XenApp und XenDesktop 7.7

May 17, 2016

Neue Funktionen

In XenApp 7.7 und XenDesktop 7.7 behobene Probleme

Bekannte Probleme in XenApp 7.7 und XenDesktop 7.7

Nicht in diesem Release enthaltene Features

Hinweise zu Drittanbietern

Systemanforderungen

Technische Übersicht

Konzepte und Komponenten

Active Directory

Datenbanken

Bereitstellungsmethoden

Referenzarchitekturen

Designanleitungen

Implementierungsanleitungen

Installation und Konfiguration

Vorbereiten der Installation

Installieren über die grafische Oberfläche

Installieren über die Befehlszeile

Installieren von VDAs mit Skripts

Installieren von VDAs unter Red Hat Linux

Installieren von VDAs mit SUSE Linux

Erstellen einer Site

Erstellen von Maschinenkatalogen

Verwalten von Maschinenkatalogen

Erstellen von Bereitstellungsgruppen

Verwalten von Bereitstellungsgruppen

Remote-PC-Zugriff

App-V

Lokaler App-Zugriff und URL-Umleitung

Server-VDI

Personal vDisk

Entfernen von Komponenten

Upgrades und Migration

Upgrade einer Bereitstellung

Migrieren von XenApp 6.x

Migrieren von XenDesktop 4

Sicherheit

Sicherheit – Überlegungen und bewährte Methoden

Delegierte Administration

Smartcards

Transport Layer Security (TLS)

Sicherheit mit Citrix XenApp und XenDesktop: Erste Schritte

Drucken

Beispiel einer Druckkonfiguration

Bewährte Methoden, Sicherheitsüberlegungen und Standardvorgänge

Druckrichtlinien und -einstellungen

Bereitstellen von Druckern

Pflege der Druckumgebung

HDX

Flash-Umleitung

HDX 3D Pro

GPU-Beschleunigung für Windows Desktopbetriebssysteme

GPU-Beschleunigung für Windows-Serverbetriebssystem

OpenGL Software Accelerator

Audiofeatures

Prioritäten für den Netzwerkdatenverkehr

Überlegungen zu USB und Clientlaufwerk

Thinwire-Kompatibilitätsmodus

Framehawk Virtual Channel

Richtlinien

Arbeiten mit Richtlinien

Richtlinienvorlagen

Erstellen von Richtlinien

Vergleichen, Priorisieren, Modellieren und Problembehandlung für Richtlinien

Standardrichtlinieneinstellungen

Referenz für Richtlinieneinstellungen

Verwaltung

Lizenzierung

Zonen

Verbindungen und Ressourcen

Verbindungsleasing

Virtuelle IP-Adressen und virtuelles Loopback

Delivery Controller

Sitzungen

Verwenden der Suche in Studio

Unterstützung für IPv4/IPv6

Clientordnerumleitung

Benutzerprofile

Überwachung

Sitzungsaufzeichnung

Konfigurationsprotokollierung

Überwachen von Personal vDisks

Director

Erweiterte Konfiguration

Überwachen von Bereitstellungen

Warnungen und Benachrichtigungen

Delegierte Administration und Director

Konfigurieren von Berechtigungen für VDAs vor XenDesktop 7

Konfigurieren von HDX Insight

Neue Funktionen

Feb 29, 2016

XenApp 7.7 und XenDesktop 7.7

Dieses Produktrelease enthält die folgenden neuen und erweiterten Features.

- **Zonen**

  In Bereitstellungen mit weit auseinanderliegenden Standorten in einem WAN kann es zu Latenz- und Zuverlässigkeitsproblemen kommen. Mit Zonen können Benutzer an entfernten Standorten eine Verbindung mit lokalen Ressourcen herstellen, ohne dass die Verbindungen durch große WAN-Segmente laufen müssen. Zonen gestatten eine effektive Siteverwaltung über eine einzelne Citrix Studio-Konsole, Citrix Director und die Sitedatenbank. Auf diese Weise können die Kosten für Bereitstellung, Personalbesetzung, Lizenzierung und Pflege 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.

  Weitere Informationen finden Sie in dem Artikel Zonen.

- **Verbesserungen an Abläufen und Konfiguration der Datenbanken**

  Bei der Siteerstellung können Sie nun separate Speicherorte für die Site-, die Konfigurationsprotokollierungs- und die Überwachungsdatenbank angeben. Später können Sie den Speicherort aller drei Datenbanken ändern. In vorherigen Releases wurden alle drei Datenbanken an der gleichen Adresse erstellt, die später nicht geändert werden konnte.

  Sie können jetzt beim Erstellen einer Site und zu einem späteren Zeitpunkt weitere Delivery Controller hinzufügen. In vorherigen Releases konnten weitere Controller erst nach dem Erstellen der Site hinzugefügt werden.

  Weitere Informationen finden Sie in den Artikeln Datenbanken und Controller.

- **Anwendungslimits**

  Durch Konfigurieren von Anwendungslimits können Sie die Anwendungsnutzung verwalten. Sie können z. B. die Zahl der Benutzer, die gleichzeitig auf eine Anwendung zugreifen, beschränken. Analog dazu können Sie über Anwendungslimits die Zahl gleichzeitiger Instanzen ressourcenintensiver Anwendungen limitieren, um die Serverleistung zu gewährleisten und eine Dienstverschlechterung zu vermeiden.

  Weitere Informationen finden Sie in dem Artikel Verwalten von Anwendungen.

- **Mehrere Benachrichtigungen vor Maschinenupdates und geplanten Neustarts**

  Sie können jetzt vor folgenden Aktionen wiederholt eine Benachrichtigung an die betroffenen Maschinen senden lassen:

  Update der Maschinen in einem Maschinenkatalog mit einem neuen Masterimage

  Neustart von Maschinen in einer Bereitstellungsgruppe gemäß Zeitplan

Wenn Sie angeben, dass die erste Nachricht 15 Minuten vor dem Update oder Neustart an die betroffenen Maschinen gesendet werden soll, können Sie außerdem vorgeben, dass die Nachricht alle fünf Minuten bis zum Update/Neustart wiederholt werden soll.

Weitere Informationen finden Sie in den Artikeln Maschinenkataloge und Verwalten von Maschinen in Bereitstellungsgruppen.

- **API-Unterstützung für die Verwaltung des Sitzungsroamings**

  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. Ebenso folgen Drucker und andere Ressourcen, die einer Anwendung zugewiesen sind.

  Sie können das Sitzungsroaming jetzt mit dem PowerShell-SDK anpassen. In der vorherigen Version war dies ein experimentelles Feature.

  Weitere Informationen finden Sie im Artikel Sitzungen.

- **API-Unterstützung für das Provisioning von VMs über Hypervisor-Vorlagen**

  Wenn Sie einen Maschinenkatalog mit dem PowerShell-SDK erstellen oder aktualisieren, können Sie nun eine Vorlage aus anderen Hypervisor-Verbindungen wählen. Diese Option besteht zusätzlich zu der derzeitigen Auswahl von VM-Images und Snapshots.

- **Unterstützung für neue und zusätzliche Plattformen**

  Ausführliche Informationen zu unterstützten Plattformen finden Sie im Artikel Systemanforderungen. Die Informationen über die Unterstützung der Versionen der Produkte anderer Hersteller werden regelmäßig aktualisiert.

  Standardmäßig wird zusammen mit dem Delivery Controller SQL Server 2012 Express SP2 installiert. SP1 wird nicht mehr installiert.

  Mit den Installationsprogrammen werden jetzt automatisch neuere Microsoft Visual C++-Laufzeitversionen bereitgestellt: 32-Bit und 64-Bit Microsoft Visual C++ 2013, 2010 SP1 und 2008 SP1. Visual C++ 2005 wird nicht mehr bereitgestellt.

  Sie können Studio und VDAs für Windows-Desktopbetriebssysteme auf Maschinen mit Windows 10 installieren.

  Sie können Verbindungen mit Microsoft Azure-Virtualisierungsressourcen erstellen.

