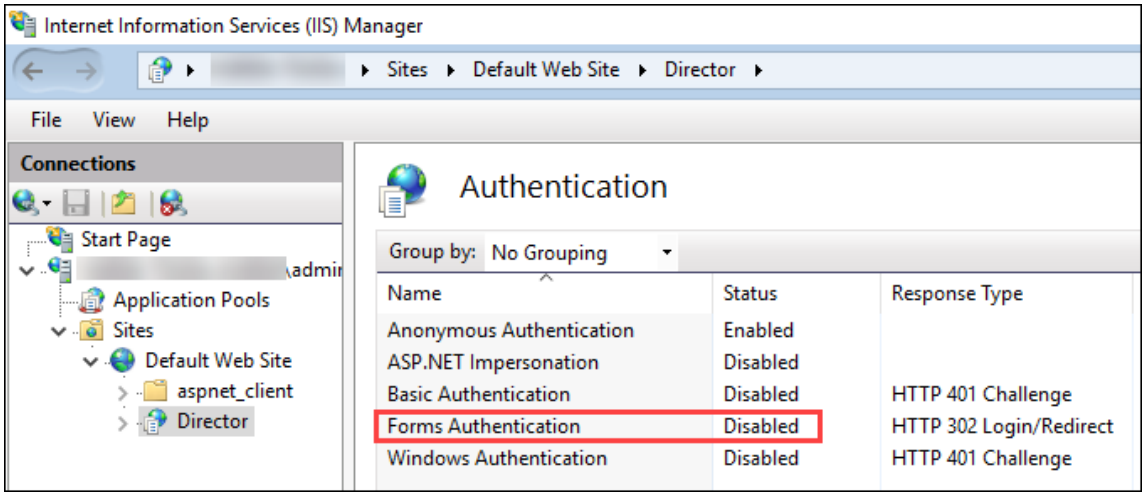
1. Installieren und aktivieren Sie die Clientzertifikatzuordnung-Authentifizierung. Folgen Sie den Anweisungen im Abschnitt **Client Certificate Mapping authentication using Active Directory** des Microsoft-Dokuments Client Certificate Mapping Authentication.
2. Deaktivieren Sie die Formularauthentifizierung 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.

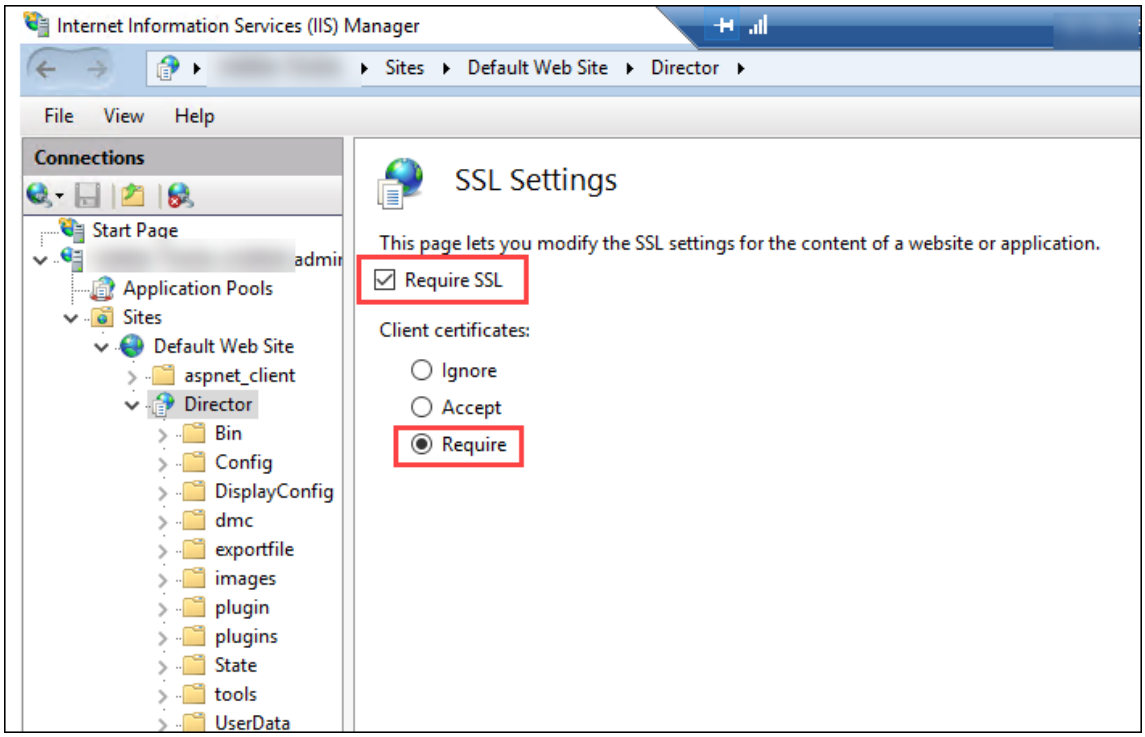
   a) Starten Sie IIS-Manager.

   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>
```

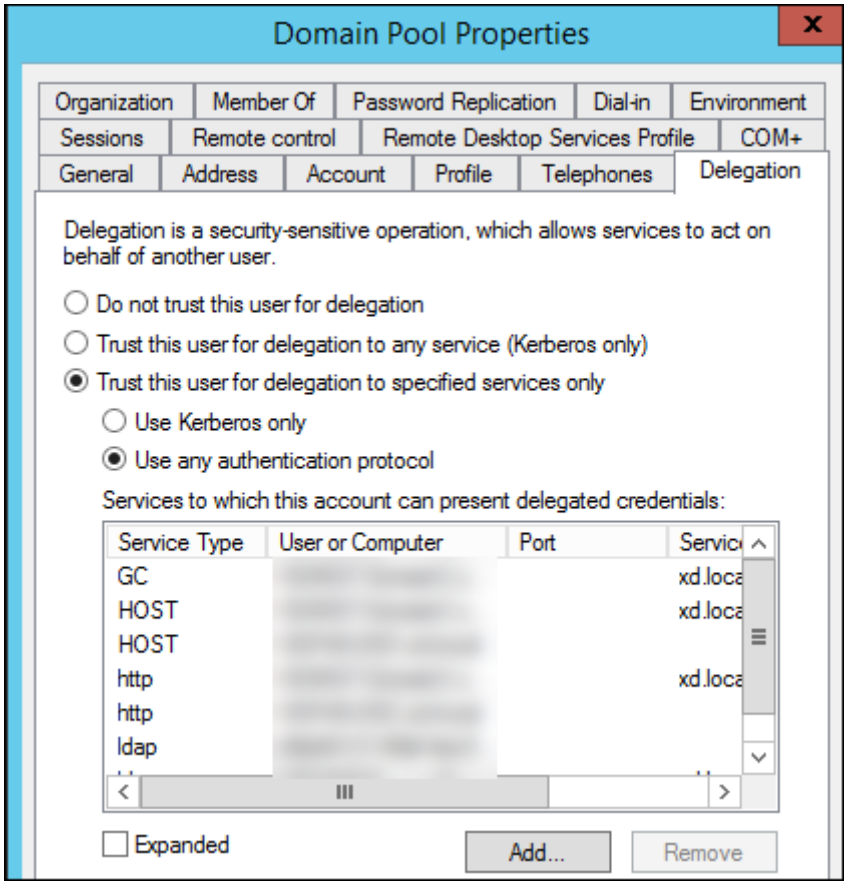
### Active Directory-Konfiguration

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 die Application Pool-Identität. Erstellen Sie das Dienstkonto und weisen Sie TCB-Privilegien zu (siehe MSDN-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”.



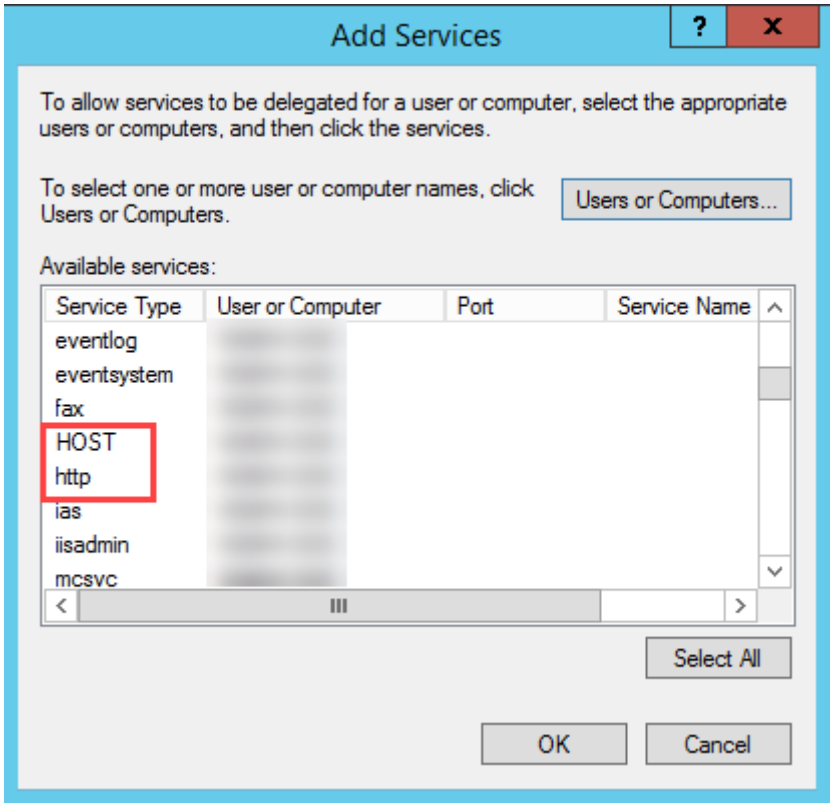

Konfigurieren Sie die folgenden Dienste für dieses Konto:

- Delivery Controller: HOST, HTTP
- Director: HOST, HTTP
- Active Directory: GC, LDAP

Zum Konfigurieren

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.

### Dienstprinzipalnamenseinträge erstellen

Sie müssen ein Dienstkonto für jeden Director-Server und jede virtuelle IP-Adresse mit Lastausgleich erstellen, die für den Zugriff auf einen Director-Serverpool verwendet wird. Sie müssen Dienstprinzipalnamenseinträge erstellen, um eine Delegierung an das neu erstellte Dienstkonto zu konfigurieren.

- Verwenden Sie den folgenden Befehl, um einen Dienstprinzipalnamenseintrag für einen Director-Server zu erstellen:

```
1   setspn -a http/<directorServer>.<domain_fqdn> <domain><
       DirectorAppPoolServiceAcct>
2
3  <!--NeedCopy-->
```

- Use the following command to create an SPN record for a load-balanced VIP:

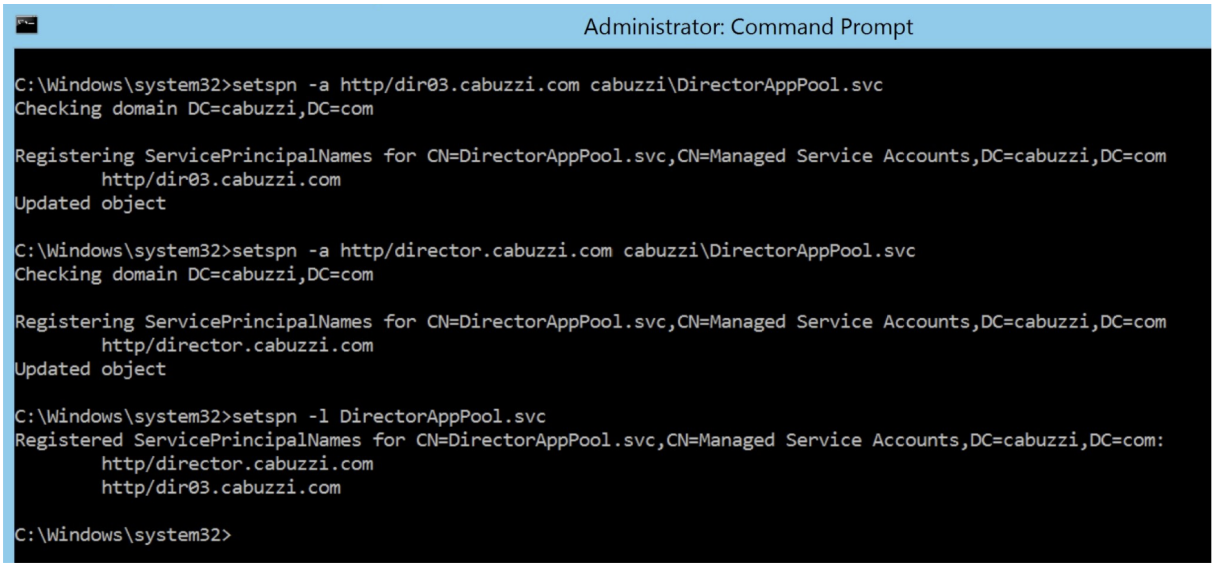
```
1   setspn -S http/<DirectorFQDN> <domain>\<
       DirectorAppPoolServiceAcct>
2
3  <!--NeedCopy-->
```

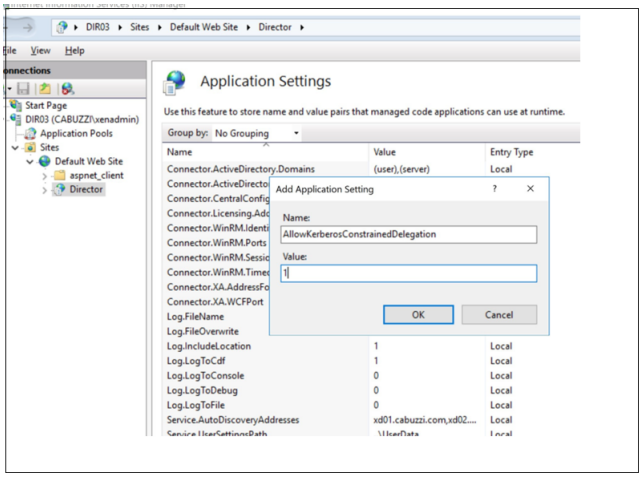
- Verwenden Sie den folgenden Befehl, um die erstellten Dienstprinzipalnamen anzuzeigen oder zu testen:

```
setspn  – l <DirectorAppPoolServiceAcct>

<!--NeedCopy-->
```

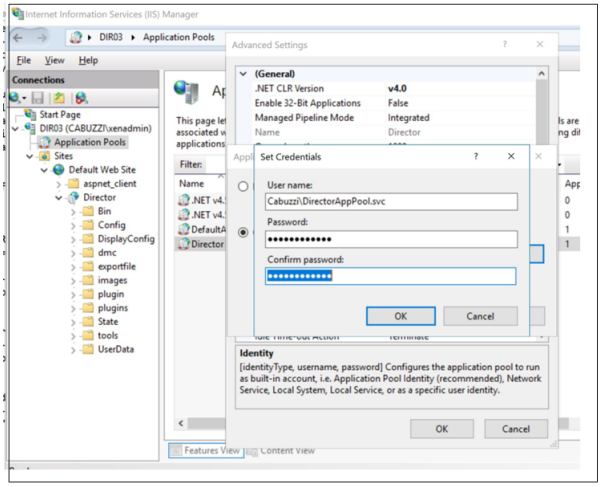



- Select the Director virtual directory in the left pane and double click **Application Settings**. Inside the Application Settings window, click **Add** and ensure **AllowKerberosConstrainedDelegation** is set to 1.




- Select **Application Pools** in the left-hand pane, then right-click the Director application pool and select **Advanced Settings**.
- Select **Identity**, click the ellipses (“…”) to enter the service account domain\logon and password credentials. Close the IIS console.




- From an elevated command prompt, change the directory to C:\Windows\System32\inetsrv and enter the following commands:

```
appcmd.exe set config "Default Web Site" -section:system.webServer/security/authentication/clientCertificateMappingAuthentication /enabled:"True" /commit:apphost

<!--NeedCopy-->
```

```
appcmd.exe set config "Default Web Site" -section:system.webServer/security/access /sslFlags:"Ssl,SslNegotiateCert" /commit:apphost
\`\`\`

![Eingabeaufforderung](/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/dir-smart-card-auth-5-scaled.png)

## Firefox-Konfiguration

Installieren Sie zur Verwendung von Firefox den auf [OpenSC 0.17.0](https://github.com/OpenSC/OpenSC/releases/tag/0.17.0) verfügbaren PIV-Treiber. Anweisungen zu Installation und Konfiguration finden Sie unter [Installing OpenSC PKCS#11 Module in Firefox, Step by Step](https://github.com/OpenSC/OpenSC/wiki/Installing-OpenSC-PKCS%2311-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](/de-de/citrix-virtual-apps-desktops/2402-ltsr/director.html#use-director-with-piv-smart-card-authentication).<!--NeedCopy-->
```

# Konfigurieren der Netzwerkanalyse

June 27, 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 eine virtuelle Appliance, die unter XenServer ausgeführt wird. Mit der Netzwerkanalyse sammelt Director Daten zur Bereitstellung.

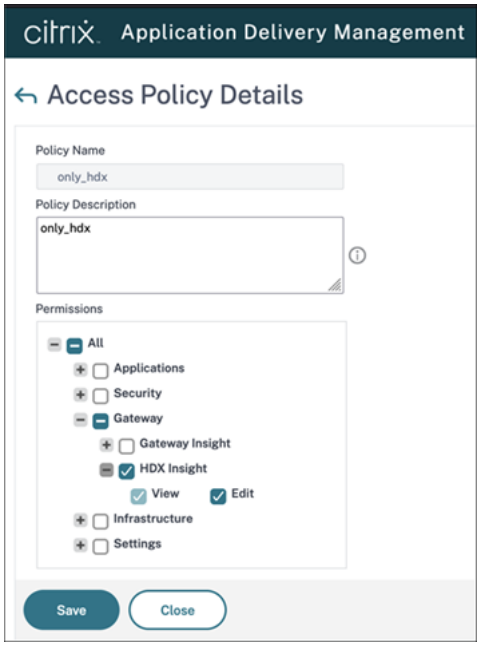
Weitere Informationen finden Sie in der Dokumentation zu Citrix ADM.

> **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

June 27, 2024

Bei der delegierten Administration werden drei Konzepte eingesetzt: Administratoren, Rollen und Geltungsbereiche. Berechtigungen richten sich nach der Administratorrolle und dem Geltungsbereich dieser Rolle. Beispiel: Einem Administrator wird die Helpdeskadministratorrolle zugewiesen, bei der der Geltungsbereich die Verantwortung für Endbenutzer an nur einer Site umfasst.

Weitere Informationen über das Erstellen von delegierten Administratoren finden Sie im Hauptartikel zur delegierten Administration.

Durch die administrativen Berechtigungen wird festgelegt, wie die Director-Benutzeroberfläche für Administratoren dargestellt wird und welche Aufgaben sie ausführen können. Mit Berechtigungen wird Folgendes festgelegt:

- Die Seiten, auf die der Administrator zugreifen kann, kollektiv als "Ansicht"bezeichnet
- Die Desktops, Maschinen und Sitzungen, die der Administrator anzeigen und verwenden kann
- Die Befehle, die der Administrator ausführen kann, z. B. das Spiegeln einer Benutzersitzung oder das Aktivieren des Wartungsmodus

Über die integrierten Rollen und Berechtigungen wird außerdem gesteuert, wie Administratoren Director verwenden:

| Administratorrolle | Berechtigungen in Director |
|---|---|
| Volladministrator | Hat vollständigen Zugriff auf alle Ansichten und kann alle Befehle ausführen, einschließlich Spiegeln einer Benutzersitzung, Aktivieren des Wartungsmodus und Exportieren von Trenddaten. |
| Bereitstellungsgruppenadministrator | Hat vollständigen Zugriff auf alle Ansichten und kann alle Befehle ausführen, einschließlich Spiegeln einer Benutzersitzung, Energieverwaltung und Sitzungverwaltung, Aktivieren des Wartungsmodus und Exportieren von Trenddaten. |
| Lesezugriffadministrator | Kann auf alle Ansichten zugreifen und alle Objekte in angegebenen Geltungsbereichen sowie globale Informationen anzeigen. Kann Berichte aus HDX-Kanälen herunterladen und Trenddaten mit der Exportoption in der Ansicht "Trends"exportieren. Kann keine anderen Befehle ausführen oder Daten in den Ansichten ändern. |

| Administratorrolle | Berechtigungen in Director |
| --- | --- |
| 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. |

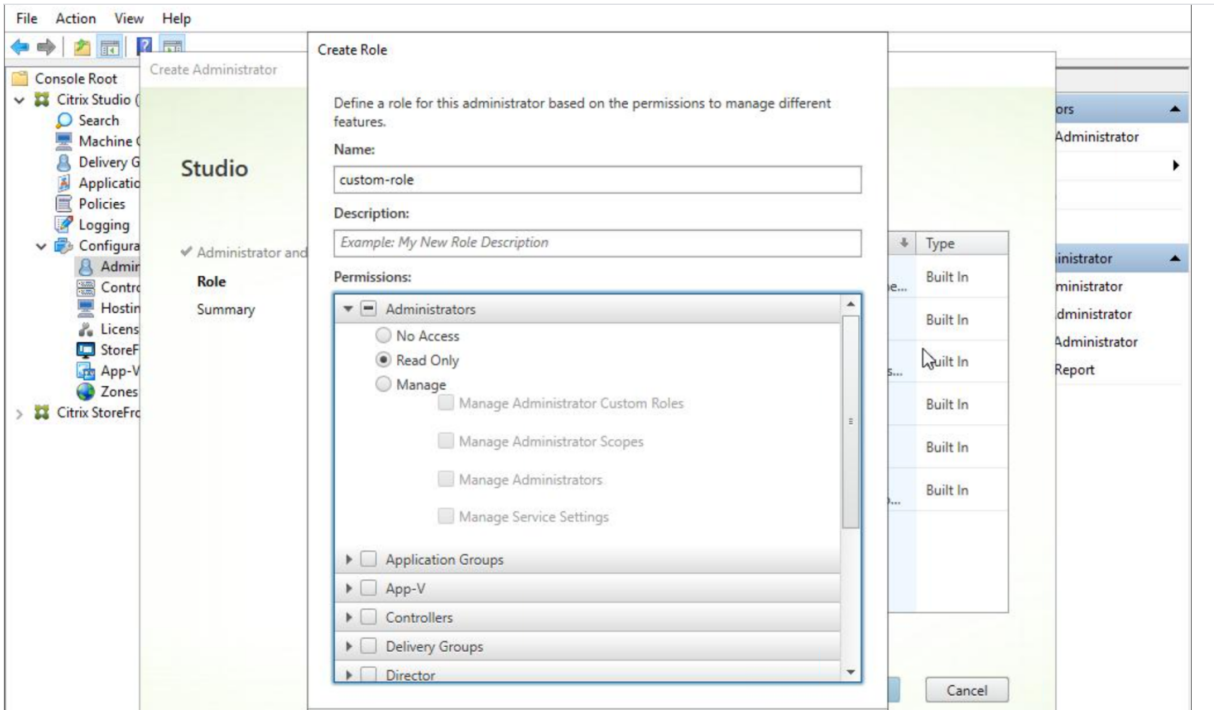
### Konfigurieren von benutzerdefinierten Rollen für Director-Administratoren

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



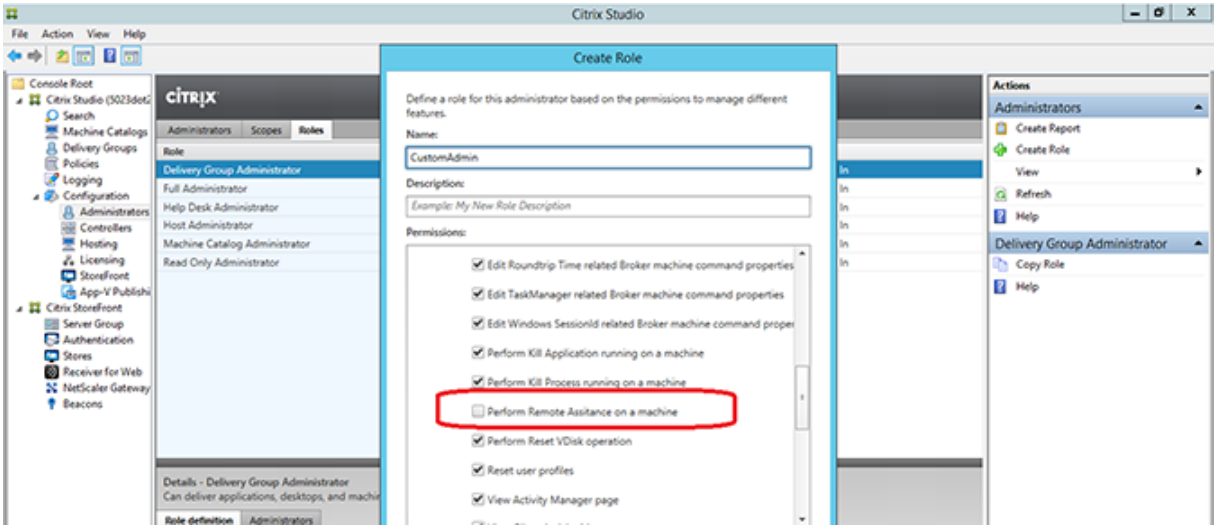

Alternativ können Sie eine benutzerdefinierte Rolle erstellen, indem Sie eine vorhandene Rolle kopieren und dieser zusätzliche Berechtigungen für die verschiedenen Ansichten erteilen. Sie können beispielsweise die Rolle “Helpdesk”kopieren und Berechtigungen zum Anzeigen des Dashboards oder der Seiten “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
- 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

June 27, 2024

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.

### 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
- .png
- .json
- .woff
- .woff2
- .ttf

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 ist, erhalten die Anwendungspools folgende Berechtigungen:

- **Anmelden als Dienst**
- **Anpassen von Speicherkontingenten für einen Prozess**, **Generieren von Sicherheitsüberwachungen** und **Ersetzen eines Tokens auf Prozessebene**

Die Zuweisung der Berechtigungen 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

Verwenden Sie für Produktionsumgebungen IPsec (Internet Protocol Security) oder HTTPS-Protokollen zum Schutz der Datenübertragung zwischen Director und den 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, den Zugriff auf die Director-Konsole innerhalb des Intranetnetzwerks einzuschränken.
- 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.
- Schützen Sie die Kommunikation mit Citrix ADC mit TLS und nicht IPsec.

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

Sie können beliebige Webanwendungen in der Webdomäne (Domänenname und Port) von Director bereitstellen. Allerdings können Sicherheitsrisiken in den Webanwendungen die Sicherheit der Director-Bereitstellung beeinträchtigen. Ist höhere Sicherheit erforderlich, empfiehlt Citrix die Bereitstellung von Director in einer getrennten Webdomäne.

## Konfigurieren von On-Premises-Sites mit Citrix Analytics for Performance

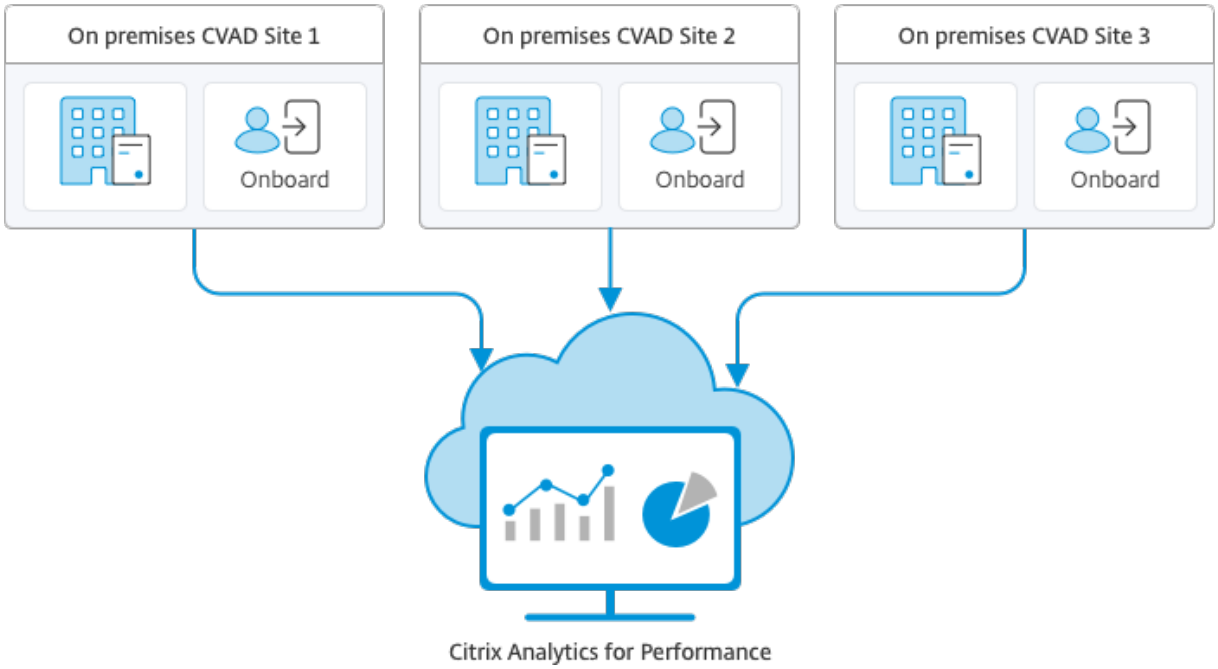
June 27, 2024

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 in **Director** auf der Registerkarte **Analytics** die On-Premises-Sites mit Citrix Analytics für Leistung konfigurieren.




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

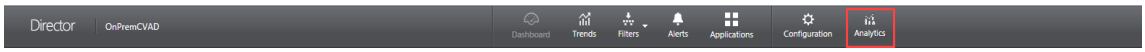
Änderungen machen. Starten Sie den Überwachungsdienst auf dem Delivery Controller neu, damit die Änderungen umgesetzt werden.

- 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.

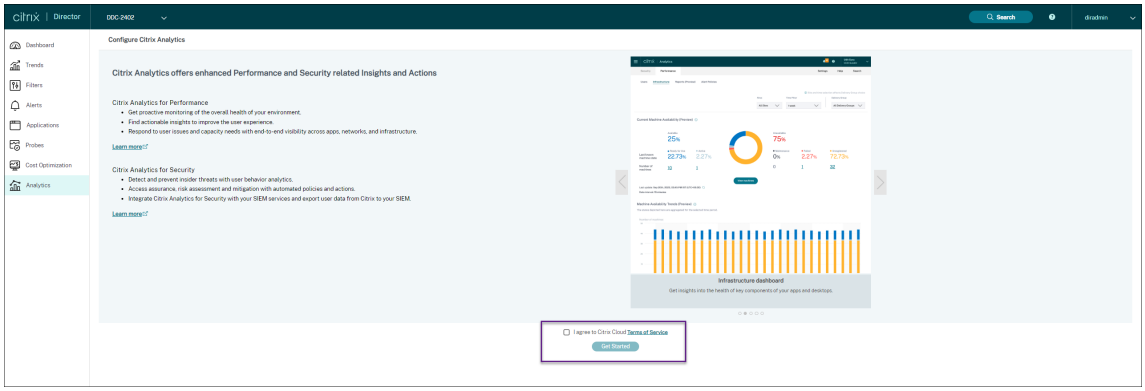
## Konfigurationsschritte

Nachdem Sie die Voraussetzungen überprüft haben, gehen Sie folgendermaßen vor:

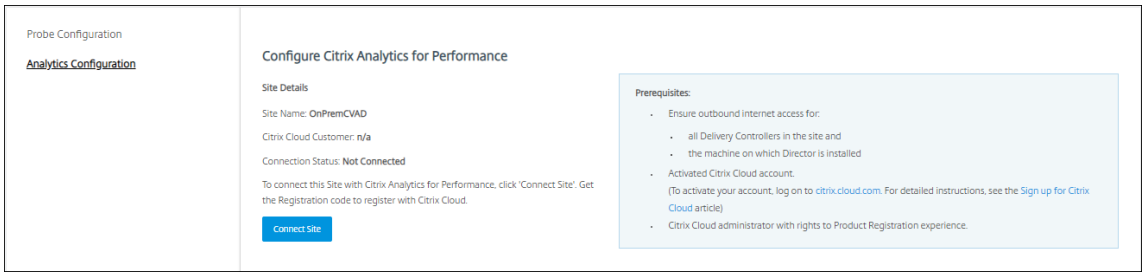
1. Melden Sie sich bei Director als Volladministrator an und wählen Sie die Site aus, für die Sie die Leistungsanalyse konfigurieren möchten. Die Director-Dashboardseite wird angezeigt.




2. Klicken Sie auf die Registerkarte **Analytics**. Die Seite **Citrix Analytics konfigurieren** wird angezeigt.



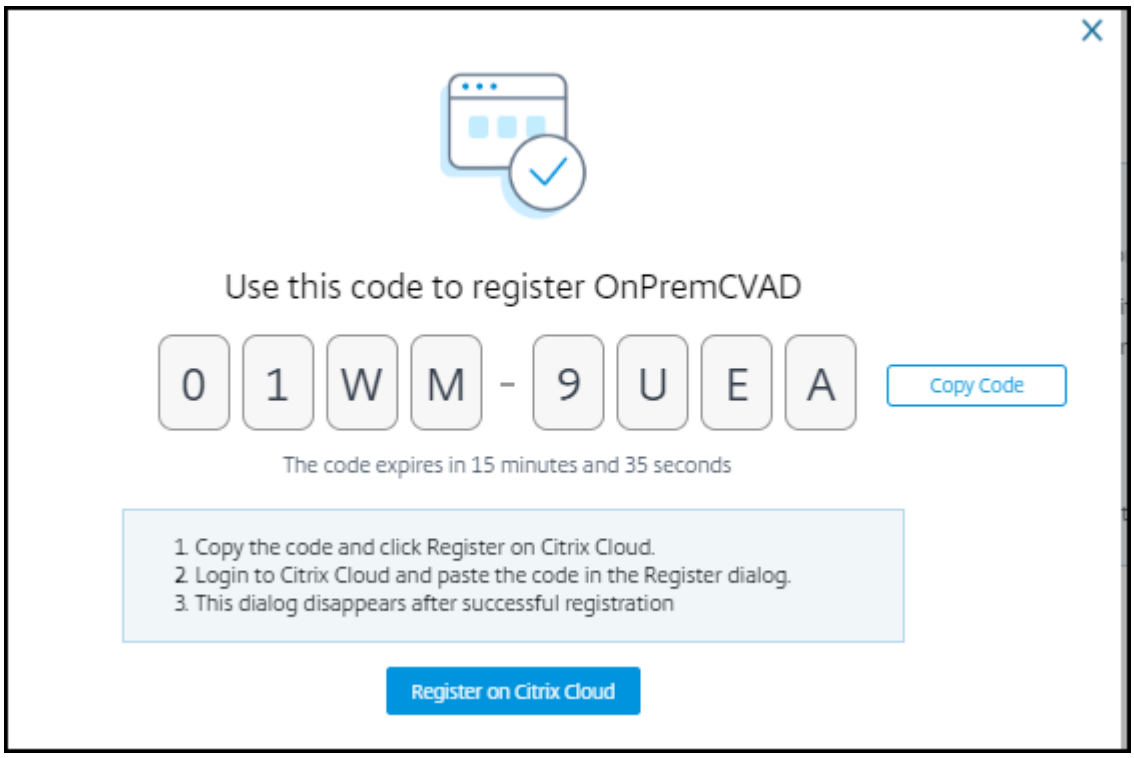

3. Lesen Sie die Anweisungen, bestätigen Sie die Nutzungsbedingungen und klicken Sie auf **Erste Schritte**. Die Seite **Details** wird angezeigt.




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.

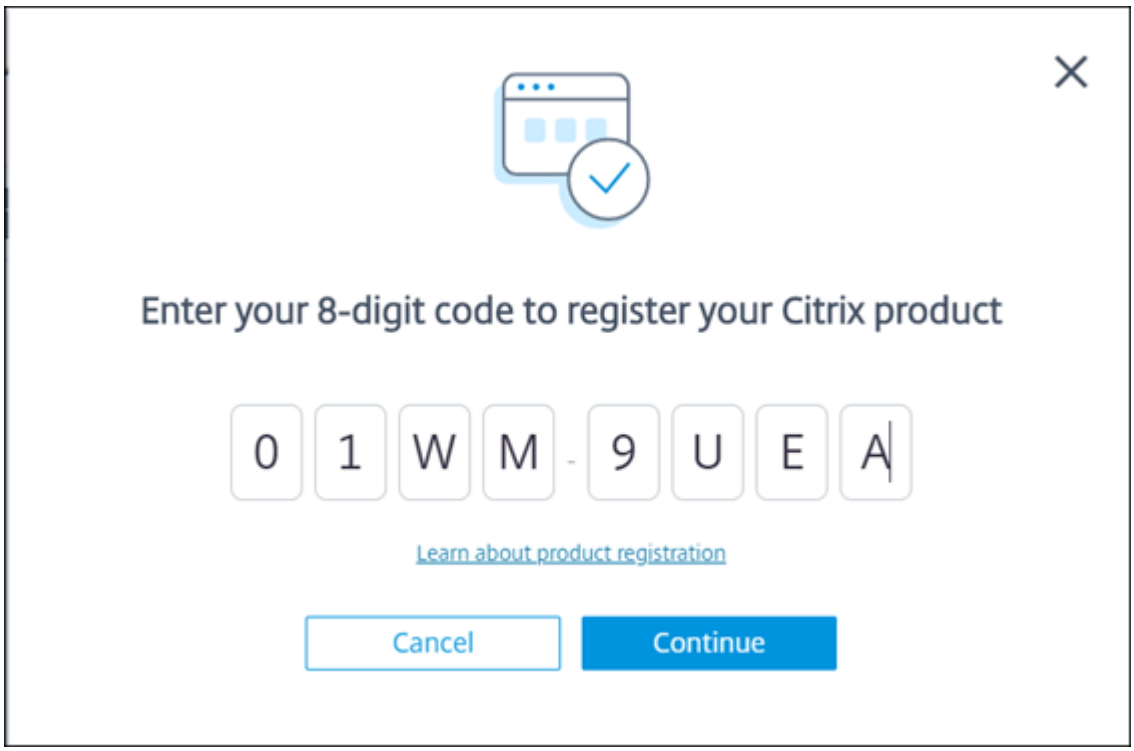
   Zur Registrierung der Site bei Citrix Cloud wird ein 8-stelliger Registrierungscode generiert.



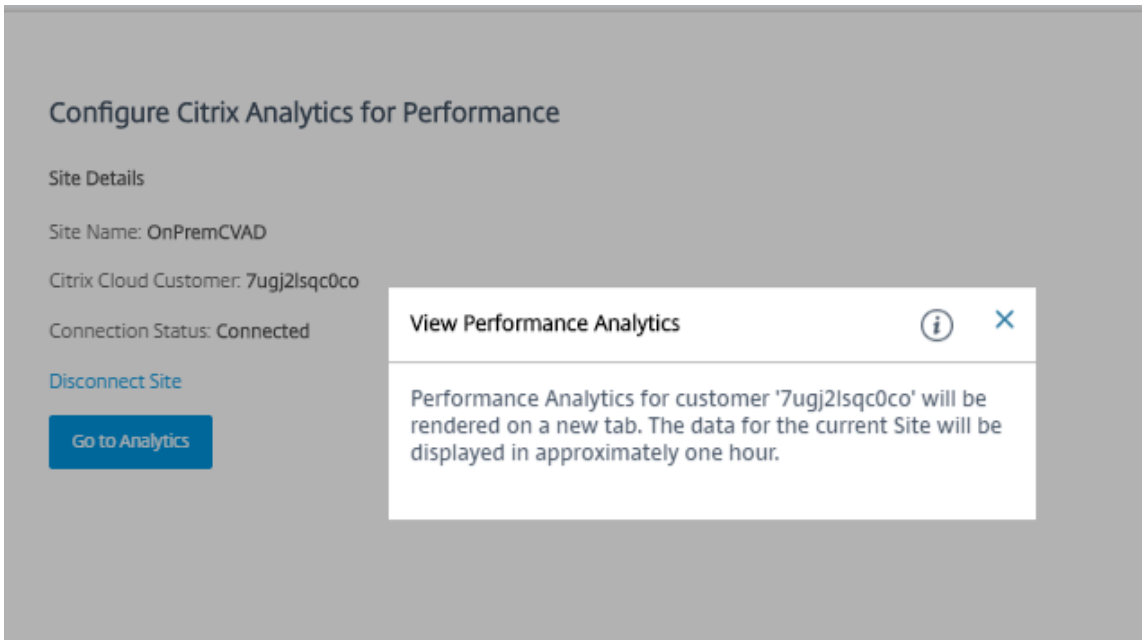

6. Klicken Sie auf **Code kopieren** und dann auf **Bei Citrix Cloud registrieren**. Sie werden zur Registrierungs-URL in Citrix Cloud weitergeleitet.
7. Melden Sie sich mit Ihren Citrix Cloud-Anmeldeinformationen an und wählen Sie Ihren Kunden aus.
8. Fügen Sie den kopierten Registrierungscode in Citrix Cloud auf der Seite "Produktregistrierungen"ein. Klicken Sie auf **Weiter**, um sich zu registrieren. Überprüfen Sie die Registrierungsdetails und klicken Sie auf **Registrieren**.



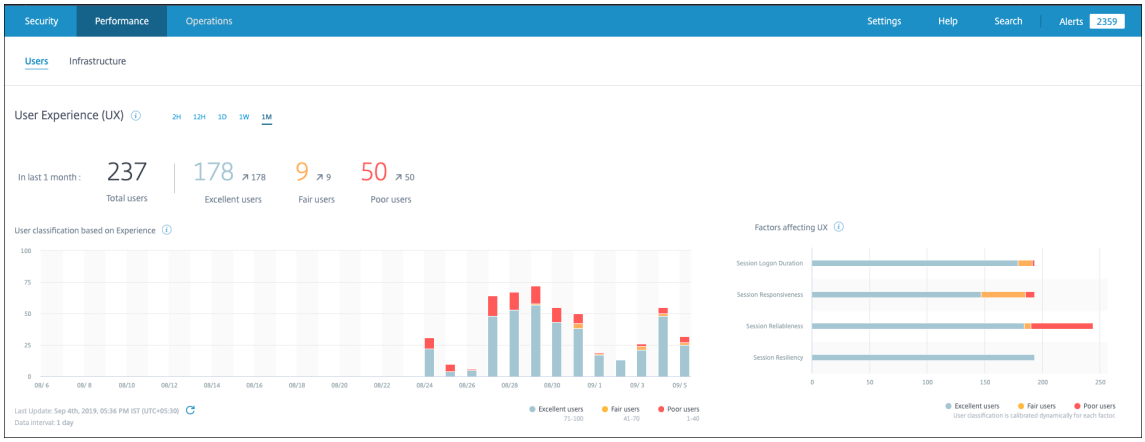

Ihre On-Premises-Site wird bei Citrix Cloud registriert.

9. Klicken Sie in **Director** auf der Registerkarte **Analytics** auf **Gehe zu Analytics**.




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.

10. 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.

    Falls mehrere Director-Instanzen mit der Site verbunden sind, nutzen Sie eine beliebige Director-Instanz zur Konfiguration. Alle übrigen Director-Instanzen werden nach der Konfiguration mit der nächsten Aktualisierung angepasst.

11. Klicken Sie auf **Site trennen**, um Ihre Site von Citrix Cloud zu trennen. Diese Option löscht die vorhandene Konfiguration.

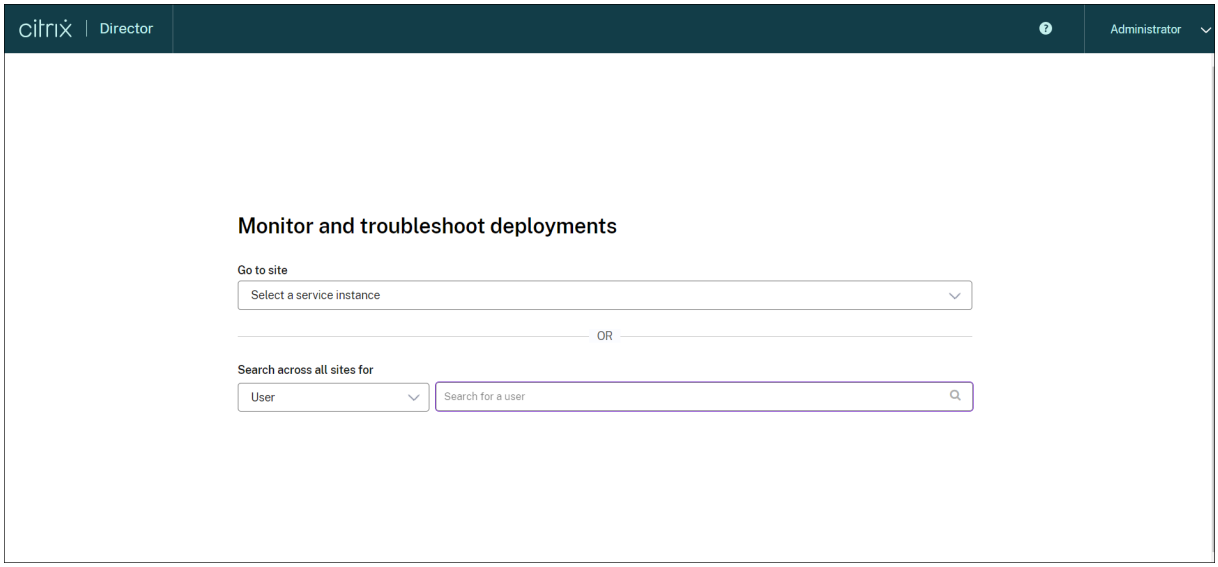
    > **Hinweise:**
    >
    > Beim ersten Konfigurieren einer Site kann die Verarbeitung der Site-Ereignisse rund eine Stunde dauern, sodass Metriken verzögert im Leistungsanalyse-Dashboard angezeigt werden. Danach werden die Ereignisse in regelmäßigen Abständen aktualisiert.
    >
    > Nach der Trennung 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

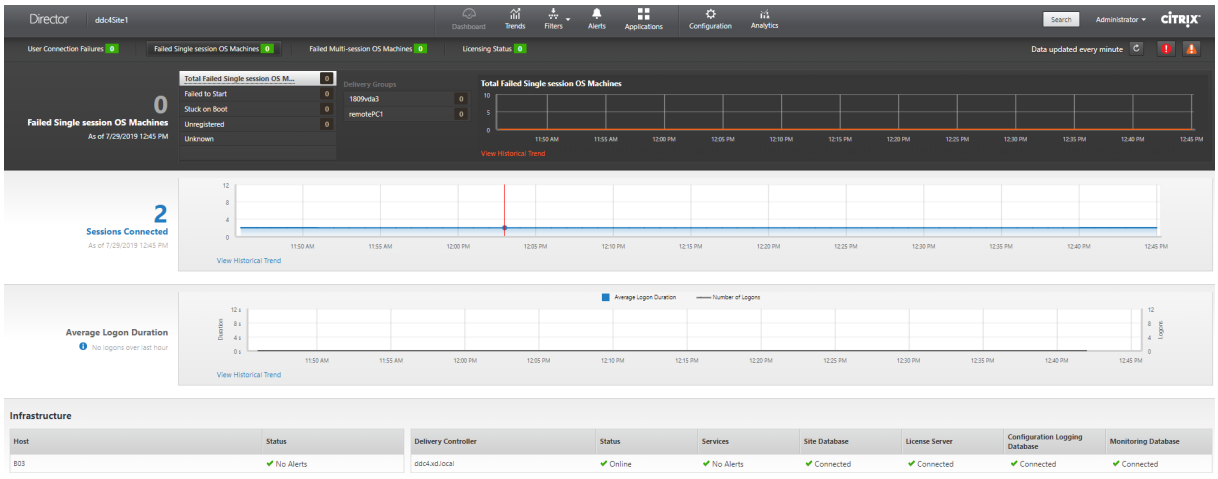
June 27, 2024

Mit Director können Sie den Zustand Ihrer Bereitstellungen überwachen. Sie können Leistungsprobleme beheben, indem Sie auf allen integrierten Sites nach einem Benutzer, Endpunkt oder einer Maschine suchen.




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 die 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.

## Bereiche im Director-Dashboard

### 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.

### 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**.

### Kulanzzeitraum

Director zeigt einen der folgenden Kulanzzeiträume an. Diese Informationen werden vom Delivery Controller abgerufen.

1. **Nicht aktiv:** Es ist kein Kulanzzeitraum aktiviert. Es gelten die normalen Lizenzbeschränkungen.
2. **Notfallkulanzzeitraum:** Dieser Kulanzzeitraum wird aktiviert, wenn der Lizenzserver nicht erreichbar ist oder die Lizenzinformationen beim Verbindungsaufbau nicht abgerufen werden können. Benutzer sind davon nicht betroffen. In Director angezeigte Fehler können erst geschlossen werden, nachdem eine Verbindung mit dem Lizenzserver hergestellt wurde.
3. **Kulanzzeitraum abgelaufen:** Notfall- oder Zusatzkulanzzeitraum sind abgelaufen.

Weitere Informationen finden Sie unter Lizenzüberziehung und Zusatzkulanzzeitraum.

#### 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.

#### Infrastruktur

Liste der zu der Siteinfrastruktur gehörigen Hosts und Controller. Auf XenServer oder VMware können für die Infrastruktur Leistungswarnungen angezeigt werden. Sie können beispielsweise XenCenter so konfigurieren, dass Warnungen zur Leistung generiert werden, wenn die CPU-, Netzwerk-E/A- oder Datenträger-E/A-Nutzung einen angegebenen Schwellenwert auf einem verwalteten Server oder einer virtuellen Maschine übersteigt. Standardmäßig ist das Warnungswiederholungsintervall 60 Minuten, Sie können jedoch auch eine andere Einstellung wählen. Weitere Informationen finden Sie im Abschnitt "XenCenter Performance Alerts"der XenServer-Produktdokumentation.

> **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 folgende Abschnitte) 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.

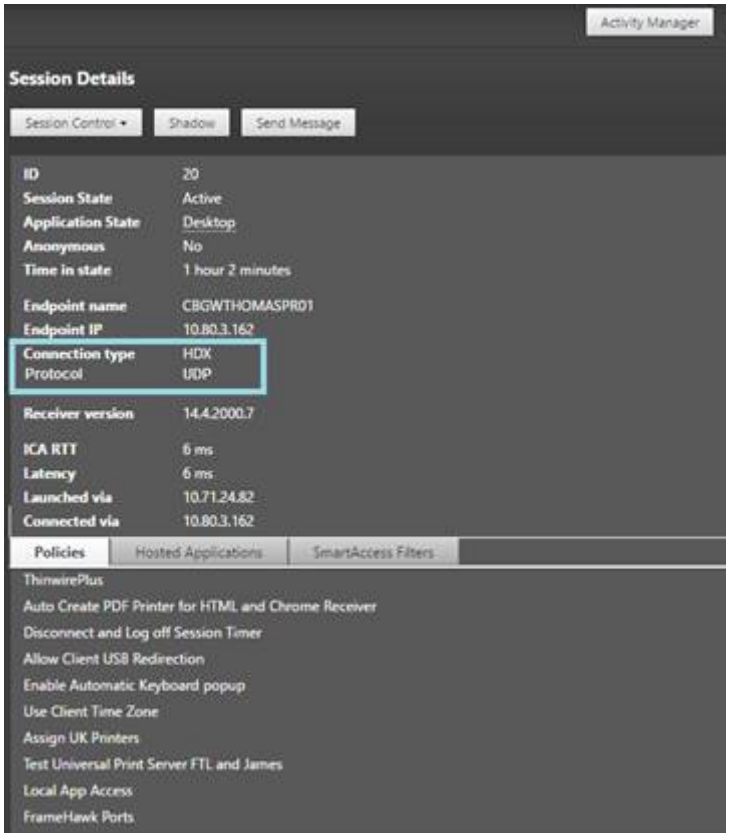