Citrix Receiver für Mac und Citrix Receiver für Linux sind nicht mehr im Produkt-ISO-Image enthalten. Sie oder die Benutzer können diese Citrix Receiver-Versionen von der Citrix Website herunterladen und installieren. Alternativ können Sie diese Citrix Receiver-Versionen auf dem StoreFront-Server zur Verfügung stellen. Informationen hierzu finden Sie im Abschnitt Verfügbarmachen von Citrix Receiver-Installationsdateien auf dem Server in der Dokumentation zu StoreFront 3.0.x bzw. in der Dokumentation zu der von Ihnen verwendeten StoreFront-Version.

Citrix Director

Die in diesem Release enthaltene Director-Version bietet die folgenden neuen und erweiterten Features:

- **Proaktive Überwachung und Warnungen**

  Sie können jetzt proaktive Benachrichtigungen bei Erreichen von Schwellenwerten konfigurieren. Dies ermöglicht schnellere Reaktionen, selbst wenn Sie gerade nicht an der Überwachungskonsole sind.

  Weitere Informationen finden Sie unter Warnungen und Benachrichtigungen.

- **SCOM-Integration**

  In Bereitstellungen, die mit Microsoft System Center 2012 - Operations Manager überwacht werden, können SCOM-Warnungen im Dashboard und in anderen Ansichten der obersten Ebene in Director angezeigt werden. Wenn beispielsweise Verbindungen mit unterstützten Hypervisoren fehlschlagen, kann der Administrator Director auf entsprechende SCOM-Warnungen prüfen. Anschließend kann er bei Bedarf zur Operations Manager-Konsole wechseln, um weitere Informationen zur Problembehandlung anzuzeigen.

  Weitere Informationen finden Sie unter SCOM-Warnungen.

- **Windows-Authentifizierung**

  Director unterstützt jetzt die integrierte Windows-Authentifizierung. Die Windows-Anmeldeinformationen von Benutzern werden für das Single Sign-On automatisch beim Zugriff auf Director verwendet. Dadurch können Benutzer sich mit einem beliebigen Anmeldeinformationsanbieter und zugehöriger Hardware bei ihrer Maschine anmelden und die entsprechende Identität für den Zugriff auf Director verwenden.

  Weitere Informationen finden Sie unter Verwenden von Director mit der integrierten Windows-Authentifizierung.

- **Nutzung von Desktop- und Serverbetriebssystem**

  In der Ansicht "Trends" wird nun die Desktopbetriebssystemnutzung nach Site und Bereitstellungsgruppe und die Serverbetriebssystemnutzung nach Site, Bereitstellungsgruppe und Maschine angezeigt. Dies ist eine Echtzeitansicht der Betriebssystemnutzung, die eine schnelle Beurteilung der Kapazitätsanforderungen der Site gestattet.

  Weitere Informationen finden Sie unter Siteübergreifendes Überwachen von Verlaufstrends.

- **Anwendungslimits in Director**

  In Studio konfigurierte Anwendungslimits werden in vorhandenen Ansichten und Aufstellungen in Director angezeigt. Unter "Benutzerverbindungsfehler" im Dashboard wird beispielsweise angezeigt, wenn eine Verbindung aufgrund der Überschreitung eines Anwendungslimits fehlschlägt.

  Weitere Informationen finden Sie unter Anwendungslimits.

In XenApp 7.7 und XenDesktop 7.7 behobene Probleme

Feb 29, 2016

Die folgenden Probleme wurden in diesem Release behoben:

- Wenn mehrere Benutzer in zeitgleichen Studio-Sitzungen Richtlinien erstellen, überschreibt die zuletzt erstellte Richtlinie die älteren, wenn Desktop Studio aktualisiert wird.

  [#LA5533]

- Wenn Sie auf den Maschinenkatalog in Desktop Studio klicken, dauert es ggf. lange, bis die Kataloge angezeigt werden. Auch die Hostinginformationen werden erst nach längerer Wartezeit angezeigt.

  [#LC0237]

- Dieser Fix behebt ein Speicherproblem in einer Hintergrundkomponente.

  [#LC0320]

- Dieser Fix behebt Probleme mit der Erzwingung von Bereitstellungsgruppenrichtlinien.

  [#LC0559]

- Citrix Studio erkennt möglicherweise die XenDesktop App Edition-Lizenz nicht und folgende Fehlermeldung wird angezeigt:

  Keine gültige Lizenz gefunden

  Keine entsprechenden Lizenzen sind verfügbar. Überprüfen Sie die Lizenzserveradresse und dass Produktedition und -modell richtig angegeben sind.

  [#LC0822]

- Beim Aktualisieren eines Maschinenerstellungsdienste-Maschineimages mit vielen Snapshots kann Microsoft Management Console unerwartet schließen.

  [#LC0853]

- Durch diese Verbesserung werden in Citrix Studio die richtigen Benutzerzuweisungsdaten beim Hinzufügen von Benutzern aus mehreren Sites in einer Active Directory-Domäne angezeigt.

  [#LC0889]

- Wenn die Einstellungen "IncludedClientIPFilterEnabled" und "ExcludedClientIPFilterEnabled" auf "True" festgelegt sind, fehlen in der Bereitstellungsgruppe in Desktop Studio möglicherweise Benutzergruppen. Außerdem können die Benutzer, wenn die Einstellung "IncludedClientIPFilterEnabled" auf "True" festgelegt ist, ihre Ressourcen nach Anmeldung beim Webinterface oder bei StoreFront nicht sehen.

[#LC0892]

- Durch diese Verbesserung werden in Citrix Studio die richtigen Benutzerzuweisungsdaten beim Hinzufügen von Benutzern aus mehreren Sites in einer Active Directory-Domäne angezeigt.

  [#LC0955]

- Microsoft Management Console schlägt fehl, wenn beim Schließen von Desktop Studio im Navigationsbereich nicht "Konsolenstamm" ausgewählt ist.

  [#LC1314]

- Symbole veröffentlichter Anwendungen werden nicht in Desktop Studio angezeigt.

  [#LC1418]

- Wenn sich die Eigenschaft einer Anwendung im Fenster "Anwendungen" ändert, kann die Priorität der Bereitstellungsgruppen auf Null wechseln.

  [#LC1489]

- Nach dem Ändern der Webinterface-Portnummer kann in Desktop Studio fälschlicherweise die Aufforderung zu einem Lizenzupgrade angezeigt werden.

  [#LC1575]

- Der Versuch einer Konfiguration einer neuen Site mit dem XenDesktop PowerShell-SDK-Befehl "New-XDSite" ohne Konfiguration der Lizenzierung und anschließende Versuche den Befehl "Get-XDSite" auszuführen, schlagen fehl. Es wird gemeldet, dass das Upgrade noch nicht fertig gestellt ist, und dass mit dem Befehl "Get-XDUpgradeStatus" ermittelt werden soll, welche Schritte noch ausstehen.

  [#LC1612]

- Enthält der NetBIOS-Domänenname ein kaufmännisches Und (&), kann Citrix Studio nicht gestartet werden. Es wird die Fehlermeldung "Sie sind nicht zum Ausführen dieses Vorgangs autorisiert" mit dem Code XDDS:72182E6B angezeigt.

  [#LC1646]

- Wenn ein Benutzer Vorabstart oder Sitzungsfortbestehen in Citrix Studio konfiguriert, wird die Eigenschaft "MaxTimeBeforeDisconnect " statt auf den Standardwert von 15 Minuten auf 0 Minuten festgelegt.

  [#LC1706]

- Nach dem Upgrade auf XenDesktop 7.6 dauert es möglicherweise drei oder vier Minuten, bis die Kataloge oder Hostinginformationen in Desktop Studio angezeigt werden.

  [#LC1851]

- Beim domänenübergreifenden Hinzufügen von Benutzern zu einer Bereitstellungsgruppe löst Citrix Studio deren tatsächliche Domäne in das lokale Domänenkonto auf.