**Einschränkung für Desktopzuweisungsregeln:**
Web Studio ermöglicht die Zuordnung mehrerer Desktopzuweisungsregeln (DAR) für verschiedene Benutzer oder Benutzergruppen zu einem VDA in einer Bereitstellungsgruppe. In StoreFront wird der zugewiesene Desktop mit dem zugehörigen **Anzeigenamen** gemäß den Desktopzuordnungsregeln 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.

So exportieren Sie einen Bericht:

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 | 5.000 |
| [Excel] | 100.000 | UI.ExportExcelDrilldownLimit | 1.000.000 |
| 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 |
| --- | --- |
| **Neu starten** | 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 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. |
| **Anhalten** | 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. |
| **Fortsetzen** | 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 nicht verfügbar ist. Es können keine neuen Verbindungen hergestellt werden, bis der Wartungsmodus deaktiviert wird.

### Anwendungsanalyse

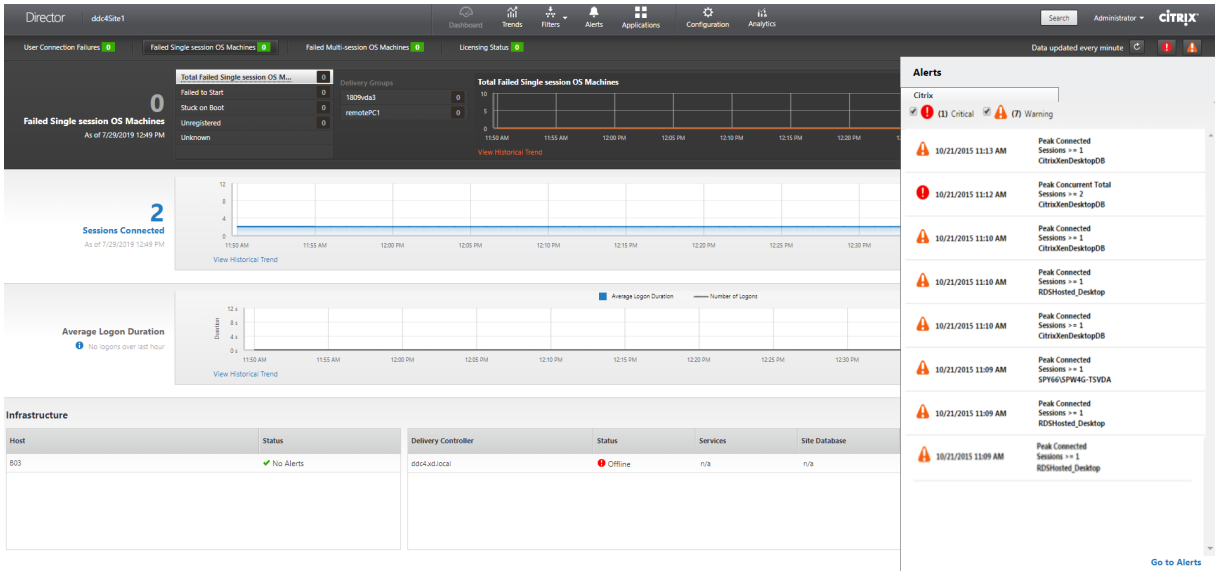
Auf der Registerkarte **Anwendungen** werden konsolidierte Anwendungsdaten zur effizienten Analyse und Verwaltung der Anwendungsleistung angezeigt. Sie erhalten hier wertvolle Einblicke in die Integrität und Nutzung aller in der Site veröffentlichten Anwendungen. Die Ansicht enthält Anwendungstestergebnisse, 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

June 27, 2024

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.

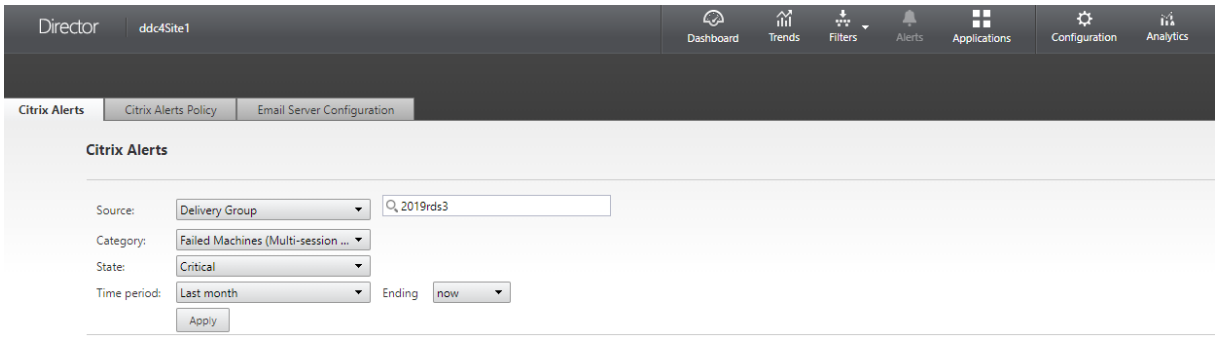



Eine Warnung (gelbes Dreieck) zeigt an, dass der Schwellenwert einer Bedingung erreicht oder überschritten wurde.

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.

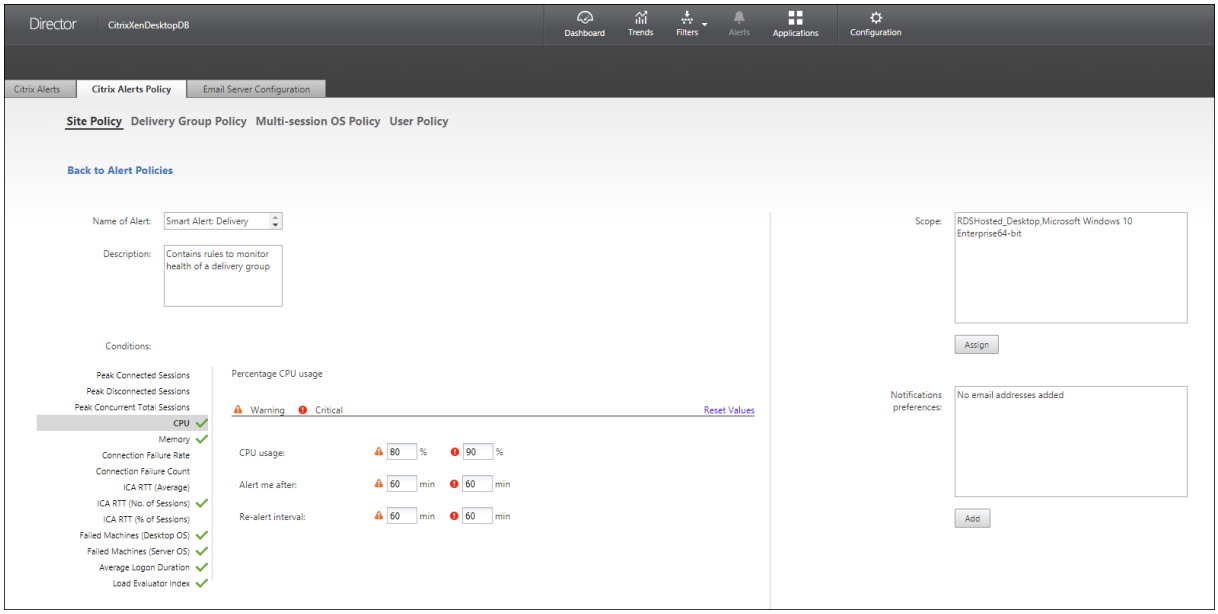
> **Hinweis:**
>
> Stellen Sie sicher, dass die Firewall, der Proxy und Microsoft Exchange Server die E-Mail-Benachrichtigungen nicht blockiert.

## 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.

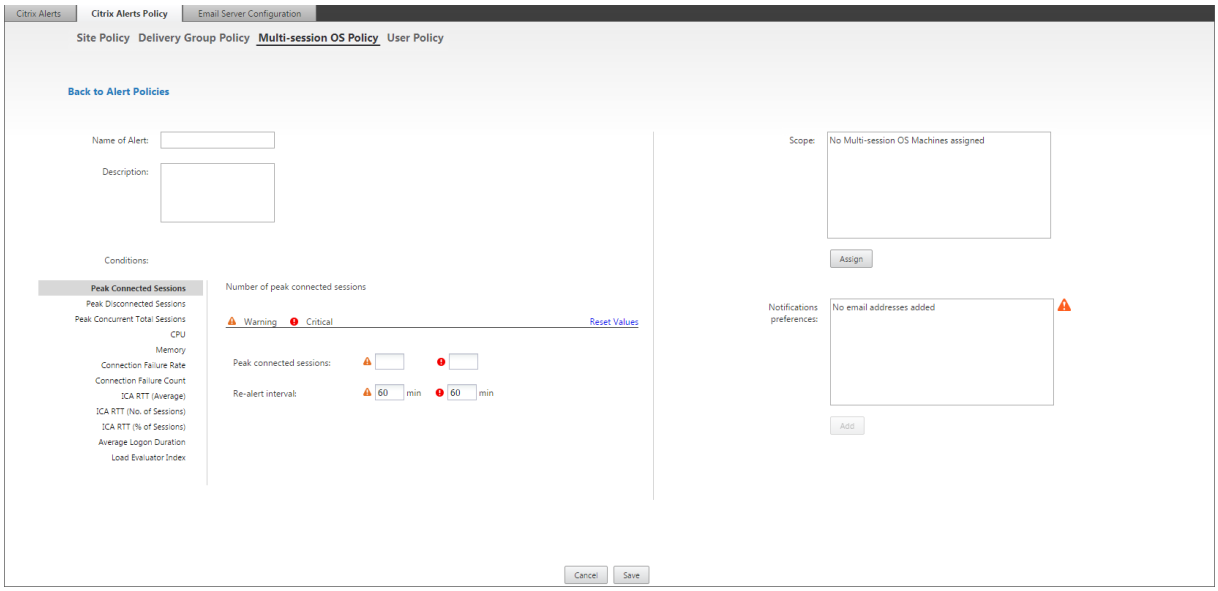
Wenn Sie Director und Ihre Site aktualisieren, werden die Benachrichtigungsrichtlinien der älteren Director-Instanz übernommen. Integrierte Benachrichtigungsrichtlinien werden nur erstellt, wenn die Überwachungsdatenbank keine entsprechenden Warnmeldungsregeln enthält.

Informationen zu den Schwellenwerten der integrierten Benachrichtigungsrichtlinien finden Sie unter Bedingungen für Benachrichtigungsrichtlinien.



## 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 Benachrichtigungsrichtlinien 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.

> **Hinweis:**
> Wenn Sie eine Warnmeldungsrichtlinie löschen, kann es bis zu 30 Minuten dauern, bis die Richtlinie aufhört, Warnmeldungen zu generieren.

## 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 zu 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 zu 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 zu 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.

  **Bedingungen für intelligente Benachrichtigungsrichtlinien:**

  - **Bereich:** Bereitstellungsgruppe, Multisitzungs-OS
  - **Schwellenwerte:** Warnung - 1, Kritisch - 2

**Fehlerhafte Maschinen (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

**Fehlerhafte Maschinen (%)**

Prozentsatz fehlerhafter Maschinen für Einzel- und Multisitzungs-OS in einer Bereitstellungsgruppe, basierend auf der Anzahl fehlerhafter Maschinen. Der Wert wird alle 30 Sekunden berechnet und erlaubt das Konfigurieren von Schwellenwerten für Warnungen als Prozentsatz fehlerhafter Maschinen in einer Bereitstellungsgruppe.
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.

**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.

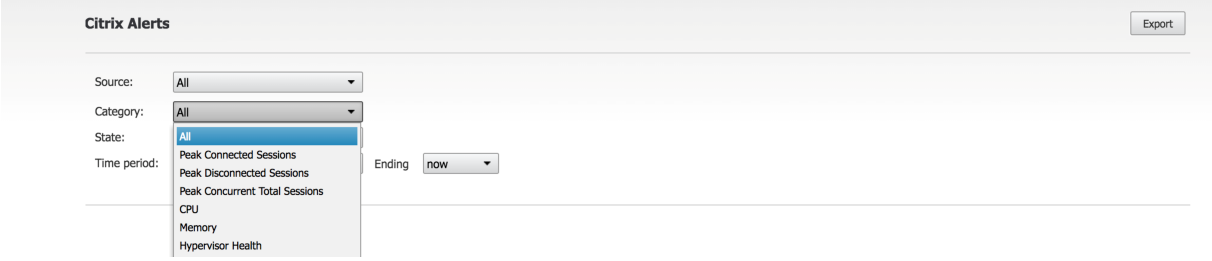
- Suchen Sie in Director nach Maschinen mit Multisitzungs-OS, die mit Spitzenlast ausgeführt werden. Zeigen Sie das Dashboard (Fehler) und die Trendansicht für den Lastauswertungsprogrammindex an.

  **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 XenServer 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.

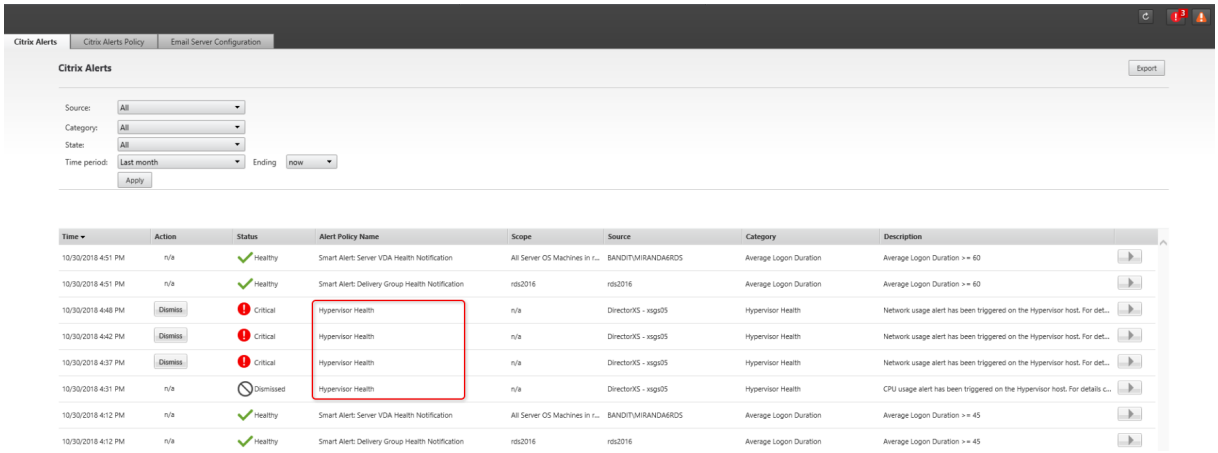



Um Hypervisorwarnungen zu erhalten, muss in Web Studio eine Hostingverbindung erstellt werden. Weitere Informationen finden Sie unter Verbindungen und Ressourcen. Nur diese Verbindungen werden auf Hypervisorwarnungen überwacht.

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.

In der folgenden Tabelle werden die verschiedenen Parameter und Zustände von Hypervisorwarnungen beschrieben.

| Warnung | Unterstützte Hypervisors | Ausgelöst durch | Bedingung | Konfiguration |
|---|---|---|---|---|
| CPU-Nutzung | XenServer, VMware vSphere | Hypervisor | Schwellenwert der CPU-Auslastung erreicht oder überschritten | Warnschwellenwerte müssen im Hypervisor konfiguriert werden. |
| Speichernutzung | XenServer, VMware vSphere | Hypervisor | Schwellenwert der Speicherauslastung erreicht oder überschritten | Warnschwellenwerte müssen im Hypervisor konfiguriert werden. |
| Netzwerknutzung | XenServer, 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 | XenServer, 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. Sie können die Warnung deaktivieren, wenn Ihre Rolle keine Infrastrukturüberwachung beinhaltet.

> **Wichtig:**
>
> - Vom Hypervisor ausgelöste Warnungen werden abgerufen und in Director angezeigt. Än-

> derungen im Lebenszyklus/Status der Hypervisorwarnungen werden jedoch nicht in Director 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.

## Filtern von Daten zur Problembehandlung

June 27, 2024

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. Klicken Sie auf **Zugeordneter Benutzer**, um den Aktivitätsmanager für den Benutzer zu öffnen. Wenn Sie auf den **Endpunktnamen** klicken, wird der Aktivitätsmanager für den Endpunkt geöffnet. Wenn Sie auf **Details anzeigen** klicken, wird die Seite **Benutzerdetails** bzw. **Endpunktdetails** geöffnet. Weitere Informationen finden Sie unter Benutzerdetails.
   - **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 zum Konfigurieren **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 unter Citrix Director failure reasons and troubleshooting.
11. Klicken Sie in der Ansicht **Maschinen** auf den 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, Datenträgerüberwachung 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:**
> Web Studio ermöglicht die Zuordnung mehrerer Desktopzuweisungsregeln (DAR) für verschiedene Benutzer oder Benutzergruppen zu einem VDA in einer Bereitstellungsgruppe. In StoreFront wird der zugewiesene Desktop mit dem zugehörigen Anzeigenamen gemäß den Desktopzuordnungsregeln 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

June 27, 2024

In der Ansicht “Trends”werden historische Trendinformationen der einzelnen Sites für die folgenden Parameter angezeigt:

- Sitzungen
- Verbindungsfehler
- Maschinenfehler
- Anmeldungsleistung
- Lastauswertung
- Kapazitätsverwaltung

- Maschinennutzung
- Ressourcenauslastung
- Netzwerkanalyse für jede Site

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 besser verstehen.

Wenden Sie einen anderen Filter auf die Daten an, um den Standardgeltungsbereich der einzelnen Diagramme zu ändern.

Wählen Sie den Zeitraum, für den Sie historische Trendinformationen benötigen. Welche Zeiträume verfügbar sind, hängt von der 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. Für den Zeitraum "Letzter Monat"mit einem benutzerdefinierten Enddatum oder "Letztes Jahr"werden die Trendinformationen nur in Form von Diagrammen angezeigt, nicht als Tabellen.
> - 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 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 |

| Parameter | Standardwerte |
| --- | --- |
| 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. Es analysiert auch Netzwerke mit einer nahtlosen 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 Citrix Gateway-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 die 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 **Nutzung gehosteter Anwendungen** aus. Wählen Sie die Bereitstellungsgruppe und den Zeitraum aus, um ein Diagramm 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.

**Nutzung virtueller Maschinen anzeigen:** Wählen Sie auf der Registerkarte **Maschinennutzung** die Option **Maschinen mit Einzelsitzungs-OS oder Maschinen mit Multisitzungs-OS**, 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. Diese Datensammlung kann über die Richtlinieneinstellung **Ressourcenüberwachung aktivieren** deaktiviert werden. Die Tabelle unterhalb der Diagrammen enthält die Ressourcenauslastung pro Maschine. Weitere Informationen finden Sie unter Einstellungen der Überwachungsrichtlinie.
> - 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.)
> - Der Maschinendrilldown listet Prozesse mit durchschnittlicher CPU- oder Arbeitsspeichernutzung über 1 % auf, was bedeutet, dass manchmal weniger als 10 Prozesse aufgelistet werden.

**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.

**Testergebnisse anzeigen:** Auf der Registerkarte **Testergebnisse** werden die Ergebnisse von Anwendungs- und Desktoptests angezeigt, die auf der Seite "Konfiguration"konfiguriert wurden. Hier wird die Startphase angegeben, während der ein Fehler auftrat.

Weitere Informationen finden Sie unter Anwendungs- und Desktoptests.

**Erstellen benutzerdefinierter Berichte:** Über die Registerkarte "Benutzerdefinierte Berichte"können benutzerdefinierte Berichte mit Echtzeit- und historischen Daten aus der Überwachungsdatenbank in tabellarischer Form erstellt werden.

Für dieses Feature sind Director und Delivery Controller ab **Version 7.12** erforderlich.

Von der Liste der benutzerdefinierten Berichtsabfragen aus können Sie auf **Ausführen 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 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 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.

## Mit Autoscale verwaltete Maschinen überwachen

June 27, 2024

Autoscale ermöglicht die proaktive Energieverwaltung aller registrierten Maschinen mit Multisitzungs-OS und Einzelsitzungs-OS in einer Bereitstellungsgruppe. Sie können Autoscale für eine ausgewählte Bereitstellungsgruppe in Web Studio konfigurieren. Weitere Informationen finden Sie unter Autoscale.
Sie können wichtige Kennzahlen mit Autoscale verwalteter Maschinen über Director überwachen.

### Maschinennutzung

Auf der Seite **Maschinennutzung** wird die Gesamtzahl der mit Autoscale verwalteten Maschinen mit Multisitzungs-OS und Einzelsitzungs-OS angezeigt, die für eine ausgewählte Bereitstellungsgruppe und eine bestimmte Zeitdauer eingeschaltet sind. Diese Kennzahl gibt die derzeitige Maschinennutzung in der Bereitstellungsgruppe an.