  [#LC1886]

- Wenn ein Delivery Controller offline geht oder aus anderen Gründen nicht verfügbar ist, wird Citrix Studio möglicherweise

langsam ausgeführt.

[#LC1891]

- Das Ausführen des Assistenten zum Erstellen von Katalogen kann fehlschlagen. Das Problem tritt auf, wenn einer der verbundenen Hypervisors im Wartungsmodus ist.

  [#LC1916]

- Beim Ausführen einer Abfrage in Citrix Studio, die mit dem Operator "is empty" gespeichert wurde, wird der Operator durch den Standardoperator ersetzt.

  [#LC1940]

- Automatische Upgrades einer Site von XenDesktop 7.5 auf 7.6 können fehlschlagen, weil die Eigenschaft "binding" in Brokerdienstinstanzen bei der Überprüfung der neuen und vorhandenen Instanzen möglicherweise nicht richtig verglichen wird. Dies kann dazu führen, dass ein Fehler aufgrund einer bereits registrierten Dienstinstanz auftritt. Das Problem tritt auf, wenn versucht wird, die Dienstendpunkte zu registrieren, ohne die Registrierung der vorhandenen Endpunkte aufzuheben.

  [#LC2043]

- Nach einem erfolgreichen Upgrade von XenDesktop 5.x oder 7.x auf XenDesktop 7.6 kann beim Starten von Studio folgende Fehlermeldung angezeigt werden:

  Upgrade der übrigen Delivery Controller durchführen

  In der Fehlermeldung ist der Name des Lizenzservers aufgeführt, obwohl der Delivery Controller nicht auf dem Lizenzserver installiert ist.

  [#LC2044]

- Studio kann möglicherweise keine Verbindung mit der Site herstellen, wenn die SDK-Schnittstellenportnummer im zentralen Konfigurationsdienst (CCS) geändert wurde.

  [#LC2045]

- Ein Versuch, ein Upgrade der Site auf die aktuelle Version des Produkts durchzuführen, kann fehlschlagen. Das Problem tritt auf, wenn die Set-ConfigSite-Befehle die aktualisierten Werte nicht abrufen können.

  [#LC2047]

- Beim Hinzufügen oder Erstellen eines Citrix Administrators in Citrix Studio mit einem Benutzer oder einer Gruppe, dessen bzw. deren Name einen oder mehrere Unterstriche enthält (z. B. get\dl_lab_gruppe), wird der erste Unterstrich nicht in den Details der Administratorenliste angezeigt. Der Name erscheint als "dllab_gruppe".

  [#LC2284]

- Beim Zusammenfassen von XenApp- und XenDesktop-Lizenzen mit demselben Subscription Advantage-Ablaufdatum in einer Lizenzdatei werden möglicherweise nicht alle XenApp-Lizenzen in Studio angezeigt.

  [#LC2325]

- Wird in Bereitstellungsgruppen versucht, einen Anwendungsordner mit dem Wort "Applications" zu erstellen, können

möglicherweise keine Unterordner erstellt werden.

[#LC2349]

- Beim Zusammenfassen von XenApp- und XenDesktop-Lizenzen mit demselben Subscription Advantage-Ablaufdatum in einer Lizenzdatei werden möglicherweise nicht alle XenApp-Lizenzen in Studio angezeigt.

  [#LC2350]

- Beim Erstellen einer benutzerdefinierten Rolle für Administratoren wird gemeldet, dass der angegebene Schlüssel nicht im Wörterbuch enthalten ist. Derselbe Fehler wird gemeldet, wenn Desktop Studio zum ersten Mal mit einem Administratorkonto gestartet wird.

  [#LC2680]

- Citrix Studio erkennt Citrix Service Provider-Lizenzen möglicherweise nicht und es wird folgende Fehlermeldung angezeigt:

  Keine gültige Lizenz gefunden

  [#LC2813]

- Ist eine Active Directory-Gruppe Besitzer der Datenbank, können Versuche, einen XenDesktop-Controller aus einer Site zu entfernen, fehlschlagen.

  [#LC2912]

- Nach der Installation von Hotfix DStudio760WX64001 wird möglicherweise ein "Zugriff verweigert"-Fehler angezeigt, wenn Sie versuchen, die Sichtbarkeit von Anwendungen für Benutzer einzuschränken.

  Dieses Problem tritt nur in Umgebungen mit unidirektionaler Vertrauensstellung zwischen Domänen auf.

  [#LC2956]

- Versuche, eine Bereitstellungsgruppe mit mehreren Desktops über Befehle oder Studio zu aktualisieren, schlagen mit der folgenden Fehlermeldung fehl:

  - Object reference not set to an instance of an object.
  - Fehlercode: XDDS:0E01FE12

  [#LC2958]

- Benutzereinstellungen werden gelöscht, wenn unter "Bereitstellungsgruppe bearbeiten" auf der Seite "Maschinenzuweisung" im Bereich "Benutzer" Änderungen vorgenommen werden. Das Problem tritt auf, wenn Benutzer manuell hinzugefügt oder aus einer Microsoft Excel-CSV-Datei importiert werden.

  [#LC3267]

- Diese Erweiterung macht das Feld "Hostingservername" in den Suchansichten für Desktopbetriebssystemmaschinen und Serverbetriebssystemmaschinen in Desktop Studio verfügbar.

  [#LC3343]

- Diese Erweiterung ist für gemischte Umgebungen mit einem XenDesktop-Controller der Version 7.6 oder höher und VDAs

der Version 7.1 vorgesehen. Wenn Sie dieses Update auf einen solchen VDA anwenden, kann der Controller der höheren Version von diesem Hotfixbestandsinformationen abrufen.

[#LC0248]

- Wenn ein Benutzer einen Katalog aktualisiert, wird in der Konfigurationsprotokollierung angezeigt, dass die Aktualisierung erfolgreich war, in der Ansicht "Aufgabendetails" wird jedoch für eine der Aufgaben gemeldet, dass die Freigabe des Provisioningschemas fehlgeschlagen ist.

  [#LC0518]

- Wenn Benutzer versuchen, den gepoolten Katalog unter XenServer zu löschen und dann den Katalog aktualisieren, werden die Basisdatenträger nicht aus dem Speicher entfernt und die Anzahl der Basisdatenträger kann steigen.

  [#LC0577]

- Die Sitzungszuverlässigkeit kann weder über das Active Directory-Gruppenrichtlinienobjekt noch über Desktop Studio in VDA 7.x-Sitzungen, die mit XenDesktop 5.6-Desktop Delivery Controllern (DDCs) starten, deaktiviert werden.

  [#LC0878]

- Wird in Bereitstellungen mit Microsoft System Center Virtual Machine Manager und eigenständigem Hyper-V, in dem die VMs im Hyper-V-Stammlaufwerk gespeichert sind, eine VM mit den Maschinenerstellungsdiensten bereitgestellt und dann einer Desktopgruppe zugewiesen, wird im Controller ein Systemereignis mit der ID 2006 protokolliert.

  [#LC0905]

- Wird mit den Maschinenerstellungsdiensten eine gepoolte Maschine von einem Masterimage mit benutzerdefinierten VMX- und NVRAM-Einstellungen erstellt, werden diese Einstellungen nicht auf die neuen virtuellen Maschinen kopiert.

  [#LC0967]

- Liegt der XenServer-Parameter "TimeOffSe" auf der virtuellen Maschine mit dem Masterimage vor, schlägt die Erstellung des Katalogs für die Maschinenerstellungsdienste fehl. Um zu prüfen, ob der Parameter vorliegt, führen Sie in der XenServer-Konsole den Befehl "xe vm-list uuid= params=other-config" aus. Zum Beheben des Problems wenden Sie diesen Hotfix an oder entfernen Sie den Parameter mit dem XenServer-Befehl "xe vm-param-remove uuid= param-name=other-config param-key=timeoffset" manuell.

  [#LC1071]

- Der Überwachungsdienst löscht den Anwendungsinstanzverlauf vorzeitig nach sieben Tagen anstatt der standardmäßigen 90 Tage. Dies tritt in XenDesktop- und XenApp-Bereitstellungen mit Platinum Edition auf.

  [#LC1129]

- Die Summen der einzelnen Anwendungen auf der Registerkarte "Trends > Nutzung gehosteter Anwendungen" in Desktop Director sind ungleich der Gesamtsumme aller Anwendungen. Dies tritt in Umgebungen auf, die sieben Tage oder länger ausgeführt wurden.

  [#LC1130]

- Wenn Sie virtuelle Maschinen mit Desktop Studio und Maschinenerstellungsdienste erstellen und die VMs auf einem VMware-Hypervisor gehostet werden, können VMs, die Teil des Maschinenkatalogs sind, nicht aktualisiert werden. In

diesem Fall enthält das Maschinenerstellungsprotokoll eine Fehlermeldung, dass der virtuelle Datenträger nicht vorhanden ist, obwohl das Verzeichnis im Datenspeicher existiert.

[#LC1201]

- In manchen Amazon Web Services-Umgebungen schlägt die Bereitstellung von Desktops mit Maschinenerstellungsdienste fehl und der Fehler "No facility for disk upload" wird gemeldet, obwohl die Umgebung ordnungsgemäß konfiguriert ist.

  [#LC1295]

- Beim Provisioning von VDAs mit Maschinenerstellungsdienste ändert sich das Suffix der primären DNS für die VDAs.

  [#LC1300]

- Werden im Ereignisprotokoll zwei oder mehr Instanzen von Ereignis 3012 verzeichnet, dann werden auch die Ereignisse 3020 und 3021 im Protokoll aufgeführt und die Meldungen sind falsch. Durch diesen Fix werden die Ereignisse 3020 und 3021 richtig im Protokoll aufgeführt, wenn zwei oder mehr Instanzen von Ereignis 3012 verzeichnet werden.

  [#LC1425]

- Die Fehlermeldungen für Ereignis 1110 und 1111 im Ereignisprotokoll sind falsch. Durch diesen Fix werden die richtigen Meldungen im Ereignisprotokoll angezeigt:

  - Ereignis 1110: Um übermäßige Ereignisprotokollierung zu vermeiden, werden diese Meldungen (Ereignis-IDs 1100-1109, 1112-1118) zeitweilig vom Dienst unterdrückt.
  - Ereignis 111: Diesbezügliche Meldungen (Ereignis-IDs 1100-1109, 1112-1116) werden vom Dienst nicht mehr unterdrückt.

  [#LC1485]

- Ist ein VDA in einer freigegebenen Bereitstellungsgruppe mit Tags versehen und ein Tag wird in einem Richtlinienfilter verwendet, werden die Richtlinien nicht auf andere VDAs in der Bereitstellungsgruppe angewendet.

  [#LC1506]

- Nach Installation aller Updates in CTX141087 (Hotfixupdate 2 für XD 7.1 Delivery Controller x64) werden beim Zugriff auf Desktop Delivery Controller 7.1 die Anmeldedauerdaten nicht in Director 7.1 bzw. Director 7.6 angezeigt.

  [#LC1581]

- Das Erstellen neuer Kataloge schlägt nach einem Upgrade auf XenDesktop 7.6 fehl, wenn das VM-Masterimage eine Eigenschaft für die Virtualisierung geschachtelter Hardware (aktiviert unter VMware vSphere 5.1) enthält.

  [#LC1586]

- Werden viele Sitzungen innerhalb kurzer Zeit gestartet, dauert es möglicherweise lange, bis Sitzungsinformationen in Director angezeigt werden.

  [#LC1617]

- Enthält der NetBIOS-Domänenname ein kaufmännisches Und (&), kann Citrix Studio nicht gestartet werden. Es wird die Fehlermeldung "Sie sind nicht zum Ausführen dieses Vorgangs autorisiert" mit dem Code XDDS:72182E6B angezeigt.

[#LC1646]

- Durch diesen Fix wird ein Speicherproblem in einer grundlegenden Komponente behoben, das bei System Center Virtual Machine Manager-Verbindungen auftritt.

  [#LC1730]

- Enthält der Name einer Active Directory-Organisationseinheit Sonderzeichen, kann es vorkommen, dass der Brokerdienst keine Bindung mit der Organisationseinheit herstellen kann. Dies kann zu einer gesteigerten CPU-Auslastung führen. Darüber hinaus kann möglicherweise nicht mehr auf Studio zugegriffen werden und Dienste können unerwartet geschlossen werden.

  [#LC1979]

- Auf den Registerkarten der Seiten "Trends" und "Filteroptionen" in Desktop Director werden möglicherweise keine Daten angezeigt und es wird ein Fehler gemeldet.

  [#LC2035]

- Bei Ausführung des Befehls "Get-Help set-MonitorConfiguration -detailed" im Powershell-Snap-In wird die Fehlermeldung "GroomApplicationInstanceRetentionDays FIXME" angezeigt.

  [#LC2176]

- Die folgende Fehlermeldung wird ggf. fälschlicherweise jedes Mal im Anwendungsprotokoll verzeichnet, wenn Citrix Service Monitor gestartet wird, obwohl der Dienst einwandfrei funktioniert:

  Error querying the Broker via GetBrokerObjects to obtain 'Controller Machine Details'

  [#LC2239]

- Ist für einen delegierten Administrator die Benutzerzugriffssteuerung aktiviert, werden Updates für den Delivery Controller fälschlicherweise am Standardspeicherort installiert. Der Standardspeicherort ist "%systemroot\Programme\Citrix" und möglicherweise nicht mit dem Speicherort identisch, an dem Sie den Delivery Controller ursprünglich installiert haben.

  [#LC2252]

- Ist im VM-Masterimage unter VMware vSphere 6 mit GRID-Platine ein virtueller Grafikprozessor aktiviert, schlägt die Maschinenerstellung fehl.

  [#LC2326]

- Meldet sich ein Benutzer von einer Sitzung ab, wird das Enddatum in der Datenbank für alle in der Sitzung ausgeführten Anwendungsinstanzen und die vor Sitzungsende geschlossenen Anwendungen falsch aktualisiert.

  [#LC2435]

- Ein vom integrierten Hyper-V bereitgestellter VDA wird nach erfolgreichem Abonnement als nicht registriert angezeigt.

  [#LC2722]

- Wird nach dem Upgrade des Desktop Controllers von Version 7.x auf Version 7.6 der PowerShell-Befehl "Set-

MonitorConfiguration" ausgeführt, wird die folgende Fehlermeldung angezeigt:

A database operation failed and cannot be recovered.

[#LC2745]

- Der Versuch, einem Katalog über 999 virtuelle Maschinen hinzuzufügen, kann fehlschlagen.

  [#LC2873]

- Enthält der Name einer veröffentlichten Anwendung ein Leerzeichen am Ende, kann dies zu diversen Problemen führen. Diese Probleme treten auf, wenn Browsernamen aus dem Namen einer veröffentlichten Anwendung generiert werden, die abgeschnittene Namen mit einem Leerzeichen am Ende hat.

  [#LC2897]

- Durch diesen Fix werden die folgenden Probleme behoben:

  - Wenn für die Hostverbindung die Region US-East-1e konfiguriert ist, kann die Amazon Web Services-Verbindung zwar hergestellt werden, die Maschinenerstellung kann jedoch fehlschlagen.
  - Beim Hinzufügen einer AWS-Hostverbindung zur Verwendung von EU-Central-1 kann die Erstellung der Hostverbindung aufgrund eines Authentifizierungsfehlers fehlschlagen.

  [#LC3239]

- In Maschinenerstellungsdienste wird das Flag "AvailableForPlacement" von System Center Virtual Machine Manager 2012-Hosts möglicherweise ignoriert. Dies kann dazu führen, dass ein Host mit nicht ausreichenden Ressourcen ausgewählt wird und die Maschinenerstellung fehlschlägt.

  [#LC3426]

- Nach einem Upgrade auf XenDesktop 7.6 unter Verwendung des lokalen Systemkontos (normalerweise durch Tools zur elektronischen Softwareverteilung) kann der Analysedienst nicht gestartet werden.