Wählen Sie auf der Registerkarte **Einzelsitzungs-OS-Maschinen**oder **Maschinen mit Multisitzungs-OS** die Bereitstellungsgruppe und den Zeitraum aus.

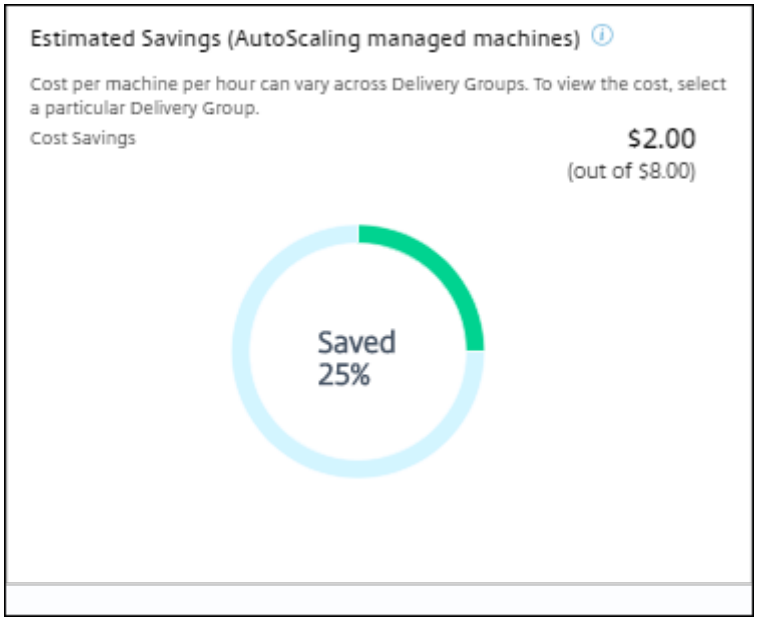
Im Diagramm werden folgende Kennzahlen dargestellt:

- **Eingeschaltete Maschinen** - Anzahl der mit Autoscale verwalteten Maschinen, die eingeschaltet sind
- **Registrierte Maschinen** - Anzahl der registrierten Maschinen mit Multisitzungs-OS und Einzelsitzungs-OS
- **Maschinen in Wartung** - Anzahl der Maschinen mit Multisitzungs-OS und Einzelsitzungs-OS im Wartungsmodus.

### Geschätzte Einsparungen

Auf der Seite **Maschinenauslastung** werden auch die geschätzten Kosteneinsparungen angezeigt, die durch Aktivieren von Autoscale in der ausgewählten Bereitstellungsgruppe erzielt wurden.




Die Einsparungen werden als Prozentsatz der Einsparungen pro Maschine und Stunde (in US-Dollar) berechnet, die unter **Bereitstellungsgruppe bearbeiten** > **Autoscale** konfiguriert wurden. Weitere Informationen zum Konfigurieren der Einsparungen pro Maschine finden Sie unter Autoscale.

Wenn Sie alle Bereitstellungsgruppen auswählen, wird der Durchschnittswert der geschätzten Einsparungen für alle Bereitstellungsgruppen angezeigt.

Anhand der geschätzten Einsparungen können Administratoren die Infrastruktur konsolidieren und Kapazität mit dem Ziel maximaler Einsparungen und Auslastung planen.

### Warnmeldungsbenachrichtigungen für Maschinen und Sitzungen

Auf dem Director-Dashboard werden Warnmeldungen angezeigt, für die weitere Details aufgerufen werden können. Details zu Warnmeldungen werden auf der Seite **Warnungen** angezeigt.

- Um eine Warnrichtlinie für eine Bereitstellungsgruppe zu erstellen, gehen Sie zu **Warnungen** > **Citrix Benachrichtigungsrichtlinie** > **Bereitstellungsgruppenrichtlinie**.
- Hier können Sie die folgenden Warnungen und Schwellenwerte festlegen:
  - Fehlgeschlagene Maschinen (Einzelsitzungs-OS) und fehlgeschlagene Maschinen (Multisitzungs-OS),
  - Max. verbundener Sitzungen, max. getrennter Sitzungen und Max. gleichzeitiger Sitzungen insgesamt in der Bereitstellungsgruppe.
- Warnungen werden generiert, wenn der entsprechende Parameter in der Bereitstellungsgruppe den Schwellenwert erreicht.

For more details regarding the alert policy conditions and creation of new alert policies, see Alerts and notifications.

### Maschinenstatus

- Über **Filter** > **Maschinen** wird der Energiezustand aller Maschinen in einem tabellarischen Format angezeigt. Sie können die Anzeige nach Bereitstellungsgruppen filtern.
- Über **Filter** > **Sitzungen** werden die Maschinen zugeordneten Sitzungen und deren Echtzeitstatus angezeigt.
- Wählen Sie unter **Trends** > **Sitzungen** die Bereitstellungsgruppe und den Zeitraum aus, um den Trend der Sitzungen und die zugehörigen Kennzahlen anzuzeigen.

Weitere Informationen finden Sie unter Filtern von Daten bei der Problembehandlung.

### Lastauswertungstrends

Auf der Seite **Trends** > **Lastauswertung** wird ein Diagramm angezeigt, das ausführliche Informationen zu der auf die Multisitzungs-OS-Maschinen verteilten Last bietet. 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. Der Lastauswertungsindex wird als Prozentsatz von CPU gesamt, Speicher, Datenträger oder Sitzungen dargestellt und zwar im Vergleich mit der Zahl der verbundenen Benutzer im letzten Intervall.

## Problembehandlung bei Bereitstellungen

June 27, 2024

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.

Verfügbare Aktionen:

- Beenden von Anwendung und Prozessen, die nicht mehr reagieren
- Spiegeln von Vorgängen auf Benutzermaschinen
- Abmelden nicht reagierender Sitzungen
- Neustarten von Maschinen

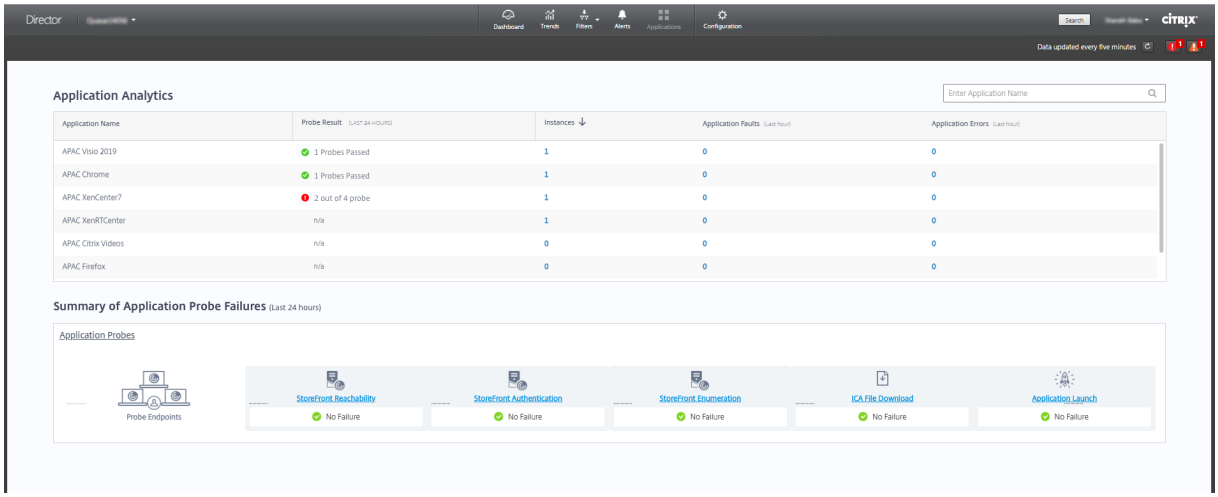
- Versetzen der Maschine in den Wartungsmodus
- Zurücksetzen des Benutzerprofils

# Problembehandlung bei Anwendungen

June 27, 2024

## 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 Anwendungs- und Desktoptests.

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 ihrer Bearbeitung finden Sie im Artikel Einstellungen der Überwachungsrichtlinie unter **Richtlinien für die Überwachung auf Anwendungsfehler**.

### 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.

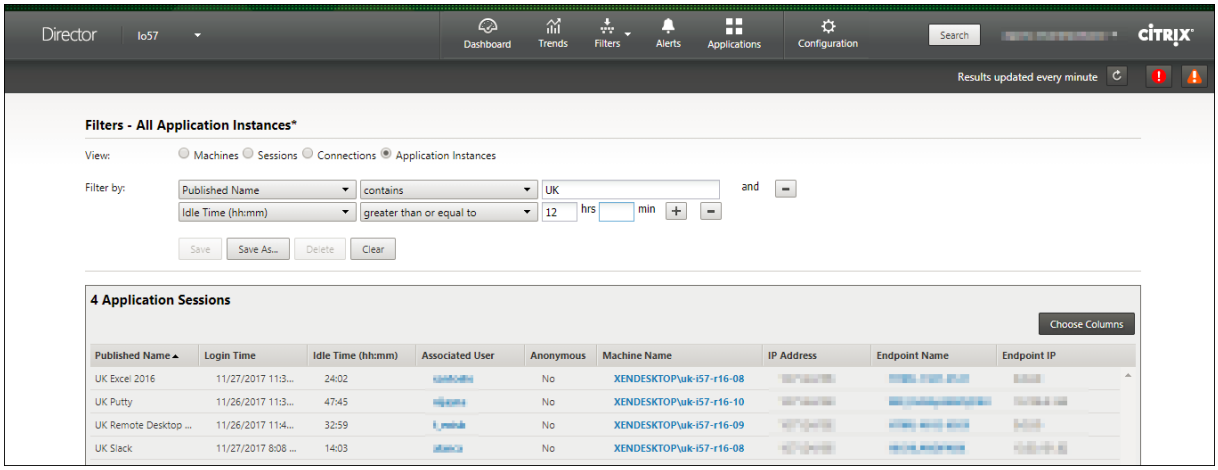
Typische Einsatzbereiche für die Problembehandlung bei Anwendungen ist der Gesundheitssektor, wo Mitarbeiter Anwendungslizenzen gemeinsam verwenden. Sie müssen dort Sitzungen und Anwendungsinstanzen im Leerlauf beenden, um die Citrix Virtual Apps and Desktops-Umgebung zu bereinigen, Server mit schlechter 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.

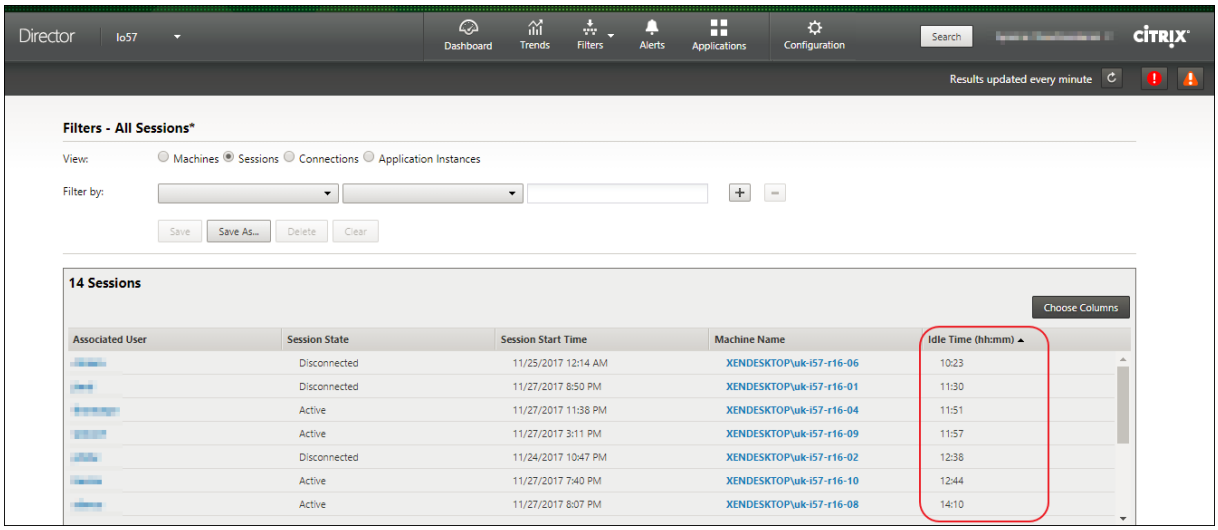
 




Beispiel für einen Filter: Wählen Sie für **Filtern nach** die Kriterien **Veröffentlichter Name** (der Anwendung) und **Leerlaufzeit**. Legen Sie für **Leerlaufzeit** unter **größer als oder gleich** ein Zeitlimit fest und speichern Sie den Filter. Wählen Sie aus der gefilterten Liste die Anwendungsinstanzen 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

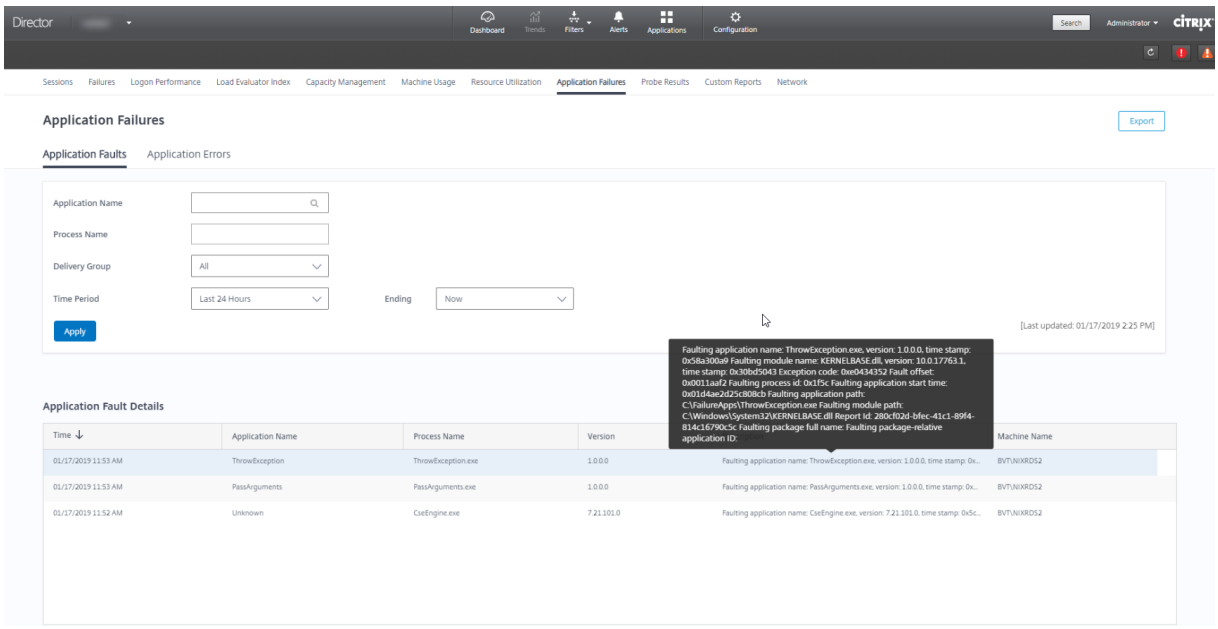
## Überwachen historischer Anwendungsstörungen

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.

## 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 Verbindungsfehlern sowie empfohlene Korrekturmaßnahmen finden Sie unter Citrix Director failure reasons and troubleshooting.

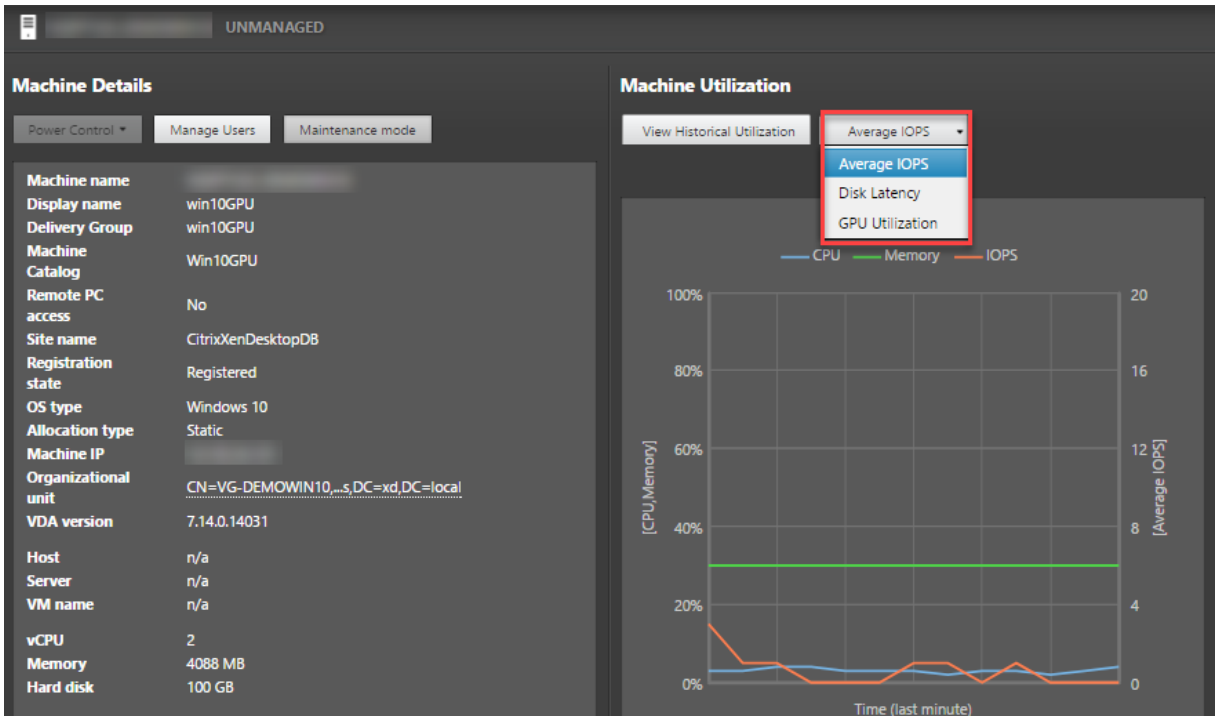
Klicken Sie auf Link mit dem Maschinennamen, um die Seite **Maschinendetails** aufzurufen.

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 Controllern 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.



### GPU-Auslastung

Über **GPU-Auslastung** können Sie die prozentuale Auslastung von GPU, GPU-Speicher und Encoder sowie Decoder aufrufen und anhand dieser Informationen GPU-Probleme auf Multisitzungs-OS- oder Einzelsitzungs-OS-VDAs behandeln.

**Unterstützte GPU-Versionen:**

- NVIDIA Tesla M60-GPUs mit Display Driver Version 369.17 oder höher. Weitere Informationen finden Sie unter NVIDIA vGPU Software.
- AMD Radeon Instinct MI25-GPUs und AMD EPYC 7V12-CPUs (Rom). Weitere Informationen finden Sie unter AMD Drivers and Support.

**Treiber:**

Die entsprechenden Treiber oder Erweiterungen müssen auf den VDAs installiert sein.

- Installieren Sie für NVIDIA-GPUs die GRID-Treiber manuell oder über Erweiterungen. Weitere Informationen finden Sie unter NVIDIA vGPU Software.
  - Beachten Sie, dass für NVIDIA nur GRID-Treiber unterstützt werden. CUDA-Treiber funktionieren nicht mit der NVadsA10 v5-Serie und werden nicht unterstützt.
  - Ein Beispielverfahren für die Installation von Nvidia Grid GPU-Treibern über Erweiterungen auf Azure-basierten Maschinen finden Sie unter NVIDIA GRID drivers. NVIDIA GPU Driver Extension - Azure Windows VMs - Azure Virtual Machines.
  - Ein Beispielverfahren für die manuelle Installation von Nvidia Grid GPU-Treibern finden Sie unter Azure N-series NVIDIA GPU driver setup for Windows - Azure Virtual Machines.
- Installieren Sie für AMD-GPUs AMD-Grafiktreiber manuell oder über Erweiterungen. Weitere Informationen finden Sie unter AMD Drivers and Support.
  - Ein Beispielverfahren für die Installation von AMD GPU-Treibern über Erweiterungen auf Azure-basierten Maschinen finden Sie unter AMD GPU Driver Extension - Azure Windows VMs - Azure Virtual Machines.
  - Ein Beispielverfahren für die manuelle Installation von AMD GPU-Treibern auf Azure-Maschinen finden Sie unter Install AMD GPU drivers on N-series VMs running Windows.

**Hinweise zur Verwendung:**

- Die GPU-Auslastungsdiagramme sind nur für VDAs verfügbar, auf denen 64-Bit-Windows ausgeführt wird.
- 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.
- Für AMD werden Encoder und Decoder nicht getrennt unterstützt. Jede Codierungs- und Decodierungsworkload, die die GPU verwendet, wird als allgemeine 3D-Last der GPU-Workload gemeldet.
- Stellen Sie sicher, dass Sie NVIDIA WMI während der Installation installieren. Dieses Fenster ist nur während der manuellen Installation verfügbar.
- Wenn Treiber installiert sind, Director die GPU jedoch nicht erkennt
  - Sehen Sie im Task-Manager nach. Wenn die Treiber ordnungsgemäß installiert sind, sollte die GPU im Task-Manager angezeigt werden.
  - Prüfen Sie, ob die Maschine registriert ist. Manchmal kann es einige Zeit dauern, bis Maschinen als online erkannt werden.
- Wenn die GPU-Auslastung in Director keine Aktivität anzeigt, vergewissern Sie sich, dass die von Ihnen ausgeführte Workload die GPU verwendet. Für Grafikworkloads können Sie über "Einstellungen > System > Anzeige > Grafikeinstellungen > App auswählen"die Präferenz festlegen. Stellen Sie sicher, dass "High Performance"aktiviert ist. Manchmal verwendet Windows standardmäßig die CPU für Grafikworkloads, wenn auf der Grundlage anderer Einstellungen der Systemstandard oder Energiesparen eingestellt ist.
- Die Daten werden jede Minute aktualisiert und die Datenvisualisierung beginnt innerhalb einer Minute nach der Auswahl der **GPU-Auslastung**.

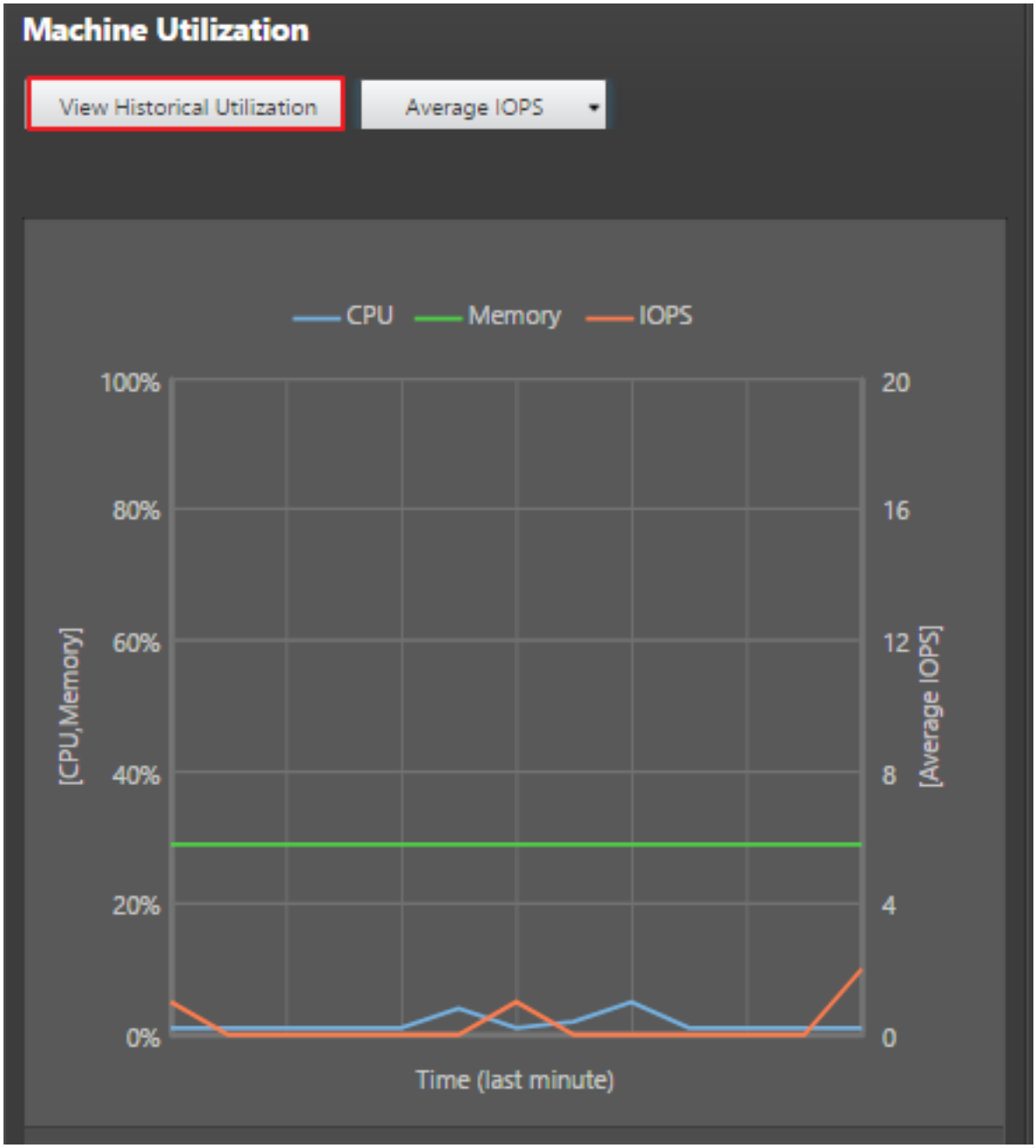
### Historische Ressourcennutzung auf Maschinen

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.



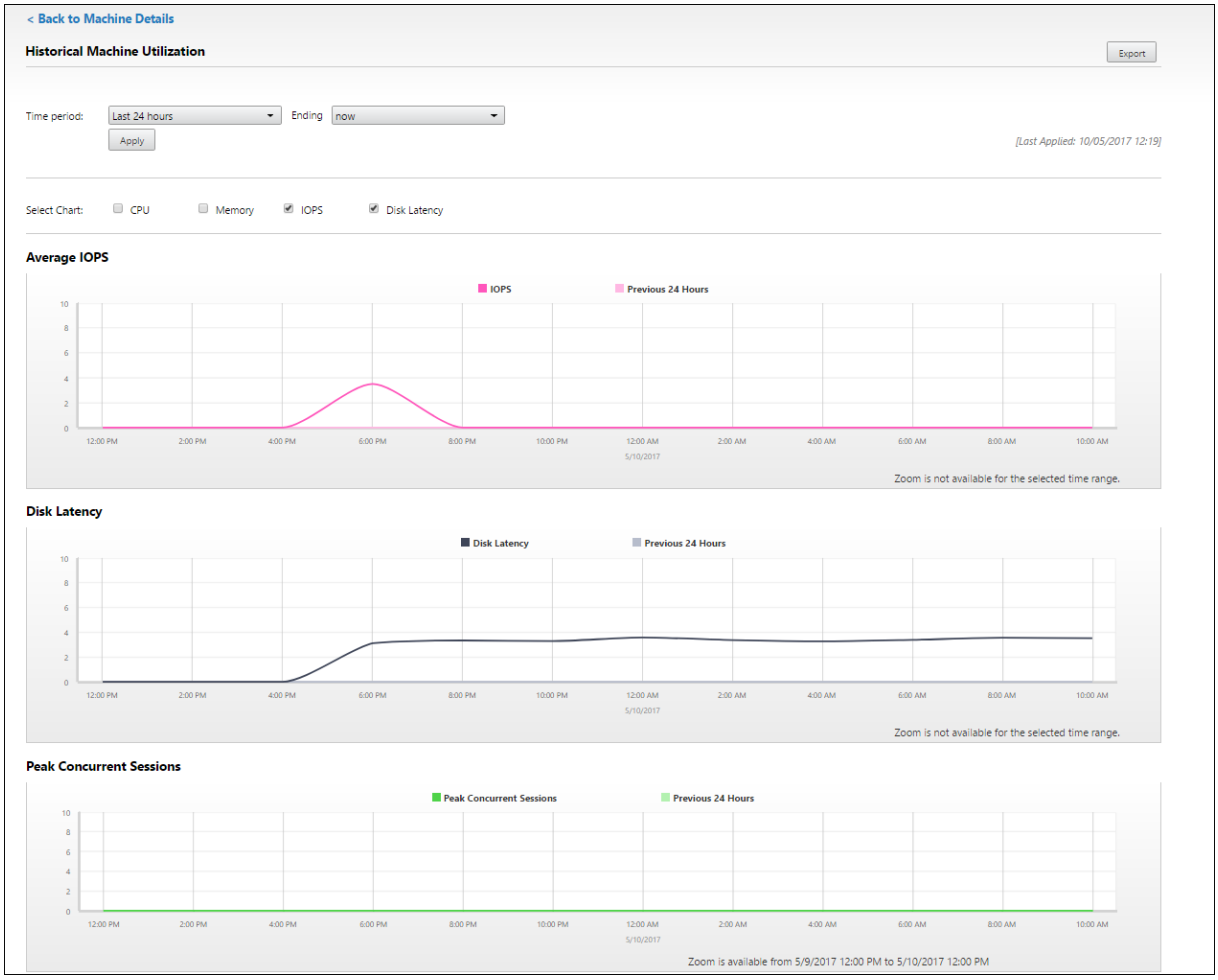

1. Wählen Sie im Bereich **Maschinenauslastung** der Ansicht **Maschinendetails** die Option **Historische Auslastung anzeigen**.
2. Legen Sie auf der Seite **Historische Maschinenauslastung** die Option **Zeitraum** auf die letzten 2 oder 24 Stunden, auf die letzten 7 Tage, den letzten Monat oder das letzte Jahr fest.

> **Hinweis:**
>
> IOPS-Durchschnitt und Datenträgerlatenz sind 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.

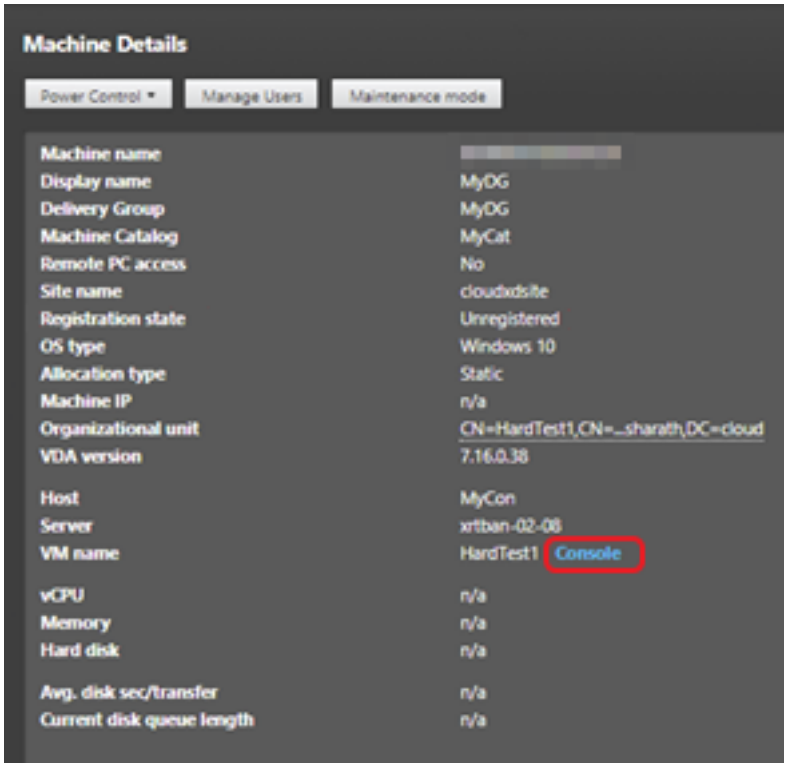
> **Hinweis:**
>
> Die Sitzungs-ID für Systemprozesse wird mit "0000"angegeben.

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”kann 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).

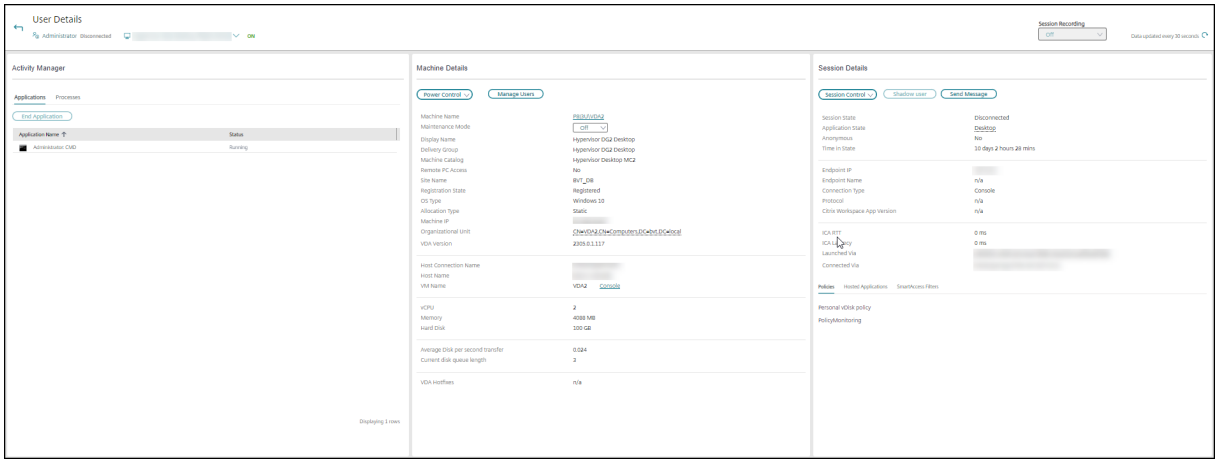
 

# Behandeln von Benutzerproblemen

June 27, 2024

In der Ansicht **Helpdesk** (Seite **Aktivitätsmanager**) in Director zeigen Sie Informationen über den Benutzer oder die Sitzung an:


Wenn Sie im Aktivitätsmanager für einen Benutzer auf **Details anzeigen** klicken, wird die Seite **Benutzerdetails** geöffnet.
Wenn Sie im Aktivitätsmanager für Endpunkte auf **Details anzeigen** klicken, wird die Seite **Endpunktdetails** geöffnet.




## Sitzungsauswahl

Wenn der Benutzer mehrere Sitzungen gestartet hat, hilft die Sitzungsauswahl bei der Auswahl einer Sitzung.


Wählen Sie eine Sitzung aus, um die Details anzuzeigen.

- Überprüfen Sie die Details zur Sitzung, zur Anmeldung des Benutzers, zum Sitzungsstart, zur Verbindung und zu den Anwendungen.
- Sie können die Maschine des Benutzers spiegeln.
- Zeichnen Sie die ICA-Sitzung auf.

### Microsoft Teams-Optimierungsstatus

Director zeigt den Microsoft Teams-Optimierungsstatus für HDX-Sitzungen auf der Seite **Benutzerdetails** im Bereich **Sitzungsdetails** im Feld **MS Teams-Optimierung** an. Die Optimierung von Microsoft Teams ist entscheidend für eine bessere Benutzererfahrung, z. B. für klares Audio und Video. Aufgrund der Sichtbarkeit des Optimierungsstatus von Microsoft Teams kann der Zeitaufwand für die Lösung von Tickets reduziert werden und Administratoren können damit wichtige Kennzahlen bei der Problembehandlung identifizieren.

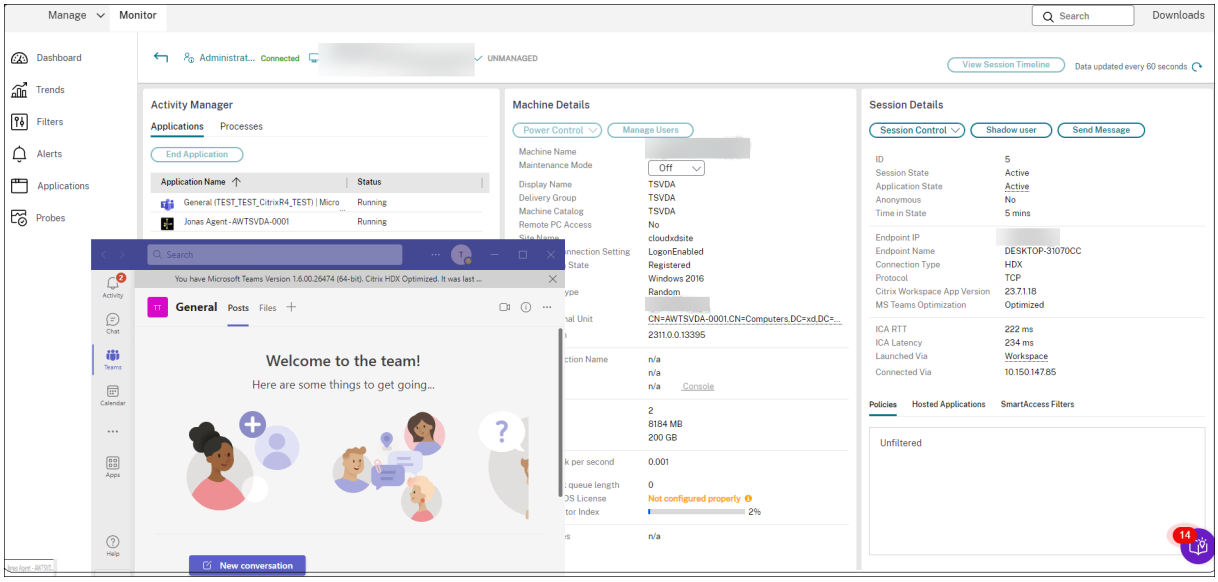
> **Hinweis:**
>
> Citrix Director unterstützt Microsoft Teams Version 2.1 oder früher.

Voraussetzungen:

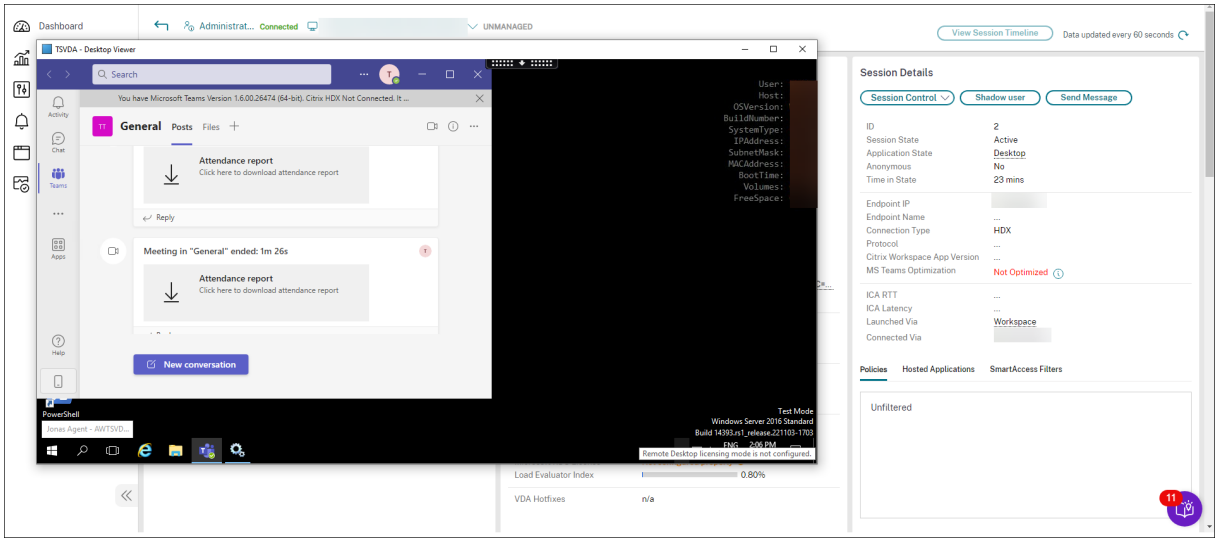
- Auf VDA wird Version 2311 und höher ausgeführt.
- Die unterstützten Versionen der Citrix Workspace-App sind unter Optimierung für Microsoft Teams aufgeführt.

- Microsoft Teams wird als veröffentlichte App oder auf einem veröffentlichten Desktop ausgeführt.
- Wichtige Dienste wie der Citrix HDX HTML5 Video Redirection Service werden ausgeführt.




Wenn Microsoft Teams nicht optimiert ist, enthält die QuickInfo einen Link zu einem externen Liveartikel zur Problembehandlung von HDX mit Tipps zur Optimierung von Microsoft Teams. Problembehandlung bei der HDX-Optimierung.




## Tipps zur Problembehandlung

Behandeln Sie das Problem mit den in der folgenden Tabelle empfohlenen Aktionen und eskalieren Sie das Problem ggf. an den entsprechenden Administrator.

| Benutzerproblem | Vorschläge |
| --- | --- |
| Anmeldung dauert lange oder schlägt periodisch oder wiederholt fehl | Diagnose von Benutzeranmeldeproblemen |
| Sitzungsstart dauert lange oder schlägt periodisch oder wiederholt fehl | Diagnose von Sitzungsstartproblemen |
| Sitzung reagiert langsam oder gar nicht | Sitzungsleistungsprobleme diagnostizieren |
| Anwendung ist langsam oder reagiert nicht mehr | Anwendungsstörungen beheben |
| Verbindung fehlgeschlagen | Desktopverbindungen wiederherstellen |
| Sitzung ist langsam oder reagiert nicht | Sitzungen wiederherstellen |
| Sitzungen aufzeichnen | Sitzungen aufzeichnen |
| Video ist langsam oder von schlechter Qualität | HDX-Kanalsystemberichte ausführen |

> **Hinweis:**
> Um sicherzustellen, dass die Maschine nicht im Wartungsmodus ist, überprüfen Sie in der Ansicht "Benutzerdetails"den Bereich "Maschinendetails".

### Sitzungsanmeldung

In der Ansicht **Benutzerdetails** > Registerkarte **Sitzungsanmeldung** wird eine umfassende Ansicht des Sitzungsanmeldevorgangs angezeigt. Die Registerkarte enthält das Diagramm mit den Phasen der Anmeldedauer, in dem die verschiedenen Anmeldephasen dargestellt sind. Verwenden Sie diese Daten, um Probleme mit der Benutzeranmeldung zu beheben. Weitere Informationen finden Sie unter Diagnose von Benutzeranmeldeproblemen.

### Sitzungsleistung

Auf der Registerkarte **Sitzungsleistung** wurden die Workflows zur Fehlerbehebung verbessert, etwa durch die Möglichkeit, Echtzeitmetriken zur Identifizierung von Problemen in Benutzersitzungen zu korrelieren. Der Bereich **Sitzungstopologie** bietet eine visuelle Darstellung des sitzungsinternen Pfads für verbundene HDX-Sitzungen. Der Bereich **Leistungsmetriken** enthält Trends für Sitzungsmetriken wie ICARTT, ICA-Latenz, Frames pro Sekunde, verfügbare Ausgabebandbreite und verbrauchte Ausgabebandbreite, die Aufschluss darüber geben, wie sich diese Metriken im Zeitverlauf entwickelt haben. Weitere Informationen finden Sie unter Sitzungsleistungsprobleme diagnostizieren.

### 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. Diese Suche ermöglicht die Fehlerbehebung nicht authentifizierter Sitzungen. Vergewissern Sie sich, dass Endpunktnamen eindeutig sind, damit die Problembehandlung von nicht authentifizierten Sitzungen durchgeführt werden kann.

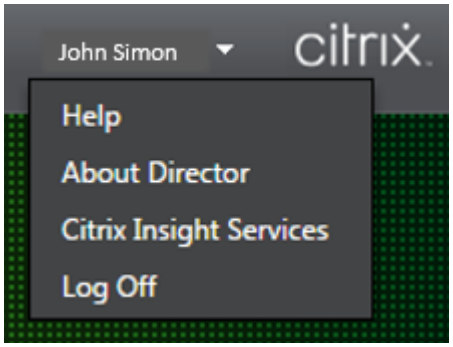
Die Suchergebnisse schließen auch Benutzer ein, die derzeit keine Maschine verwenden bzw. keiner Maschine zugewiesen sind.

- Bei der Suche wird die Groß- und Kleinschreibung nicht beachtet.
- Teileinträge ergeben eine Liste möglicher Übereinstimmungen.
- Nachdem Sie einige Buchstaben eines zweiteiligen Namens, getrennt durch ein Leerzeichen, eingegeben haben, enthalten die Ergebnisse Treffer für beide Zeichenfolgen. Die Beispiele für zweiteilige Namen sind Benutzername, Familienname und Vorname oder Anzeigename. 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 **Windows-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

June 27, 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.

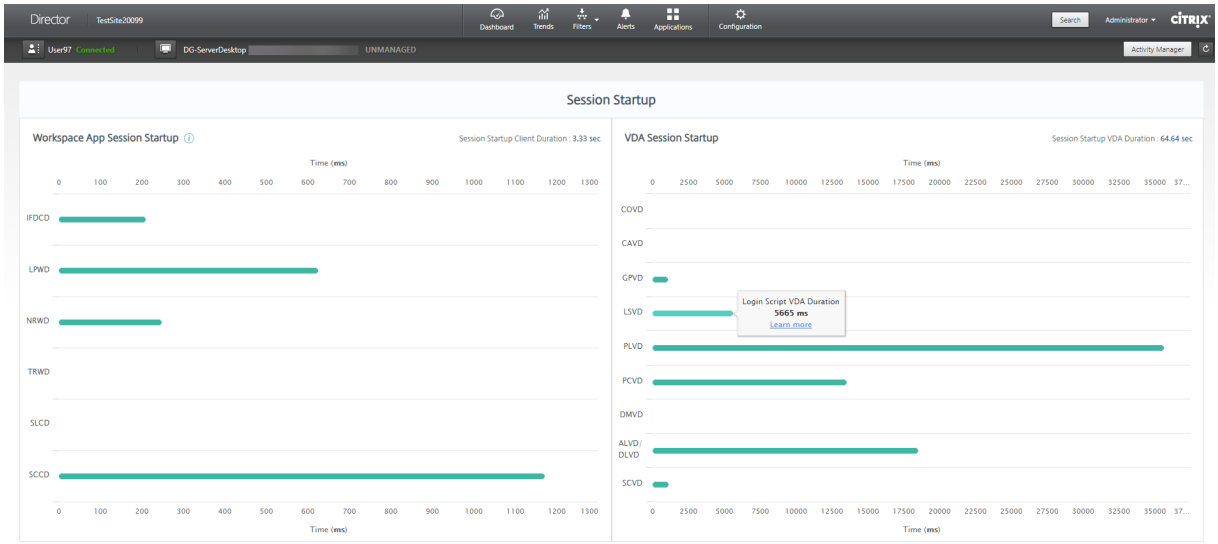
 

## Einschränkungen

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. SSCD beginnt so bald wie möglich nach der Anforderung (Mausklick). Es wird beendet, wenn die ICA-Verbindung zwischen Clientgerät und dem VDA hergestellt ist. 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 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 benötigt, um die Anmeldeinformationen des Benutzers gegen den Authentifizierungsanbieter zu prüfen. Es kann sich um Kerberos, Active Directory oder ein SSPI (Security Support Provider Interface) handeln.

#### 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. Dies erfordert zusätzliche Ressourcen. 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 der PCVD-Wert nicht 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 enthalten. Beispielsweise Audio- oder COM-Portzuordnung, um das ICA-Protokoll zu optimieren und die Sitzungsleistung insgesamt 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. 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 jegliche Verzögerungen bei der Erstellung der Sitzung auf dem VDA.

# Diagnose von Benutzeranmeldeproblemen

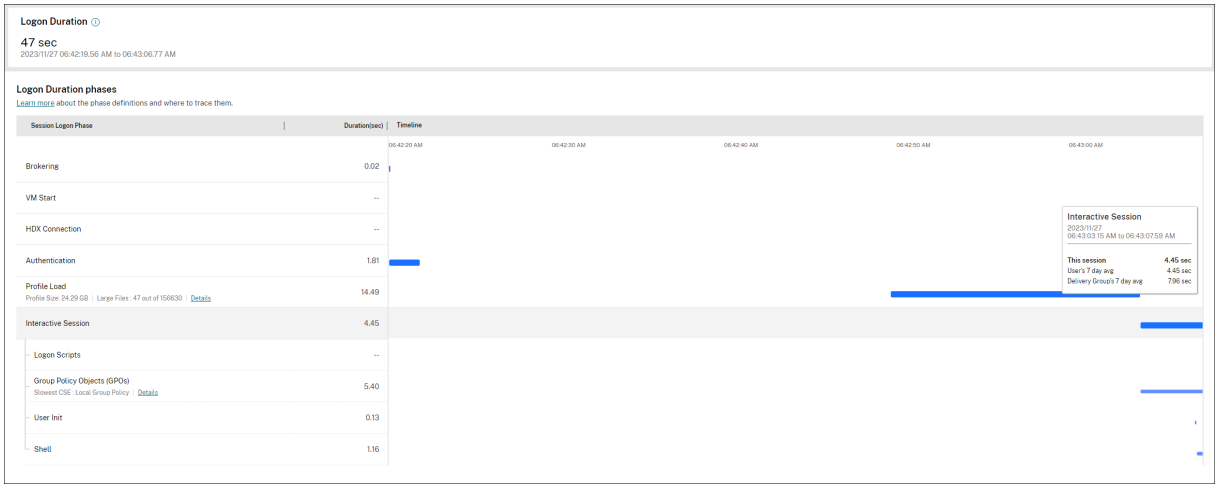
June 27, 2024

In der Ansicht **Benutzerdetails** > Registerkarte **Sitzungsanmeldung** wird eine umfassende Ansicht des Sitzungsanmeldevorgangs angezeigt. Verwenden Sie diese Daten, um Probleme mit der Benutzeranmeldung zu 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.

Wenn Benutzer sich bei Citrix Virtual Apps and Desktops anmelden, verfolgt der Überwachungsdienst die Phasen des Anmeldevorgangs. Die Phasen reichen von dem Zeitpunkt, zu dem der Benutzer eine Verbindung von der Citrix Workspace-App aus herstellt, bis zu dem Zeitpunkt, zu dem die App oder der Desktop bereit ist.

Die Registerkarte **Sitzungsanmeldung** enthält das Diagramm mit den Phasen der Anmeldedauer, in dem die verschiedenen Anmeldephasen dargestellt sind. Die Anmeldedauer entspricht der Zeit, die für den Verbindungsaufbau und das Abrufen einer App oder eines Desktops vom Delivery Controller aufgewendet wurde, sowie die Zeit, die für die Authentifizierung und Anmeldung bei einer virtuellen App oder einem virtuellen Desktop verstrichen ist. Die Dauer wird in Sekunden (oder Sekundenbruchteilen) angezeigt.




Das Diagramm mit den Phasen der Anmeldedauer bietet einen klaren Überblick über die verschiedenen Anmeldephasen sowie deren Start- und Endzeiten. Das Diagramm zeigt die Überlappung der einzelnen Anmeldephasen. Die gesamte Anmeldezeit ist möglicherweise nicht die Summe der einzelnen Anmeldephasen. Dies liegt daran, dass sich die einzelnen Phasen möglicherweise überschneiden

und nicht alle Anmeldephasen Teil dieser Darstellung sind. Außerdem können sich bestimmte Phasen verlängern, auch wenn der Benutzer anfängt, mit der virtuellen App oder dem Desktop zu interagieren, und diese Dauer wird nicht als Teil der gesamten Anmeldedauer gemessen.

Verwenden Sie diese Ansicht, um bestimmte Anmeldephasen zu identifizieren, die zu einem verzögerten Sitzungsstart führen. Die Definition für jede Anmeldephase und die Ereignisquelle, von der aus Sie Informationen verfolgen können, helfen bei der weiteren Problembehandlung. Wenn Sie mit der Maus auf das Diagramm zeigen, wird eine QuickInfo angezeigt, der die Phasendauer für die aktuelle Sitzung sowie den 7-Tage-Durchschnitt des Benutzers und den 7-Tage-Durchschnitt der Bereitstellungsgruppe enthält. Diese Informationen helfen dabei, die aktuelle Sitzungsanmeldedauer mit den Durchschnittswerten von 7 Tagen zu vergleichen. Im Fall von GPO- und Profildetails können Sie weitere Details zu Teilphasenmessungen anzeigen. Diese Visualisierung hilft dabei, Probleme im Zusammenhang mit der Anmeldedauer auf einfache Weise zu verstehen und zu beheben.

### 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.

> **Hinweise:**
>
> - Die Anmeldedauer wird nur auf der Standard-Windows-Shell (explorer.exe) und nicht auf benutzerdefinierten Shells unterstützt.
> - Die Anmeldedauer für Remote-PC-Zugriff ist nur verfügbar, wenn **Citrix User Profile Manager** und das **Citrix User Profile Manager WMI-Plug-In** bei der Installation von Remote-PC-Zugriff als zusätzliche Komponenten installiert werden. Weitere Informationen finden Sie unter Schritt 4 von Remote-PC-Zugriff: Konfiguration und Reihenfolge.

### Beheben von Benutzeranmeldeproblemen

1. Führen Sie in der Ansicht **Benutzerdetails** auf der Registerkarte **Sitzungsanmeldung** anhand des Diagramms "Anmeldedauer"eine Fehlerbehebung für den Anmeldestatus durch.

- Wenn Benutzer sich anmelden, wird der Anmeldeprozess in der Ansicht widergespiegelt.
- Wenn der Benutzer 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.

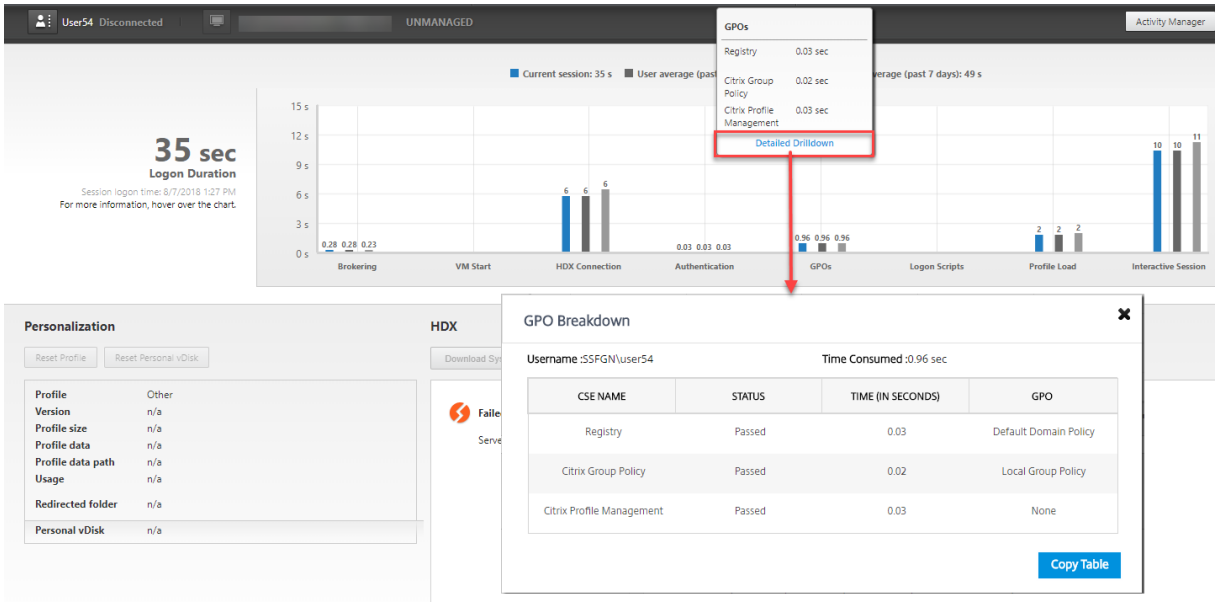
### Authentifizierung

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 **Details**, 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 TechNet-Artikel zum Konfigurieren von Ereignisprotokollen.

### Anmeldeskripts

Zum Ausführen von Anmeldeskripts benötigte Zeit, wenn Anmeldeskripts für die Sitzung konfiguriert sind.

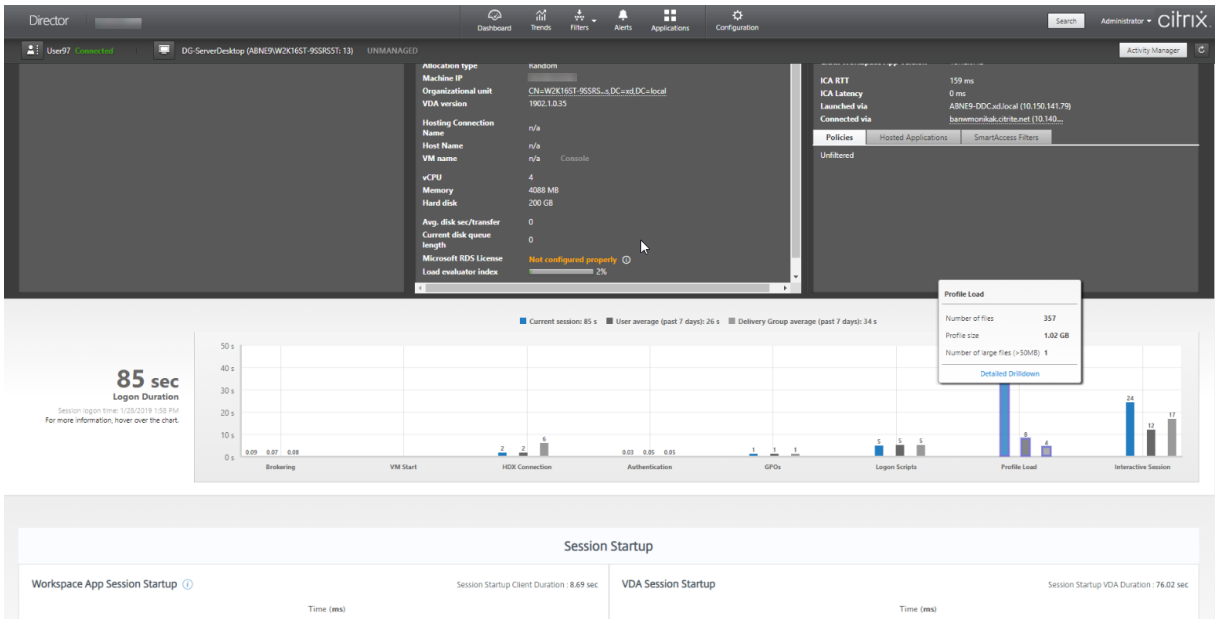
### Profilladezeit

Zum Laden des Profils benötigte Zeit, wenn für den Benutzer Profileinstellungen auf der virtuellen Maschine konfiguriert sind.

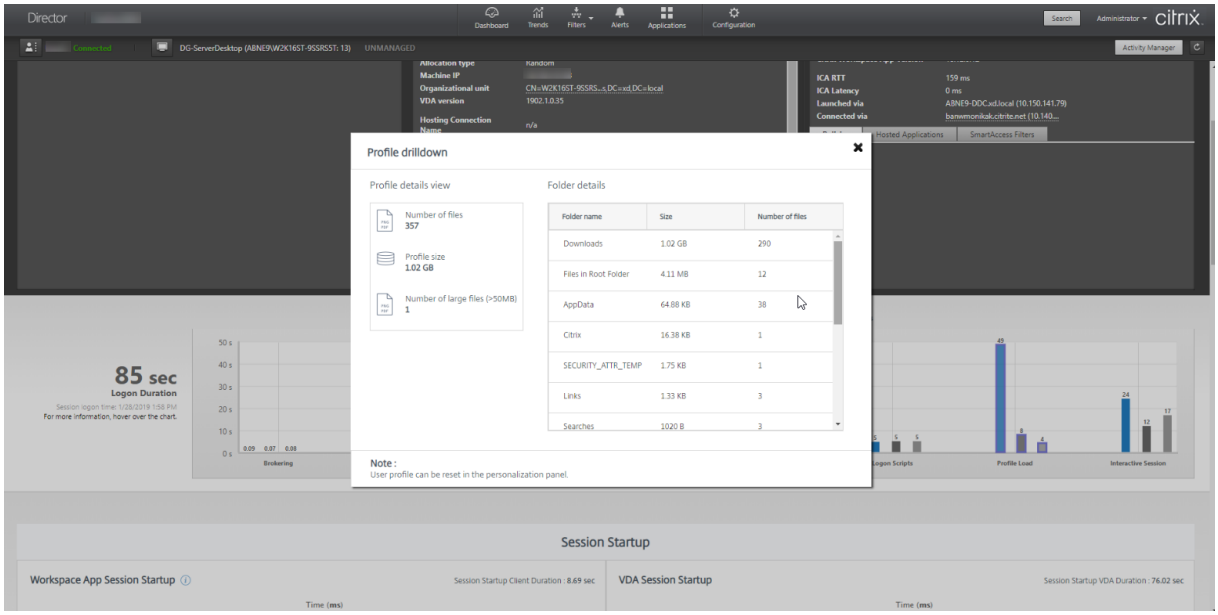
Wenn die Citrix Profilverwaltung konfiguriert ist, wird die Dauer der Profilverarbeitung durch die Profilverwaltung im Balken “Profilladezeit”angezeigt. Anhand dieser Informationen ist eine gezieltere Problembehandlung bei langsamer Profilverarbeitung möglich. Wenn die Profilverwaltung konfiguriert ist, 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 **Details**, um Informationen zu den einzelnen Ordnern im Profilstammordner (z. B. C:/Benutzer/Benutzername), 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. Erstellen 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