  [#LC3493]

- Nach Installation des aktuellen Microsoft Update Rollups 7 in der System Center Virtual Machine Manager 2012 R2-Umgebung kann die Katalogerstellung mit Maschinenerstellungsdienste fehlschlagen.

  [#LC3822]

- Das Cmdlet "Add-XDController" weist dem Controller keine vollständigen benutzerdefinierten Datenbankverbindungszeichenfolgen zu.

  [#LC3860]

- Bei der Suche nach Benutzernamen in Director können wahllos Verzögerungen von bis zu zwei Minuten auftreten.

  [#LC1250]

- Werden viele Sitzungen innerhalb kurzer Zeit gestartet, dauert es möglicherweise lange, bis Sitzungsinformationen in Director angezeigt werden.

[#LC1617]

- Bei hoher Latenz kann die Citrix Gruppenrichtlinienengine (CitrixCseEngine.exe) Verzögerungen bei der Anmeldung verursachen.

  Um den Fix zu aktivieren, erstellen Sie die folgenden Registrierungsschlüssel:

  - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\GroupPolicy
    Name: GpoCacheEnabled
    Typ: REG_DWORD
    Wert: 1
  - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\GroupPolicy
    Name: CacheGpoExpireInHours
    Typ: REG_DWORD
    Wert: 5 bis 24

  [#LC0559]

- Microsoft Management Console schlägt fehl, wenn beim Schließen von Desktop Studio im Navigationsbereich nicht "Konsolenstamm" ausgewählt ist.

  [#LC1314]

- Der Lizenzserver besteht unter Umständen nicht den Payment Card Industry-Konformitätstest für Clickjacking, weil der Headertyp "X-Frame-Options" nicht festgelegt ist.

  [#LC1983]

- Das Hinzufügen von Domänengruppen, deren Name mehr als 32 Zeichen enthält, kann fehlschlagen.

  [#LC1986]

- Beim Hinzufügen oder Erstellen eines Citrix Administrators in Citrix Studio mit einem Benutzer oder einer Gruppe, dessen bzw. deren Name einen oder mehrere Unterstriche enthält (z. B. get\dl_lab_gruppe), wird der erste Unterstrich nicht in den Details der Administratorenliste angezeigt. Der Name erscheint als "dllab_gruppe".

  [#LC2284]

- Enthält der NetBIOS-Domänenname ein kaufmännisches Und (&), kann die Registerkarte "Lizenzierung" in Citrix Studio möglicherweise nicht geöffnet werden und es wird folgende Fehlermeldung angezeigt:

  Citrix Lizenzserver ist nicht verfügbar

  [#LC2728]

- Dieser Fix behebt Probleme mit der Erzwingung von Bereitstellungsgruppenrichtlinien.

  [#LC0559]

- Durch diesen Fix werden in Citrix Studio die richtigen Benutzerzuweisungsdaten beim Hinzufügen von Benutzern aus mehreren Sites in einer Active Directory-Domäne angezeigt.

  [#LC0889]

- Nach dem Ändern der Webinterface-Portnummer kann in Desktop Studio fälschlicherweise die Aufforderung zu einem Lizenzupgrade angezeigt werden.

  [#LC1575]

- Der Versuch einer Konfiguration einer neuen Site mit dem XenDesktop PowerShell-SDK-Befehl "New-XDSite" ohne Konfiguration der Lizenzierung und anschließende Versuche den Befehl "Get-XDSite" auszuführen, schlagen fehl. Es wird gemeldet, dass das Upgrade noch nicht fertig gestellt ist, und dass mit dem Befehl "Get-XDUpgradeStatus" ermittelt werden soll, welche Schritte noch ausstehen.

  [#LC1612]

- Wenn ein Benutzer Vorabstart oder Sitzungsfortbestehen in Citrix Studio konfiguriert, wird die Eigenschaft "MaxTimeBeforeDisconnect " statt auf den Standardwert von 15 Minuten auf 0 Minuten festgelegt.

  [#LC1706]

- Nach dem Upgrade auf XenDesktop 7.6 dauert es möglicherweise drei oder vier Minuten, bis die Kataloge oder Hostinginformationen in Desktop Studio angezeigt werden.

  [#LC1851]

- Wenn ein Delivery Controller offline geht oder aus anderen Gründen nicht verfügbar ist, wird Citrix Studio möglicherweise langsam ausgeführt.

  [#LC1891]

- Das Ausführen des Assistenten zum Erstellen von Katalogen kann fehlschlagen. Das Problem tritt auf, wenn einer der verbundenen Hypervisors im Wartungsmodus ist.

  [#LC1916]

- Automatische Upgrades einer Site von XenDesktop 7.5 auf 7.6 können fehlschlagen, weil die Eigenschaft "binding" in Brokerdienstinstanzen bei der Überprüfung der neuen und vorhandenen Instanzen möglicherweise nicht richtig verglichen wird. Dies kann dazu führen, dass ein Fehler aufgrund einer bereits registrierten Dienstinstanz auftritt. Das Problem tritt auf, wenn versucht wird, die Dienstendpunkte zu registrieren, ohne die Registrierung der vorhandenen Endpunkte aufzuheben.

  [#LC2043]

- Nach einem erfolgreichen Upgrade von XenDesktop 5.x oder 7.x auf XenDesktop 7.6 kann beim Starten von Studio folgende Fehlermeldung angezeigt werden:

  Upgrade der übrigen Delivery Controller durchführen

  In der Fehlermeldung ist der Name des Lizenzservers aufgeführt, obwohl der Delivery Controller nicht auf dem Lizenzserver installiert ist.

[#LC2044]

- Studio kann möglicherweise keine Verbindung mit der Site herstellen, wenn die SDK-Schnittstellenportnummer im zentralen Konfigurationsdienst (CCS) geändert wurde.

  [#LC2045]

- Ein Versuch, ein Upgrade der Site auf die aktuelle Version des Produkts durchzuführen, kann fehlschlagen. Das Problem tritt auf, wenn die Set-ConfigSite-Befehle die aktualisierten Werte nicht abrufen können.

  [#LC2047]

- In diesem Release kann das Flag *-enabled* in dem Befehl *Set-XDLogging -AdminAddress $ControllerName -AllowDisconnectedDatabase $true* verwendet werden.

  [#LC2162]

- Beim Zusammenfassen von XenApp- und XenDesktop-Lizenzen mit demselben Subscription Advantage-Ablaufdatum in einer Lizenzdatei werden möglicherweise nicht alle XenApp-Lizenzen in Studio angezeigt.

  [#LC2350]

- Beim Erstellen einer benutzerdefinierten Rolle für Administratoren wird gemeldet, dass der angegebene Schlüssel nicht im Wörterbuch enthalten ist. Derselbe Fehler wird gemeldet, wenn Desktop Studio zum ersten Mal mit einem Administratorkonto gestartet wird.

  [#LC2680]

- Ist eine Active Directory-Gruppe Besitzer der Datenbank, können Versuche, einen XenDesktop-Controller aus einer Site zu entfernen, fehlschlagen.

  [#LC2912]

- Nach der Installation von Hotfix DStudio760WX64001 wird möglicherweise ein "Zugriff verweigert"-Fehler angezeigt, wenn Sie versuchen, die Sichtbarkeit von Anwendungen für Benutzer einzuschränken.

  Dieses Problem tritt nur in Umgebungen mit unidirektionaler Vertrauensstellung zwischen Domänen auf.

  [#LC2956]

- Versuche, eine Bereitstellungsgruppe mit mehreren Desktops über Befehle oder Studio zu aktualisieren, schlagen mit der folgenden Fehlermeldung fehl:

  - Object reference not set to an instance of an object.
  - Fehlercode: XDDS:0E01FE12

  [#LC2958]

- Benutzereinstellungen werden gelöscht, wenn unter "Bereitstellungsgruppe bearbeiten" auf der Seite "Maschinenzuweisung" im Bereich "Benutzer" Änderungen vorgenommen werden. Das Problem tritt auf, wenn Benutzer manuell hinzugefügt oder aus einer Microsoft Excel-CSV-Datei importiert werden.