Interaktive Sitzung ist die 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. Zeigen Sie auf die interaktive Sitzung, um eine QuickInfo mit Folgendem anzuzeigen:

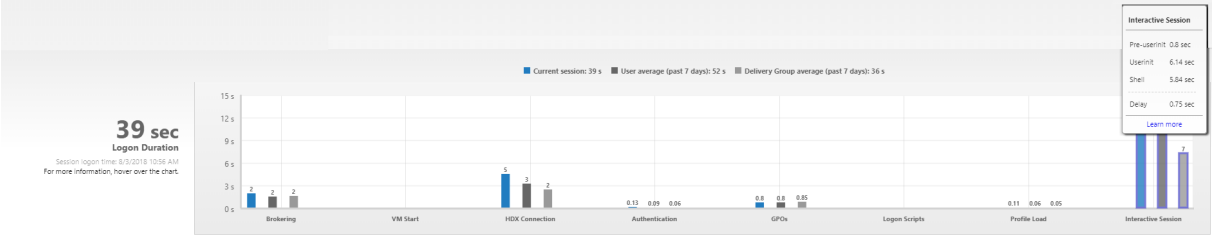
- Teilphasen
- für jede Teilphase aufgewendete Zeit
- gesamte kumulative Zeitverzögerung zwischen Teilphasen

> **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 “Drill-down 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 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 Audit process tracking in der Microsoft-Dokumentation.




Bereich “Anmeldedauer”in der Ansicht “Benutzerdetails”

- **Interaktive Sitzung –Pre-Userinit:** Teil der interaktiven Sitzung, der sich mit Gruppenrichtlinienobjekten und Skripts überschneidet. 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.:

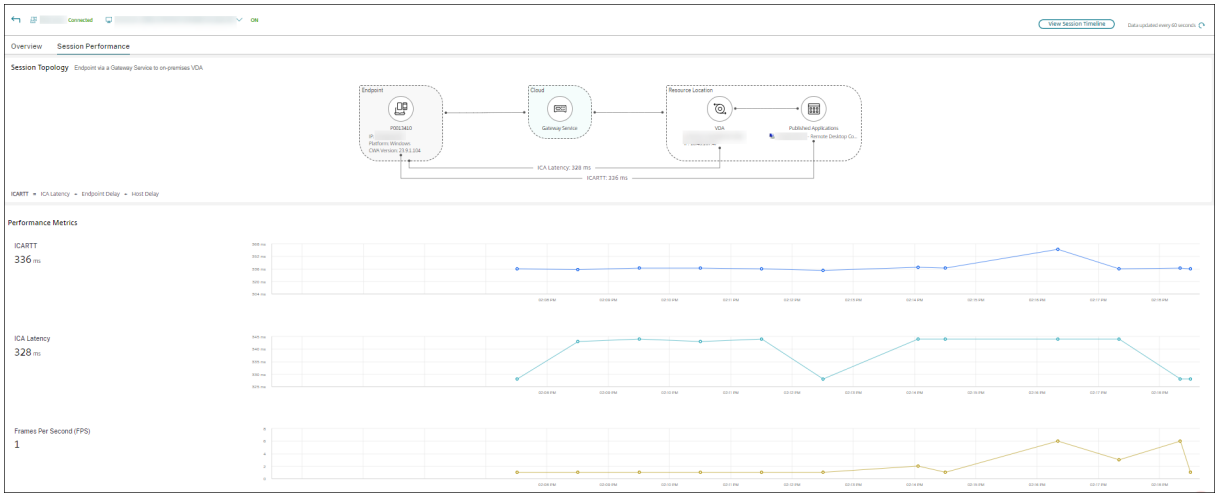
- Fehlende (aktuelle) Anmeldeleisten
- Große Abweichung zwischen der aktuellen und der durchschnittlichen Dauer für diesen Benutzer. Mögliche Ursachen:
  - Es wurde eine neue Anwendung installiert.
  - Das Betriebssystem wurde aktualisiert.
  - Es wurden Konfigurationsänderungen vorgenommen.
  - Das 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.

## Sitzungsleistungsprobleme diagnostizieren

June 27, 2024

Die Registerkarte **Sitzungsleistung** auf der Benutzerdetailseite enthält verbesserte Workflows zum Identifizieren von Problemen in HDX-Benutzersitzungen. Die Bereiche Sitzungstopologie und Leistungsmetriken helfen beim Korrelieren der Komponentenansicht und mehrerer Leistungsmetriken einer Sitzung in einer Ansicht und reduzieren die durchschnittliche Zeit für die Problemlösung bei der Sitzungserfahrung.



## Durchgängige Netzwerkhopansicht

Eine durchgängige Netzwerkhopansicht ist der nächste Schritt zur Verbesserung der Workflows zur Fehlerbehebung. Der Abschnitt **Benutzerdetails** > **Sitzungsleistung** > **Sitzungstopologie** bietet eine visuelle Darstellung der durchgängigen Netzwerkhopansicht für verbundene HDX-Sitzungen.

Für eine verbundene Sitzung zeigt die Sitzungstopologie die am Sitzungspfad beteiligten Komponenten mit zugehörigen Metadaten, die Verbindung zwischen den Komponenten und die auf dem VDA veröffentlichten Anwendungen.
Darüber hinaus werden die folgenden Sitzungsleistungsmetriken für die Sitzung angezeigt:

- ICA-Latenz: Die Latenz ist im Grunde die Netzwerklatenz. Dieser Parameter gibt an, ob das Netzwerk träge ist.
- ICA RTT: Zeitintervall zwischen der Aktion eines Benutzers und der auf seinem Bildschirm angezeigten grafischen Reaktion. Dieser Kennwert umfasst ICA-Latenz, die Endpunktverzögerung und die Hostverzögerung.

Anhand dieser Ansicht sehen Sie, durch welche Komponenten die Sitzungsdaten übertragen werden, und können Hops identifizieren, die ggf. Leistungsprobleme verursachen.

Die Leistungsmetriken in der Ansicht "Sitzungstopologie"sind nur für verbundene HDX-Sitzungen verfügbar.

### Sitzungstopologie –Szenarien

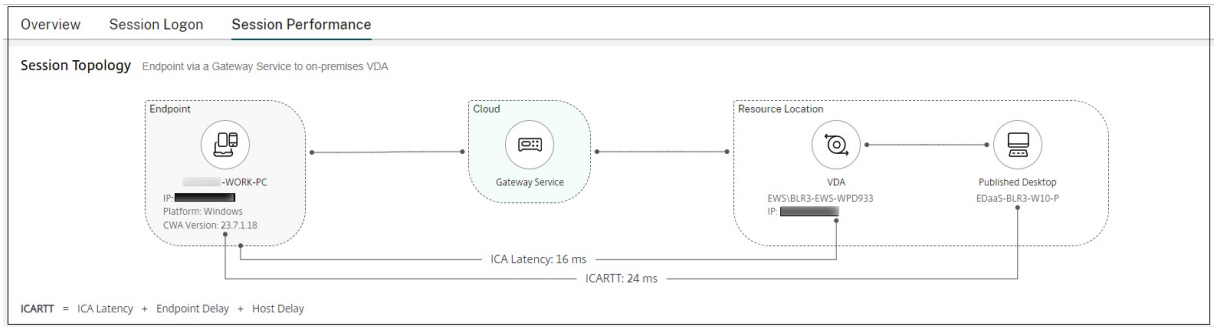
Je nach Site-Bereitstellungsszenario sind einigen oder alle der folgenden Komponenten an einer Sitzung beteiligt:

- Citrix Workspace-App auf dem Endpunkt
- Gateway Service/On-Premises-Gateway
- Cloud Connector: Bei Hybridverbindungen ist das Gateway über einen Cloud Connector mit DaaS verbunden.
- VDAs

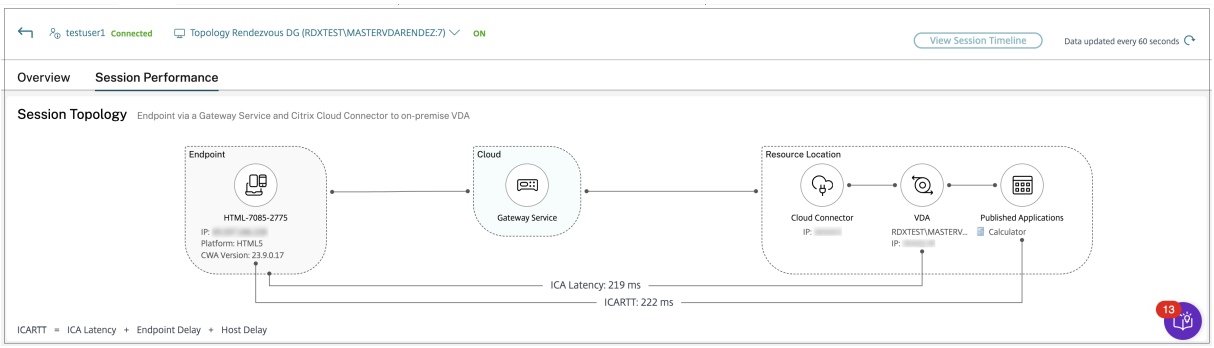
Dementsprechend sind folgende Netzwerktopologien möglich:

- Die Citrix Workspace-App auf dem Endpunkt stellt über Citrix Workspace und Gateway Service eine Verbindung zu einem On-Premises-VDA her. Für die Verbindung mit dem VDA wird kein Cloud Connector verwendet.

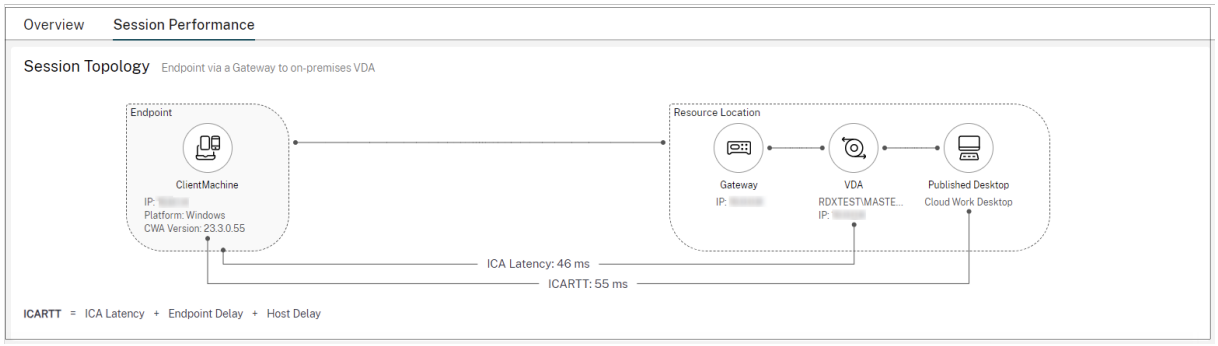
 




- Die Citrix Workspace-App auf dem Endpunkt stellt über Citrix Workspace und Gateway Service über einen Cloud Connector eine Verbindung zu einem On-Premises-VDA her.

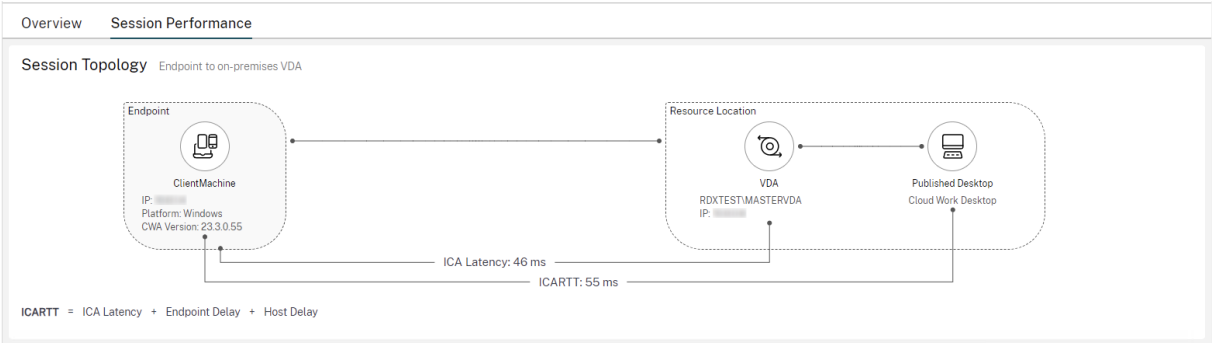



- Die Citrix Workspace-App auf dem Endpunkt stellt über StoreFront und ein On-Premises-Gateway eine Verbindung zu einem On-Premises-VDA her.




- Die Citrix Workspace-App auf dem Endpunkt stellt über StoreFront eine Verbindung zu einem On-Premises-VDA her.




## Leistungsmetriken

Im Bereich **Leistungsmetriken** können Sie Echtzeitmetriken korrelieren, um Probleme in Benutzersitzungen zu identifizieren. Sitzungsmetriktrends geben Aufschluss darüber, wie sich die Metriken im Zeitverlauf entwickelt haben. Wenn Sie mit den Echtzeitdaten auf die Registerkarte **Sitzungsleistung** klicken, können Sie die Daten der letzten 15 Minuten anzeigen, ohne auf die Ladezeit der Seite warten zu müssen. Über die Diagramme können Leistungskennzahlen mehrerer Komponenten in einer einzigen Ansicht korreliert werden.


> **Hinweis:**
>
> Da die Metriken der letzten 15 Minuten eingelesen werden, wird das Diagramm für die Dauer dargestellt, für die die Sitzung verbunden und getrennt wurde. Die Metrik der getrennten Sitzung wird mit dem Wert Null angezeigt.

Neben ICARTT und ICA-Latenz sind die folgenden Metriken verfügbar:

- Frames pro Sekunde: Wichtige Metrik, die die Reaktionsfähigkeit von Sitzungen angibt. Verfügbare Ausgabebandbreite: Die verfügbare Ausgabebandbreite ist die Gesamtbandbreite, die für die Übertragung von Daten vom VDA zum Endpunkt zur Verfügung steht.

- Verbrauchte Ausgabebandbreite: Die verbrauchte Ausgabebandbreite ist die Datenmenge, die vom VDA zur Anzeige von Sitzungen zum Endpunkt übertragen wird.

Durch die Analyse der verfügbaren Ausgabebandbreite und der verbrauchten Ausgabebandbreite können Sie überprüfen, ob ausreichend Bandbreite für die Bedienung von Sitzungen verfügbar ist, und ob die Bandbreite für eine Sitzung unzureichend ist.

## Benutzer spiegeln

June 27, 2024

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 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.

## Nachrichten an Benutzer senden

June 27, 2024

Sie können über Director eine Nachricht an einen Benutzer senden, der mit einer oder mehreren Maschinen verbunden ist. Sie können mit dieser Funktion sofortige Benachrichtigungen über administrative Aktionen senden, wie bevorstehende Desktopwartung, Abmeldungen bzw. Neustarts von Maschinen und das Zurücksetzen von Profilen.

1. Wählen Sie in der Ansicht Aktivitäts-Manager den Benutzer aus und klicken Sie auf Details.
2. Klicken in der Ansicht Benutzerdetails im Bereich Sitzungsdetails auf Nachricht senden.
3. Füllen Sie die Felder Betreff und Nachricht aus und klicken Sie auf Senden.

Wenn die Nachricht gesendet wird, wird in Director eine Bestätigungsmeldung angezeigt. Die Meldung wird auf der Maschine des Benutzers 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**.

## Anwendungsstörungen beheben

June 27, 2024

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 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. |

| Aktion | Beschreibung |
| --- | --- |
| 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. |

## Desktopverbindungen wiederherstellen

June 27, 2024

Überprüfen Sie von Director den Verbindungsstatus des Benutzers für die aktuelle Maschine in der Titelleiste des Benutzers.

Wenn die Desktopverbindung fehlgeschlagen ist, wird die Fehlerursache angezeigt, um Sie bei der Problembehandlung zu unterstützen.

| Aktion | Beschreibung |
| --- | --- |
| Stellen Sie sicher, dass die Maschine nicht im Wartungsmodus ist. | Achten Sie auf der Seite Benutzerdetails darauf, dass der Wartungsmodus deaktiviert ist. |
| Neustarten der Maschine des Benutzers | Wählen Sie die Maschine aus und klicken Sie auf **Neu starten**. Verwenden Sie diese Option, wenn die Maschine des Benutzers nicht reagiert oder keine Verbindung herstellen kann. Beispiel: Die Maschine verwendet ungewöhnlich viele Prozessorressourcen, was den Prozessor unbrauchbar machen kann. |

## Sitzungen wiederherstellen

June 27, 2024

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. |

| Aktion | Beschreibung |
| --- | --- |
| 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 von der Benutzersitzung | 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.

## HDX-Kanalsystemberichte ausführen

June 27, 2024

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.

## Benutzerprofil zurücksetzen

June 27, 2024

> **ACHTUNG:**
>
> Wenn ein Profil zurückgesetzt wird, werden die Ordner und Dateien des Benutzers gespeichert und in das neue Profil kopiert. Die meisten Benutzerprofildaten fehlen jedoch (z. B. wird die Registrierung zurückgesetzt und Anwendungseinstellungen werden evtl. gelöscht).

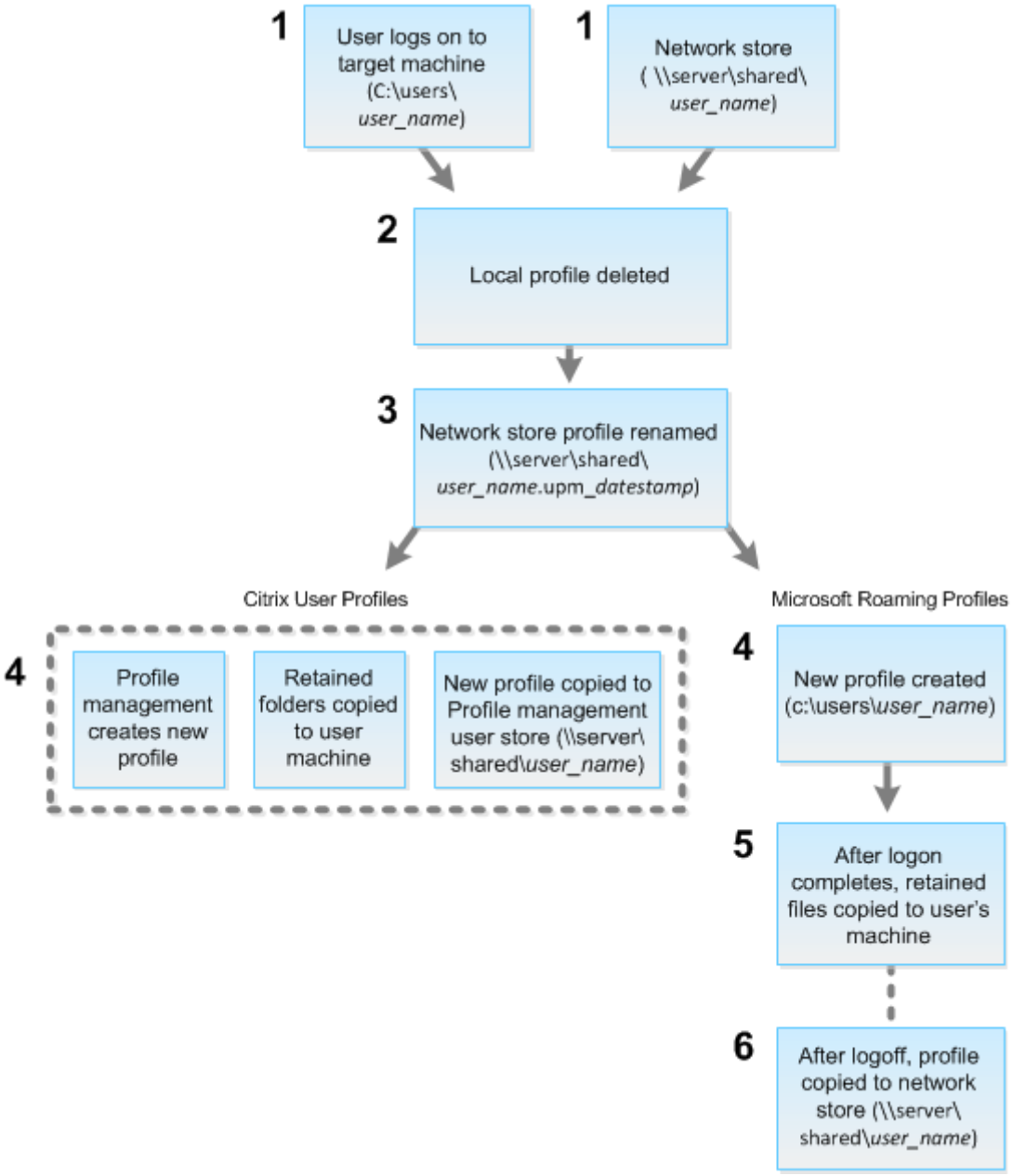
Die Zurücksetzfunktion gilt sowohl für dateibasierte als auch für containerbasierte Profillösungen.

### 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.

Bei Citrix Benutzerprofilen erfolgt die Profilerstellung mithilfe der Importregeln für die Profilverwaltung. Die Ordner werden zurück in das Netzwerkprofil kopiert und der Benutzer kann sich normal 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 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.

### Zurücksetzen von Benutzerprofilen in Director

Wenn Sie den Citrix Virtual Desktops-VDA (Desktop-VDA) verwenden, gehen Sie wie folgt vor:

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.

Wenn Sie den 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.

> **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. Die Anmeldung 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.

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.

Beachten Sie Folgendes:

- Wenn für Benutzerprofile der Benutzerspeicher aktiviert ist, enthält das neue Profil die folgenden persönlichen Ordner aus dem ursprünglichen Benutzerprofil:
  - Desktop
  - Cookies
  - Favoriten
  - Dokumente
  - Bilder
  - Musik
  - Videos
- Wenn der Citrix Management-Profilcontainer als gesamte Lösung für Benutzerprofile aktiviert ist, enthält das neue Profil die o. g. persönlichen Ordner nicht.
- In Windows 8 und höheren Versionen werden Cookies beim Zurücksetzen des Profils nicht in das neue Profil 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. Das ist die Datei ohne die Erweiterung upm_datumsstempel.
5. Benennen Sie den archivierten Ordner unter Verwendung des ursprünglichen Profilnamens um. Das heißt, entfernen Sie die Datums- und Uhrzeit-Erweiterung. 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 Backuppfad angeben, wird automatisch ein Backupordner 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
  ```