  [#LC3267]

- Diese Erweiterung macht das Feld "Hostingservername" in den Suchansichten für Desktopbetriebssystemmaschinen und Serverbetriebssystemmaschinen in Desktop Studio verfügbar.

  [#LC3343]

- Das Cmdlet "Add-XDController" weist dem Controller keine vollständigen benutzerdefinierten Datenbankverbindungszeichenfolgen zu.

  [#LC3860]

- This feature enhancement implements performance counters for the Universal Print Server and Universal Print Client. [#LC1820]

The versions of the VDA for Desktop OS included in XenApp and XenDesktop 7.6 Feature Pack 3 (7.6.300) and 7.6 LTSR are identical. The version included in XenApp and XenDesktop 7.7 contains the same fixes as Version 7.6.300, plus compatibility updates for XenApp and XenDesktop 7.7.

- Diese Funktionserweiterung führt Leistungsindikatoren für den universellen Druckerserver und den universellen Druckclient ein.
  [#LC1820]

Bekannte Probleme in XenApp 7.7 und XenDesktop 7.7

Feb 29, 2016

Der folgende Warnhinweis gilt für alle Workarounds, bei denen ein Registrierungseintrag geändert werden muss:

> **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. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.

In diesem Release bestehen die folgenden Probleme:

Installation und Upgrade

- Wenn Sie ein Upgrade von XenDesktop 5.6 auf XenApp und XenDesktop 7.6 und dann auf XenApp und XenDesktop 7.7 durchführen, können die Benutzer Desktops öffnen, aber keine Anwendungen starten. Workaround: Setzen Sie den Parameter "IncludeUsers" für die Zugriffsrichtlinie der aktualisierten Bereitstellungsgruppe manuell zurück. [#605506]
- Die Initialisierung des Brokerdiensts schlägt fehl, wenn Sie ein direktes Upgrade von XenApp und XenDesktop 7.6 auf XenApp und XenDesktop 7.7 durchführen, nachdem Sie den Linux- VDA mit dem veralteten Skript "update-BrokerServiceConfig.ps1" aktualisiert haben. Workaround: Installieren Sie HotFix2, bevor Sie das Upgrade durchführen. [#606649]
- Die neue Rollenkonfiguration wird bei Upgrades nicht immer angewendet. Als Folge werden Zonen nicht in Studio angezeigt. Workaround: Führen Sie den folgenden Befehl in PowerShell (Verzeichnis beachten). [#610875]:
  PS C:\Program Files\Citrix\XenDesktopPoshSdk\Module\Citrix.XenDesktop.Admin.V1\Citrix.XenDesktop.Admin\StudioRoleConfig> Import-AdminRoleConfiguration .\RoleConfigSigned.xml

Director

- Beim Upgrade von XenDesktop Enterprise Edition auf XenDesktop Platinum Edition sind Delivery Group-basierte Nutzungsdaten und benutzerbasierte Nutzungsdaten inkonsistent, wenn der Berichtszeitraum die Zeit enthält, zu der das Upgrade durchgeführt wurde. [#597138]
- Auf VDA-Maschinen unter Windows 10 werden vom Benutzer gestartete Anwendungen nicht im Mini-Task-Manager für getrennte oder wiederhergestellte Sitzungen angezeigt. [#603240]
- Wenn Sie für eine Richtlinie mit einer aktiven Warnung den Schwellenwert der entsprechenden Bedingung ändern, wirkt sich der geänderte Schwellenwert nicht nur auf die neuen Warnungsdetails sondern auch auf die alten aus. [#602711]

HDX

- Bei Sitzungen mit mehreren Monitoren auf Windows 10-Desktops können Benutzer mit der Standardanwendung für die Anzeigeeinstellungen die Position der Monitore ändern und die Änderungen anwenden. Solche Änderungen führen zu unkontrollierten Mausbewegungen und erschweren die Interaktion mit der Sitzung oder machen diese unmöglich. Zum Beheben des Problems trennen Sie die Sitzungsverbindung und stellen Sie sie anschließend wieder her. Zur Problemvermeidung unterbinden Sie die Verwendung der Anwendung durch die Benutzer über die folgende Microsoft-Gruppenrichtlinieneinstellung: **Benutzer > Administrative Vorlagen > Systemsteuerung > Anzeige > Systemsteuerungsoption "Anzeige" deaktivieren**. Sie können auch die Registrierungseinstellung HKLM\Software\Citrix\Graphics\SetNoDisplayCPLPolicy = 1 festlegen, durch die die Microsoft-Richtlinie während Sitzungen aktiviert und anschließend wieder auf den ursprünglichen Wert zurückgesetzt wird. In beiden Fällen wird durch die Verwendung der Richtlinie verhindert, dass Benutzer DPI- und andere, möglicherweise erforderliche Einstellungen ändern können. [#571552]

Azure-Plug-In

- In Azure gelten andere Benennungsregeln für virtuelle Maschinen als in Citrix Studio. Es ist daher möglich, VMs in Azure mit ungültigen Namen zu erstellen. Zur Vermeidung dieses Problems berücksichtigen Sie bei der Benennung von VMs in Azure die folgenden Regeln:
  - Die Länge muss zwischen 3 und 15 Zeichen liegen.
  - Der Name darf nur Buchstaben, Zahlen und Bindestriche enthalten.
  - Der Name muss mit einem Buchstaben beginnen und in einem Buchstaben oder einer Zahl enden.

Warnung: Namen, die diesen Regeln nicht entsprechen (z. B. solche, die mit einem Bindestrich beginnen oder Sonderzeichen enthalten), werden in Studio möglicherweise dennoch zugelassen. Ungültige Namen werden vom Plug-In nicht über die Benutzeroberfläche gemeldet. Wenn ein Problem auftritt, führt dies zu einem erheblichen Ausfall, der gemeldet wird.
[#554683]

Allgemein

- XenApp und XenDesktop 7.7 unterstützen ein neues Feature für eine stets aktivierte Protokollierung. Aus diesem Grund haben sich die bisherigen Tracingebenen geändert. Dies kann sich auf Umgebungen auswirken, in denen benutzerdefinierte Skripts zum Aktivieren der CDF-Traceaufzeichnung verwendet werden. Es gelten folgende neuen Richtlinien für die Traceaufzeichnung:

Bisherige Tracingebene	Neue Ebene (empfohlen)
0	9
1	9
2	10
3	10
4	11
5	12
6	13
7	14
8	15
9	16

[#605738]

- Wenn Sie eine XenApp-/XenDesktop-Site der Version 7.5 mit Studio der Version 7.7 verwalten, können Sie die Eigenschaften von Bereitstellungsgruppen nicht bearbeiten. Es wird ein interner Fehler gemeldet. Workaround: Verwenden Sie XenApp-/XenDesktop Studio 7.5 zum Bearbeiten von Bereitstellungsgruppen. [#605222]
- Wenn Sie sich über Connection Center von einer Anwendung abmelden, die auf einer Windows 10-VM gehostet wird, ohne Ihre Arbeit gespeichert zu haben, kann die Sitzung durch die entsprechenden Warnmeldungen einfrieren. Workaround: Speichern Sie Ihre Arbeit, bevor Sie sich abmelden. [#547674]
- Wenn Sie einer Site mehrere Delivery Controller gleichzeitig hinzufügen, kann Fehler auftreten, woraufhin die Datenbank aus einer Sicherungskopie wiederhergestellt werden muss. Fügen Sie zur Problemvermeidung Controller einzeln hinzu. Warten Sie jeweils bis zum Abschluss des Vorgangs, bevor Sie den nächsten Controller hinzufügen. [#607420]

Framehawk Virtual Channel

- Sitzungsaufzeichnung bzw. Smart Auditor werden für Framehawk nicht unterstützt.
- Framehawk wird in grafikintensiven Umgebungen mit hoher Last nicht unterstützt. Es wurde unter einer für XenApp und

XenDesktop normalen Arbeitslast (Wissensarbeiter, Büro-Apps) getestet.