## Sitzungen aufzeichnen

June 27, 2024

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.

### Dynamische Sitzungsaufzeichnung

Sie können die aktuelle aktive Sitzung mithilfe der Steuerelemente für die Sitzungsaufzeichnung im Bildschirm **Benutzerdetails** aufzeichnen. Weitere Informationen zur dynamischen Sitzungsaufzeichnung finden Sie im Artikel zum Sitzungsaufzeichnungsdienst.

### Richtlinienbasierte Sitzungsaufzeichnung

Informationen zum Konfigurieren der richtlinienbasierten Sitzungsaufzeichnung unter Director mit dem DirectorConfig-Tool finden Sie unter **Director zur Verwendung des Sitzungsaufzeichnungsservers konfigurieren** im Abschnitt Richtlinien für die Sitzungsaufzeichnung konfigurieren.
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 Autorisieren von Benutzern).

> **Hinweis:**
> Über Director oder die Richtlinienkonsole für die Sitzungsaufzeichnung gemachte Änderungen an den Einstellungen für die Sitzungsaufzeichnung werden in den nachfolgenden ICA-Sitzungen wirksam.

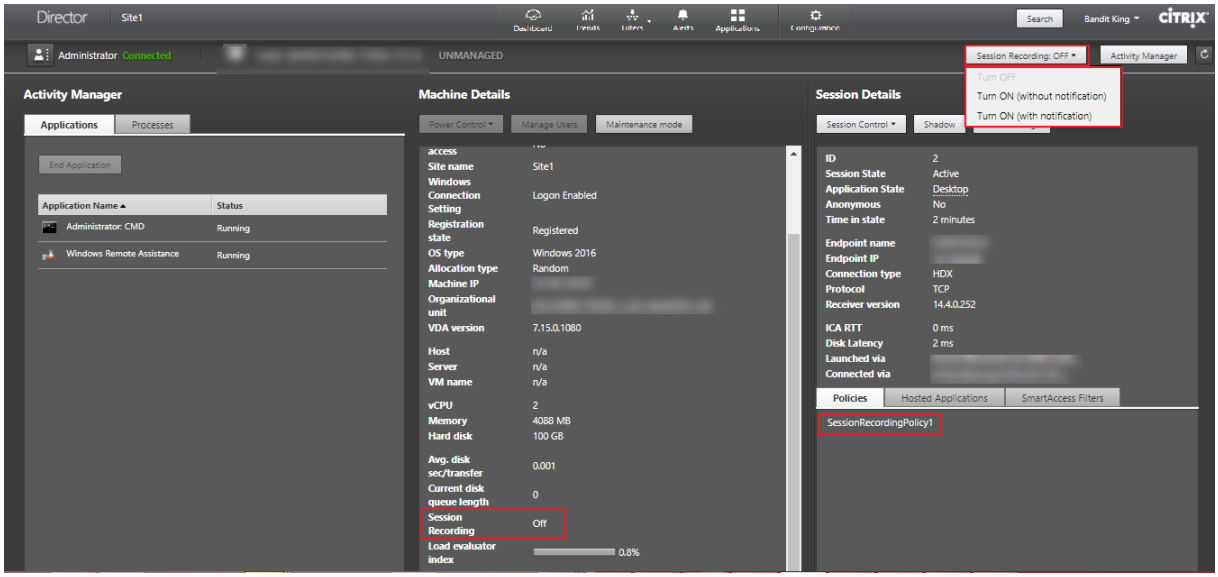
### Steuerelemente der Sitzungsaufzeichnung in Director

Sie können die Aktionen **Benutzerdetails** > **Sitzungsaufzeichnung** verwenden, um die aktuelle oder nachfolgende Sitzung aufzuzeichnen.

- Dynamische Sitzungsaufzeichnung einschalten: Die aktuelle Sitzung wird aufgezeichnet.
- Einschalten (mit Benachrichtigung): Die nachfolgenden Sitzungen werden aufgezeichnet und der Benutzer wird über die Aufzeichnung der Sitzung beim Anmelden bei der ICA-Sitzung benachrichtigt.
- Einschalten (ohne Benachrichtigung): Die nachfolgenden Sitzungen werden 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.




Im Bereich **Maschinendetails** wird der Status der Sitzungsaufzeichnungsrichtlinie für die Maschine angezeigt.