- Clients mit mehreren Monitoren werden derzeit nicht unterstützt.
- Die Vd3dn.dll kann auf dem Client unter Testbedingungen, z. B. beim Ändern der Bandbreite und Latenz auf einem WAN-Emulator während einer Sitzung, abstürzen. Trennen Sie die Sitzung, bevor Sie Änderungen an den WAN-Emulatoreinstellungen vornehmen, und stellen Sie dann die Verbindung wieder her. Framehawk wird während des Sitzungshandshakes neu kalibriert.
- Wenn Sie sowohl Framehawk- als auch Legacy-Richtlinien für einen Benutzer aktivieren, gelten unter Desktopbetriebssystemen die Framehawk-Richtlinien und unter Serverbetriebssystemen die Legacy-Richtlinien.
- Bei Framehawk-Sitzungen können Probleme mit der Sitzungszuverlässigkeit aufgrund einer Reihe von Faktoren (z. B. Abziehen und Wiedereinstecken eines Netzwerkkabels bei laufender Sitzung) auftreten. [#592502]

Nicht in diesem Release enthaltene Features

Feb 29, 2016

Tipp: Wenn die neueste Version, mit der Sie vertraut sind, XenApp 6.5 (oder eine Vorversion) ist, sollten Sie sich auch die hier beschriebenen Unterschiede bei Architektur, Terminologie und Elementen ansehen.

Die folgenden Features werden derzeit nicht bereitgestellt oder werden nicht mehr unterstützt.

- **Für Fingereingabe optimierten Desktop starten:** Diese Einstellung wurde für Windows 10-Maschinen deaktiviert. Weitere Informationen finden Sie unter Einstellungen der Richtlinie "Mobilerfahrung".
- **SecureICA-Verschlüsselung unter 128 Bit**: In Releases vor 7.x war eine Verschlüsselung von Clientverbindungen für Basic-, 40-Bit-, 56-Bit- und 128-Bit-Verschlüsselung durch SecureICA möglich. In Releases aber Version 7 steht die SecureICA-Verschlüsselung nur für die 128-Bit-Verschlüsselung zur Verfügung.
- **Legacydrucken**: Die folgenden Druckfunktionen werden für Releases 7.x nicht unterstützt:
  - Abwärtskompatibilität für DOS-Clients und 16-Bit-Drucker, einschließlich Legacy-Clientdruckernamen.
  - Unterstützung für mit Windows 95 und Windows NT verbundene Drucker, einschließlich verbesserter erweiterter Druckereigenschaften und Win32FavorRetainedSetting.
  - Möglichkeit zum Aktivieren oder Deaktivieren automatisch gespeicherter und automatisch wiederhergestellter Drucker.
  - DefaultPrnFlag, eine Registrierungseinstellung für Server zum Aktivieren/Deaktivieren automatisch gespeicherter und automatisch wiederhergestellter Drucker, die in Benutzerprofilen auf dem Server gespeichert werden.
- **Secure Gateway**: In Releases vor 7.x wurden mit Secure Gateway sichere Verbindungen zwischen dem Server und den Benutzergeräten hergestellt. Die Sicherung externer Verbindungen erfolgt nun mit NetScaler Gateway.
- **Spiegeln von Benutzern**: In Releases vor 7.x steuerten Administratoren die Benutzer-zu-Benutzer-Spiegelung mit Richtlinien. In 7.x-Releases ist das Spiegeln von Endbenutzern ein integriertes Feature in Director, wobei die Windows-Remoteunterstützung den Administratoren das Spiegeln und Beheben von Problemen auf nahtlos bereitgestellten Anwendungen und virtuellen Desktops gestattet.
- **Energie- und Kapazitätsverwaltung**: In Releases vor 7.x wurde mit der Energie- und Kapazitätsverwaltung der Stromverbrauch reduziert und die Serverkapazität verwaltet. Microsoft Configuration Manager ist das Ersatztool für diese Funktion.
- **Flash v1-Umleitung**: Bei Clients, die nicht die Flash-Umleitung der zweiten Generation unterstützen (einschließlich Citrix Receiver für Windows vor Version 3.0, Citrix Receiver für Linux 11.100 und Citrix Online-Plug-In 12.1) erfolgt ein Fallback auf serverseitige Wiedergabe für Legacyfeatures der Flash-Umleitung. VDAs in 7.x-Releases unterstützen die Flash-Umleitungsfeatures der zweiten Generation.
- **Lokales Textecho**: Dieses Feature wurde mit früheren Windows-Anwendungstechnologien zur Beschleunigung der Anzeige eingegebenen Texts auf Benutzergeräten bei Verbindungen mit hoher Latenz eingesetzt. Aufgrund von Verbesserungen am Grafiksubsystem und HDX SuperCodec ist dieses Feature in 7.x-Releases nicht enthalten.
- **SmartAuditor**: In Releases vor 7.x konnte mit SmartAuditor die Bildschirmaktivität einer Benutzersitzung aufgezeichnet werden. Ab Version 7.6 Feature Pack 1 wurde diese Funktion durch die Sitzungsaufzeichnung ersetzt.
- **Single Sign-On**: Dieses Feature zur Gewährleistung der Kennwortsicherheit wird für Windows 8- und Windows Server 2012-Umgebungen nicht unterstützt. Es wird noch für Windows 2008 R2- und Windows 7-Umgebungen unterstützt, ist aber nicht in 7.x-Releases enthalten. Es ist auf der Downloadwebsite von Citrix verfügbar: http://citrix.com/downloads.
- **Oracle-Datenbankunterstützung**: 7.x-Releases benötigen eine SQL Server-Datenbank.
- **Systemüberwachung und -wiederherstellung (HMR)**: In Releases vor 7.x konnten von HMR Tests auf den Servern einer Serverfarm durchgeführt werden, um deren Zustand zu überwachen und mögliche Integritätsrisiken zu ermitteln. In 7.x-Releases bietet Director eine zentrale Ansicht der Systemintegrität, da die Überwachungs- und Warnfunktionen für

die ganze Infrastruktur innerhalb der Director-Konsole dargestellt werden.

- **Benutzerdefinierte ICA-Dateien**: Benutzerdefinierte ICA-Dateien wurden verwendet, um direkte Verbindungen von Benutzergeräten (mit der ICA-Datei) zu einer bestimmten Maschine herzustellen. In 7.x-Releases ist dieses Feature standardmäßig deaktiviert, kann aber für die normale Verwendung mit einer lokalen Gruppe aktiviert werden, oder im Modus für hohe Verfügbarkeit verwendet werden, falls der Controller nicht mehr verfügbar ist.
- **Management Pack für System Center Operations Manager (SCOM) 2007**: Das Management Pack für die Überwachung der Aktivität der Farmen mit SCOM unterstützt 7.x-Releases nicht.
- **CNAME-Funktion**: Die CNAME-Funktion war in Versionen vor 7.x standardmäßig aktiviert. Bereitstellungen, die von CNAME-Einträgen für FQDN-Umleitung und von der Verwendung von NetBIOS-Namen abhängig sind schlagen möglicherweise fehl. In 7.x-Releases bietet stattdessen die automatische Aktualisierung von Delivery Controllern, durch die die Liste der Controller automatisch aktualisiert wird und VDAs automatisch benachrichtigt werden, wenn Controller der Site hinzugefügt und aus ihr entfernt werden. Das Feature für automatische Controller-Updates ist in den Citrix Richtlinien standardmäßig aktiviert, kann jedoch durch Erstellen einer Richtlinie deaktiviert werden.
  Alternativ können Sie die CNAME-Funktion in der Registrierung wieder aktivieren, um mit der vorhandenen Bereitstellung fortzufahren und FQDN-Umleitung und die Verwendung von NetBIOS-Namen zuzulassen. Weitere Informationen finden Sie unter CTX137960.