### Livesitzungen und aufgezeichnete Sitzungen wiedergeben

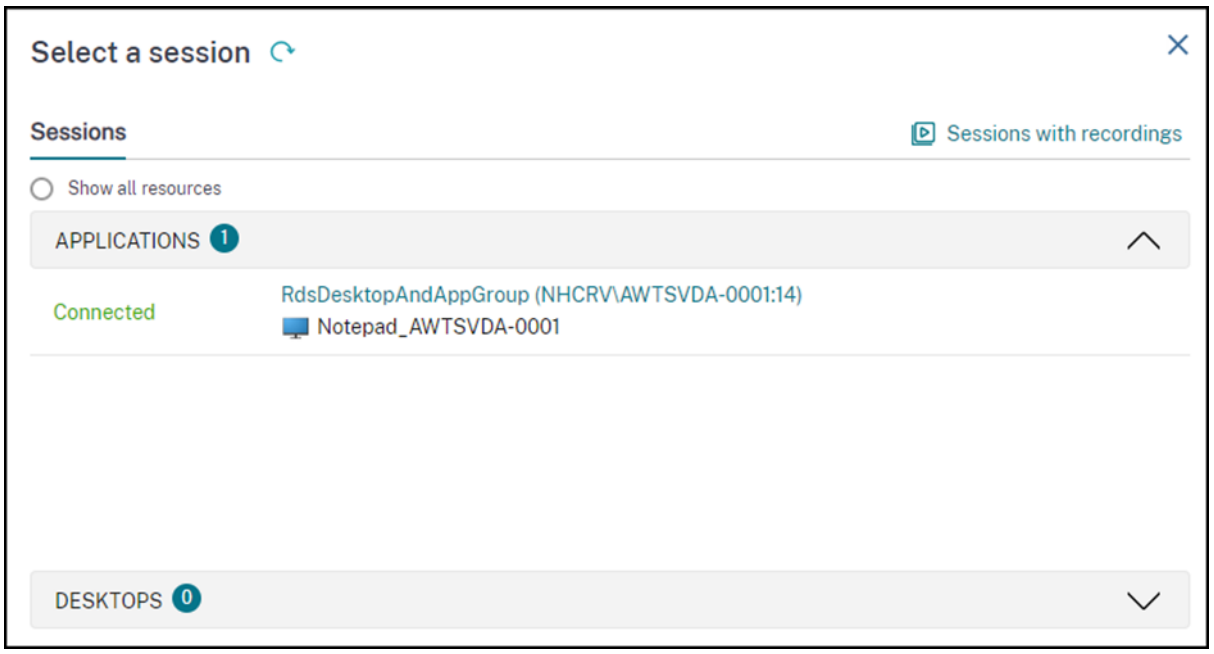
Sie können aufgezeichnete und Livebenutzersitzungen wiedergeben, um zu verstehen, auf welche Probleme der Benutzer gestoßen ist. Dank des direkten Zugriffs auf Aufzeichnungen und sitzungsbezogene Messwerte in der Director-Konsole müssen Sie nicht mehr auf mehreren Sitzungsaufzeichnungsservern nach den Aufzeichnungen suchen oder Apps von Drittanbietern aufrufen, um die Aufzeichnungen anzusehen. Die in den Aufzeichnungen festgestellten Probleme lassen sich so mit den Leistungskennzahlen verknüpfen.

Dieses Feature erfordert Folgendes:

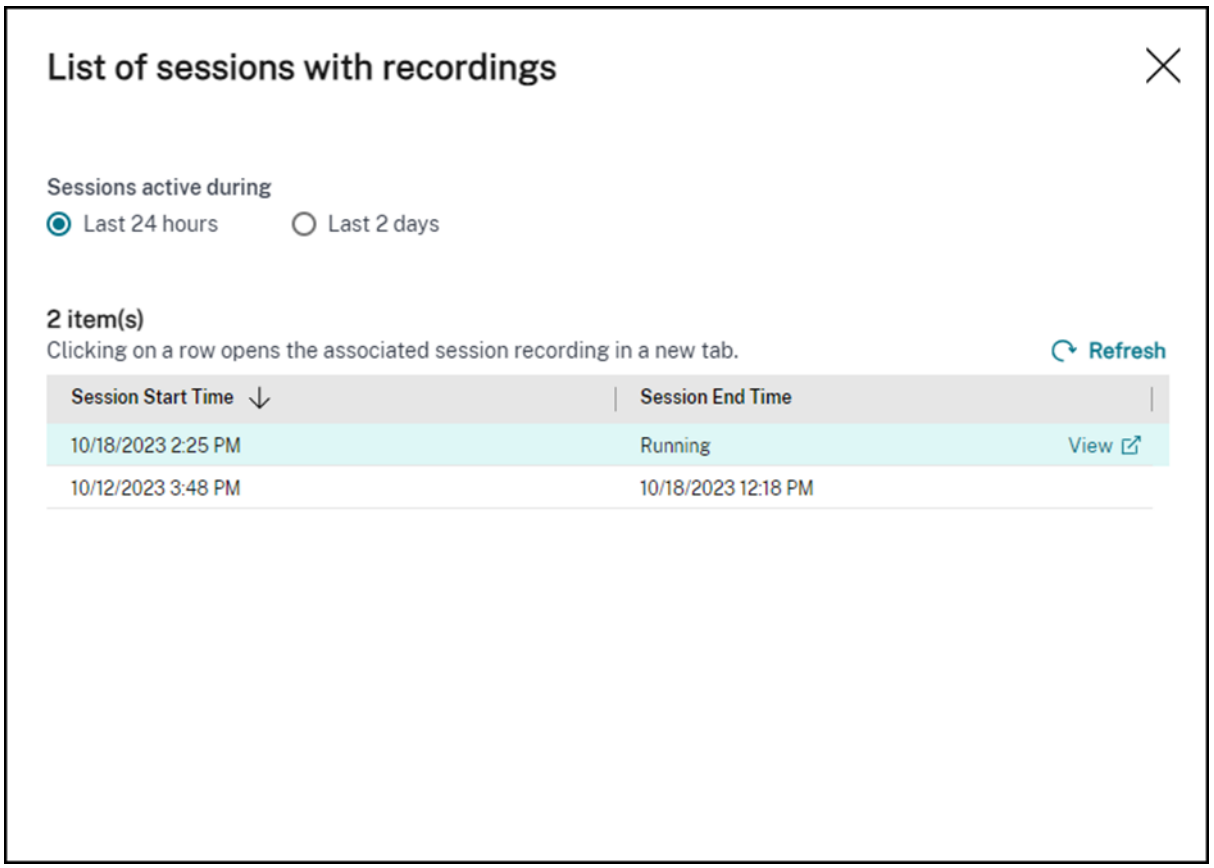
- Der VDA und die Sitzungsaufzeichnungsserver verwenden Version 2308 oder höher.
- Delivery Controller und Director sind auf Version 2311 oder höher.

Director speichert Sitzungsaufzeichnungen in einem zentralen Repository. Die Liste der Aufzeichnungen, die dem Benutzer gehören, wird angezeigt, wenn Sie auf das Modal **Sitzungsauswahl** > **Sitzungen mit Aufzeichnungen** klicken.




Sie können wählen, ob Sie Aufzeichnungen von Sitzungen anzeigen möchten, die in den letzten 24 Stunden oder in den letzten 2 Tagen aktiv waren. Liveaufzeichnungen von aktuell aktiven Sessions sind mit **Sitzungsende** als **Wird ausgeführt** gekennzeichnet.



Klicken Sie auf den Link **Anzeigen**, um die Aufzeichnung auf einer neuen Registerkarte mit dem Wiedergabeserver der Citrix Sitzungsaufzeichnung wiederzugeben.

## Featurekompatibilitätsmatrix

June 27, 2024

Citrix Director 7 2203 ist mit folgender Software kompatibel:

- Citrix Virtual Apps and Desktops 7 2112 und höher
- Citrix Virtual Apps and Desktops 7 1912 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 |
|---|---|---|---|
| 2311 | Livesitzungen und aufgezeichnete Sitzungen wiedergeben | VDA 2308 und DDC 2311 | Alle |
| 2311 | Sitzungstopologie | None | Alle |
| 2311 | Optimale Bildschirmauflösung | None | Alle |
| 2311 | MS Teams-Optimierung | VDA 2311 und aktueller DDC | Alle |
| 2311 | Verbesserungen des Überblicks über Tests | None | Alle |
| 2311 | Überarbeitete Ansicht für Sitzungsanmeldedauer | None | Alle |
| 2308 | Tests – Zusammenfassung und Details | None | Alle |
| 2308 | Citrix Probe Agent-Unterstützung für Multifaktorauthentifizierung mit Citrix Gateway | Citrix Gateway | Alle |
| 2308 | Hypervisor-Warnungen deaktivieren | None | Alle |
| 2308 | Trends für Sitzungserfahrungsmetriken | None | Alle |
| 2305 | Unterstützt die Authentifizierung über Citrix Gateway | None | Alle |
| 2305 | Autoscale-Verwaltung in Director | None | Alle |

| Director-Version | Feature | Abhängigkeiten - erforderliche Mindestversion | Edition |
|---|---|---|---|
| 2303 | Warnung "Fehlerhafte Maschinen" | DC 7 2303 | Premium |
| 2203 | TLS 1.3-Unterstützung | - | Alle |
| 2212 | GPU-Auslastung in Echtzeit für AMD-GPUs verfügbar | DC 7.14 und VDA 7.14 mit 64-Bit-Windows und aktiviertem HDX 3D Pro | Alle |
| 2212 | Erweiterte Testplanung | DC 7 1906 und Citrix Probe Agent 2209 | Premium |
| 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 |
| 1811 | Anzeige wichtiger RTOP-Daten | DC 7 1811 und VDA 1808 | Premium |
| 1808 | Export von Filterdaten | DC 7 1808 | Alle |

| Director-Version | Feature | Abhängigkeiten - erforderliche Mindestversion | Edition |
|---|---|---|---|
| 1808 | Drilldown für interaktive Sitzungen | DC 7 1808 und VDA 1808 | Alle |
| 1808 | GPO-Drilldown | DC 7 1808 und VDA 1808 | Alle |
| 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 | None | Alle |
| 7.18 | Drilldown für interaktive Sitzungen | None | Alle |
| 7.17 | PIV-Smartcardauthentifizierung | None | 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 | None | 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 |

| Director-Version | Feature | Abhängigkeiten - erforderliche Mindestversion | Edition |
|---|---|---|---|
| 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 |
| 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 | Integration der Windows-Authentifizierung | DC 7.x und VDA 7.x | Alle |

| Director-Version | Feature | Abhängigkeiten - erforderliche Mindestversion | Edition |
|---|---|---|---|
| 7.7 | Nutzung von Maschinen mit Einzelsitzungs-OS und Multisitzungs-OS | DC 7.7 und VDA 7.x | Premium (zuvor Platinum) |
| 7.6.300 | Unterstützung für Framehawk Virtual Channel | DC 7.6 und VDA 7.6 | Alle |
| 7.6.200 | Integration der Sitzungsaufzeichnung | DC 7.6 und VDA 7.x | Premium (zuvor Platinum) |
| 7 | Integration von HDX Insight | DC 7.6, VDA 7.x und Citrix ADM | Premium (zuvor Platinum) |

## Datengranularität und -beibehaltung

June 27, 2024

### 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. Wenn das Zeitintervall jedoch 1 Minute beträgt, werden alle Sitzungen in dieser Minute (unabhängig davon, ob sie sich überlappen) als gleichzeitig behandelt. Das Intervall ist so klein, dass der Mehraufwand für die Berechnung der Genauigkeit sich 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 im vorigen Abschnitt 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. Mit der Bereinigung 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 | Aufbewahrungszeit für Premium | Aufbewahrungszeit für Advanced |
|---|---|---|---|---|
| 1 | GroomSessionsRetentionDays | Beibehaltungszeitraum für Sitzungs- und Verbindungsinformationen nach Beenden der Sitzung | 90 | 31 |
| 2 | GroomFailuresRetentionDays | Einträge für MachineFailureLog und ConnectionFailureLog | 90 | 31 |
| 3 | GroomLoadIndexesRetentionDays | Einträge für LoadIndex | 90 | 31 |

| | Einstellungsname | Betroffene Bereinigung | Aufbewahrungszeit für Premium | Aufbewahrungszeit für Advanced |
|---|---|---|---|---|
| 4 | GroomDeletedRetentionDays | Maschinen-, Katalog-, Desktopgruppen- und Hypervisorentitäten, die einen LifecycleState von “Deleted” haben. Durch diese Einstellung werden auch zugehörige Einträge für Sitzung, Sitzungsdetail, Zusammenfassung, Fehler oder LoadIndex gelöscht. | 90 | 31 |
| 5 | GroomSummariesRetentionDays | Einträge für Desktop-GroupSummary, FailureLogSummary und LoadIndexSummary. Aggregierte Daten, tägliche Granularität | 365 | 31 |

| | Einstellungsname | Betroffene Bereinigung | Aufbewahrungszeit für Premium | Aufbewahrungszeit für Advanced |
|---|---|---|---|---|
| 6 | GroomMachineHotfixLogRetentionDays | Auf VDA- und Controller-maschinen angewendete Hotfixes | 90 | 31 |
| 7 | GroomMinuteRetentionDays | Aggregierte Daten - minutenge-naue Granularität | 3 | 3 |
| 8 | GroomHourlyRetentionDays | Aggregierte Daten - stun-dengenaue Granularität | 32 | 31 |
| 9 | GroomApplicationUserCountRetentionDays | Anwendungsinstanzen auf | 90 | Nicht zutreffend |
| 10 | GroomNotificationLogRetentionDays | Benachrichtigungsprotokolldaten | 90 | Nicht zutreffend |
| 11 | GroomResourceUsageRawDataRetentionDays | Rohdaten zur Ressource-nauslastung | 3 | 3 |
| 12 | GroomResourceUsageMinuteDataRetentionDays | Zusammengefasste Daten zur Ressource-nauslastung mit minuten-genauer Granularität | 7 | 7 |
| 13 | GroomResourceUsageHourDataRetentionDays | Zusammengefasste Daten zur Ressource-nauslastung mit stunden-genauer Granularität | 30 | 30 |

| | Einstellungsname | Betroffene Bereinigung | Aufbewahrungszeit für Premium | Aufbewahrungszeit für Advanced |
|---|---|---|---|---|
| 14 | GroomResourceUsageDayDataRetentionDays | Zugeordnete Daten zur Ressourcennauslastung mit tagesgenauer Granularität | 365 | 31 |
| 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 | 30 |
| 19 | GroomSessionMetricsDataRetentionDays | Daten zu Sitzungskennzahlen | 1 | 1 |
| 20 | GroomMachineMetricsDataRetentionDays | Daten zu Maschinenkennzahlen | 3 | 3 |

| | Einstellungsname | Betroffene Bereinigung | Aufbewahrungszeit für Premium | Aufbewahrungszeit für Advanced |
|---|---|---|---|---|
| 21 | GroomMachineMetricsDataRetentionDays | Zusammengefasste Daten zu Maschinenkennzahlen | 365 | 31 |
| 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:** Der Aufbewahrungszeitraum ist für alle Einstellungen auf 1000 Tage beschränkt (Citrix empfiehlt 365 Tage).
- **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 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

June 27, 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 | None | – |

| 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 |
|---|---|---|---|
| MaxCapacity (= Max. Last in Director) | 4 | Maschine meldet für sich maximale Kapazität, d. h. Höchstlastindex | Stellen Sie sicher, dass alle Hypervisors eingeschaltet sind. Fügen Sie den betroffenen Bereitstellungsgruppen weitere Maschinen hinzu, indem Sie dem Hypervisor mehr Kapazität hinzufügen oder indem Sie weitere Hypervisoren hinzufügen. |
| 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. |
| None | 0 | - | - |

### Grund für die nicht vorhandene Registrierung von Maschinen (Fehlertyp “nicht registriert”oder “unbekannt”)

| Fehlercode | Fehlercode-ID | Problem | Aktion |
|---|---|---|---|
| AgentShutdown | 0 | Der VDA wurde ordnungsgemäß heruntergefahren. | Schalten Sie den VDA ein, wenn er nicht aufgrund von Energieverwaltungsrichtlinien deaktiviert sein soll. Überprüfen die Ereignisprotokolle auf Fehler. |
| AgentSuspended | 1 | Der VDA ist im Ruhezustand oder Energiesparmodus. | Schalten Sie den VDA aus dem Ruhezustand um in den Betrieb. Deaktivieren Sie den Ruhezustand für Citrix Virtual Apps and Desktops-VDAs über die Energieeinstellungen. |
| IncompatibleVersion | 100 | Der VDA kann wegen einer Diskrepanz in den Citrix Protokollversionen nicht mit dem Delivery Controller kommunizieren. | Stellen Sie sicher, dass die Versionen von VDA und Delivery Controller dieselben sind. |

| Fehlercode | Fehlercode-ID | Problem | Aktion |
| --- | --- | --- | --- |
| AgentAddressResolutionFailed | 101 | Der Delivery Controller konnte die IP-Adresse des VDAs nicht auflösen. | Stellen Sie sicher, dass das VDA-Maschinenkonto in AD vorhanden ist. Ist dies nicht der Fall, erstellen Sie es. Überprüfen Sie den Namen und die IP-Adresse des VDAs in DNS. Sind sie nicht korrekt, korrigieren Sie sie. Ist das Problem verbreitet, prüfen Sie die DNS-Einstellungen auf den Delivery Controllern. Überprüfen Sie die DNS-Auflösung über den Controller mit dem Befehl `nslookup`. |
| | 101 | Der Delivery Controller konnte die IP-Adresse des VDAs nicht auflösen. | Stellen Sie sicher, dass das VDA-Maschinenkonto in AD vorhanden ist. Ist dies nicht der Fall, erstellen Sie es. Überprüfen Sie den Namen und die IP-Adresse des VDAs in DNS. Sind sie nicht korrekt, korrigieren Sie sie. |

| Fehlercode | Fehlercode-ID | Problem | Aktion |
| --- | --- | --- | --- |
| AgentNotContactable | 102 | Zwischen dem Delivery Controller und dem VDA ist ein Kommunikationsproblem aufgetreten. | Prüfen Sie per Ping, ob Delivery Controller und VDA kommunizieren können. Ist dies nicht der Fall, lösen Sie jegliche Probleme mit der Firewall und dem Netzwerk. Die Anweisungen zur Problembehandlung im Knowledge Center-Artikel Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668) enthalten Informationen zu häufigen Ursachen für Kommunikationsprobleme zwischen Controller und VDA. |

| Fehlercode | Fehlercode-ID | Problem | Aktion |
|---|---|---|---|
| | 102 | Zwischen dem Delivery Controller und dem VDA ist ein Kommunikationsproblem aufgetreten. | Die Anweisungen zur Problembehandlung im Knowledge Center-Artikel Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668) enthalten Informationen zu häufigen Ursachen für Kommunikationsprobleme zwischen Controller und VDA. Wenden Sie sich an den Citrix Support. |
| AgentWrongActiveDirectoryOU | 103 | Bei der Active Directory-Ermittlung ist ein Konfigurationsfehler aufgetreten. Die in der VDA-Registrierung konfigurierte sitespezifische Organisationseinheit, in der die Informationen zum Site-Controller in Active Directory gespeichert werden, ist für eine andere Site. | Stellen Sie sicher, dass die Active Directory-Konfiguration richtig ist, oder überprüfen Sie die Registrierungseinstellungen. |

| Fehlercode | Fehlercode-ID | Problem | Aktion |
|---|---|---|---|
| EmptyRegistrationRequest | 104 | Die vom VDA an den Delivery Controller gesendete Registrierungsanforderung war leer. Grund kann eine beschädigte VDA-Softwareinstallation sein. | Starten Sie den Desktopdienst auf dem VDA neu, um den Registrierungsvorgang neu zu starten, und validieren Sie die VDA-Registrierung mit dem Anwendungsereignisprotokoll. |
| MissingRegistrationCapabilities | 105 | Die VDA-Version ist nicht mit dem Delivery Controller kompatibel. | Aktualisieren Sie den VDA oder entfernen Sie den VDA und installieren Sie ihn neu. |
| MissingAgentVersion | 106 | Die VDA-Version ist nicht mit dem Delivery Controller kompatibel. | Installieren Sie die VDA-Software neu, wenn sich das Problem auf alle Maschinen auswirkt. |

| Fehlercode | Fehlercode-ID | Problem | Aktion |
| --- | --- | --- | --- |
| InconsistentRegistrationCapabilities | 107 | Der VDA kann seine Funktionen nicht an den Broker melden. Dies kann auf eine fehlende Kompatibilität zwischen VDA- und des Delivery Controller-Version zurückzuführen sein. Die Registrierungsfunktionen, die sich mit jeder Version ändern, werden in einer Form ausgedrückt, die nicht mit der Registrierungsanforderung übereinstimmt. | Stellen Sie sicher, dass die Versionen von VDA und Delivery Controller dieselben sind. |
| NotLicensedForFeature | 108 | Das Feature, das Sie verwenden möchten, ist nicht lizenziert. | Überprüfen Sie die Edition der Citrix Lizenzierung oder entfernen Sie den VDA und installieren Sie ihn neu. |
| | 108 | Das Feature, das Sie verwenden möchten, ist nicht lizenziert. | Wenden Sie sich an den Citrix Support. |
| UnsupportedCredentialSecurityversion | 109 | VDA und Delivery Controller verwenden nicht dieselben Verschlüsselungsmethoden. | Stellen Sie sicher, dass die Versionen von VDA und Delivery Controller dieselben sind. |

| Fehlercode | Fehlercode-ID | Problem | Aktion |
| --- | --- | --- | --- |
| InvalidRegistrationRequest | 110 | Der VDA hat eine Registrierungsanforderung an den Broker gesendet, aber der Inhalt der Anforderung ist beschädigt oder ungültig. | Die Anweisungen zur Problembehandlung im Knowledge Center-Artikel Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668) enthalten Informationen zu häufigen Ursachen für Kommunikationsprobleme zwischen Controller und VDA. |
| SingleMultiSessionMismatch | 111 | Der Betriebssystemtyp des VDAs ist nicht mit dem Maschinenkatalog oder der Bereitstellungsgruppe kompatibel. | Fügen Sie den VDA dem richtigen Maschinenkatalogtyp oder der Bereitstellungsgruppe hinzu, die Maschinen mit dem gleichen Betriebssystem enthalten. |
| FunctionalLevelTooLowForCatalog | 112 | Der Maschinenkatalog hat eine höhere VDA-Funktionsebene als die installierte VDA-Version. | Stellen Sie sicher, dass die Funktionsebene des Maschinenkatalogs auf dem VDA mit der des VDAs übereinstimmt. Aktualisieren oder downgraden Sie den Maschinenkatalog so, dass er dem VDA entspricht. |

| Fehlercode | Fehlercode-ID | Problem | Aktion |
| --- | --- | --- | --- |
| FunctionalLevelTooLowForDesktopGroup | 113 | 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. |

## Hinweise zu Drittanbietern

June 27, 2024

Dieses Release von Citrix Virtual Apps and Desktops enthält ggf. Software von Drittanbietern, die gemäß den in den folgenden Dokumenten aufgeführten Bestimmungen lizenziert ist:

- Citrix Virtual Apps and Desktops –Hinweise zu Drittanbietern (PDF-Download)
- Non-Commercial Software Disclosures For FlexNet Publisher 2017 (11.15.0.0) (PDF Download)
- FlexNet Publisher Documentation Supplement Third Party and Open Source Software used in FlexNet Publisher 11.15.0 (PDF Download)

## SDKs und APIs

June 27, 2024

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.

Dieses Produkt unterstützt die PowerShell-Versionen 3 bis 5.

### 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. Um das Snap-In (und nicht das Modul) zu verwenden, 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.

### REST APIs für Citrix Virtual Apps and Desktops Service

REST-APIs für Citrix Virtual Apps and Desktops ermöglichen die automatisierte Verwaltung von Ressourcen innerhalb einer Citrix Virtual Apps and Desktops-Bereitstellung.

Die REST APIs für Citrix Virtual Apps and Desktops stehen unter https://developer.cloud.com/citrix-workspace/citrix-daas-rest-apis/docs/citrix-virtual-apps-and-desktops-apis zur Verfügung. APIs, die nicht für Citrix Virtual Apps and Desktops vorgesehen sind, sind entsprechend gekennzeichnet. Folgen Sie den Anweisungen auf der Seite, um den Zugriff auf den API-Dienst zu konfigurieren und die APIs zur Verwaltung und Optimierung Ihrer Ressourcen zu verwenden.

### 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.