- **Assistent für schnelles Bereitstellen**: In Studio-Releases vor 7.x konnte mit dieser Option eine vollständig installierte XenDesktop-Bereitstellung schnell bereitgestellt werden. Durch den neuen vereinfachten Installations- und Konfigurationsworkflow in XenDesktop 7.x ist der Assistent für schnelles Bereitstellen nicht mehr nötig.
- **Konfigurationsdatei für Remote PC-Dienst und PowerShell-Skript für die automatische Verwaltung**: Remote PC ist jetzt in Studio und den Controller integriert.
- **Workflow Studio**: In Releases vor 7.x war Workflow Studio die grafische Oberfläche für den Aufbau von Workflows für XenDesktop. Das Feature wird in 7.x-Releases nicht unterstützt.
- **Farbtiefe**: In Studio-Releases vor 7.6 wurde die Farbtiefe in den Benutzereinstellungen einer Bereitstellungsgruppe angegeben. Ab Version 7.6 kann die Farbtiefe für Bereitstellungsgruppen über das PowerShell-Cmdlet "New-BrokerDesktopGroup" oder "Set-BrokerDesktopGroup" festgelegt werden.
- **Starten nicht-veröffentlichter Programme bei Clientverbindung**: In Releases vor 7.x wurde über diese Citrix Richtlinieneinstellung angegeben, ob Startanwendungen oder veröffentlichte Anwendungen über ICA oder RDP auf dem Server gestartet werden sollten. In 7.x-Releases wird mit dieser Einstellung nur festgelegt, ob Startanwendungen oder veröffentlichte Anwendungen über RDP auf dem Server gestartet werden.
- **Desktop starten**: In Releases vor 7.x wird mit dieser Citrix Richtlinieneinstellung angegeben, ob Benutzer, die keine Administratoren sind, eine Verbindung zu einer Desktopsitzung herstellen dürfen. In 7.x-Releases müssen Benutzer ohne Administratorrechte zur Gruppe der Benutzer mit direktem Zugriff für eine VDA-Maschine gehören, um Verbindungen zu Sitzungen auf diesem VDA herzustellen. Die Einstellung **Desktop starten** ermöglicht Benutzern ohne Administratorrechte, die in der Gruppe der Benutzer mit direktem Zugriff eines VDAs sind, über eine ICA-Verbindung eine Verbindung zum VDA herzustellen. Die Einstellung **Desktop starten** hat keine Auswirkungen auf RDP-Verbindungen. Unabhängig von dieser Einstellung können Benutzer, die in der Gruppe der Benutzer mit direktem Zugriff eines VDAs sind, über eine RDP-Verbindung eine Verbindung zum VDA herstellen.

- **COM-Portzuordnung**: Mit der COM-Portzuordnung wurde der Zugriff auf COM-Ports auf dem Benutzergerät erlaubt oder verhindert. Die COM-Portzuordnung wurde zuvor standardmäßig aktiviert. In 7.x-Versionen von XenDesktop und XenApp ist die COM-Portzuordnung standardmäßig deaktiviert. Einzelheiten finden Sie unter Konfigurieren von COM-Port- und LPT-Portumleitungseinstellungen in der Registrierung.
- **LPT-Portzuordnung**: Mit der LPT-Portzuordnung wird der Zugriff von Legacyanwendungen auf LPT-Ports gesteuert.

Die LPT-Portzuordnung wurde zuvor standardmäßig aktiviert. In 7.x-Releases ist die LPT-Portzuordnung standardmäßig deaktiviert.

- **PCM-Audiocodec**: In 7.x-Releases wird der PCM-Audiocodec nur von HTML5-Clients unterstützt.
- **Unterstützung für Microsoft ActiveSync**
- **Proxyunterstützung für ältere Versionen**, dies umfasst:
  - Microsoft Internet Security und Acceleration (ISA) 2006 (Windows Server 2003)
  - Oracle iPlanet-Proxyserver 4.0.14 (Windows Server 2003)
  - Squid-Proxyserver 3.1.14 (Ubuntu Linux Server 11.10)

Hinweise zu Drittanbietern

Feb 29, 2016

XenApp und XenDesktop 7.7 enthalten ggf. Software von Drittanbietern, die gemäß den in den folgenden Dokumenten aufgeführten Bestimmungen lizenziert ist:

- XenApp 7.7 und XenDesktop 7.7 Hinweise zu Drittanbietern
- FlexNet Publisher Documentation Supplement Third Party and Open Source Software used in FlexNet Publisher 11.13.1

Systemanforderungen

Feb 29, 2016

Dieser Abschnitt enthält folgende Themen:

Einführung

Die Systemanforderungen in diesem Dokument galten zum Zeitpunkt der Freigabe der Produktversion, Änderungen werden regelmäßig veröffentlicht. Nicht in diesem Dokument aufgeführte Systemanforderungen (z. B. StoreFront, Hostsysteme, Citrix Receiver und Plug-Ins oder Provisioning Services) werden in der jeweiligen Dokumentation behandelt.

Wichtig: Vor Beginn einer Installation lesen Sie Vorbereiten der Installation.
Sofern nicht anders angegeben, wird erforderliche Software (z. B. .NET und C++-Pakete), wenn sie nicht auf einer Maschine erkannt wird, automatisch bereitgestellt. 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.

Die Speicherplatzangaben sind Schätzwerte und verstehen sich zuzüglich des für Produktimage, Betriebssystem und andere Software erforderlichen Speicherplatzes.

Wenn Sie die Kernkomponenten (Controller mit SQL Server Express, Studio, Director, StoreFront und Lizenzierung) auf einem Server installieren, benötigen Sie für die Evaluierung des Produkts mindestens 4 GB Arbeitsspeicher; mehr Speicher wird empfohlen, wenn Sie eine Umgebung für Benutzer ausführen. Die Leistung schwankt abhängig von der genauen Konfiguration, einschließlich der Anzahl der Benutzer, Anwendungen und Desktops sowie anderen Faktoren.

Wichtig: Verwenden Sie nach der Installation von XenApp auf einem Windows Server 2012 R2-System das Tool zum Aktivieren von Kerberos (XASsonKerb.exe), um die ordnungsgemäße Funktion der Citrix Kerberos-Authentifizierung sicherzustellen. Das Tool ist im Ordner "Support > Tools>XASsonKerb" auf dem Installationsmedium und für die Verwendung benötigen Sie lokale Administratorrechte. Damit Kerberos ordnungsgemäß funktioniert, führen Sie xassonkerb.exe –install über eine Eingabeaufforderung auf dem Server aus. Wenn Sie später ein Update ausführen, bei dem der Registrierungspfad HKLM\System\CurrentControlSet\Control\LSA\OSConfig geändert wird, führen Sie den Befehl noch einmal aus. Zum Anzeigen aller verfügbaren Tooloptionen führen Sie den Befehl mit dem Parameter –help aus.

Delivery Controller

Unterstützte Betriebssysteme:

- Windows Server 2012 R2, Standard und Datacenter Edition
- Windows Server 2012, Standard und Datacenter Edition
- Windows Server 2008 R2 SP1, Standard, Enterprise und Datacenter Edition

Anforderungen:

- Speicherplatz auf dem Datenträger: 100 MB Verbindungsleasing (standardmäßig aktiviert) steigert diese Anforderungen; die Dimensionierung hängt von der Anzahl der Benutzer und Anwendungen sowie dem Modus (RDS oder VDI) ab. Beispiel: 100.000 RDS Benutzer mit 100 vor kurzem verwendeten Anwendungen benötigten ca. 3 GB Speicherplatz für das Verbindungsleasing; Bereitstellungen mit mehr Anwendungen benötigen u. U. mehr Speicherplatz. Bei dedizierten VDI-Desktops benötigen 40.000 Desktops mindestens 400-500 MB. Auf jeden Fall sollten Sie mehrere GBs an zusätzlichem Speicherplatz bereitstellen.
- Microsoft .NET Framework 3.5.1 (nur Windows Server 2008 R2)
- Microsoft .NET Framework 4.5.1 (4.5.2 und 4.6 werden auch unterstützt).
- Windows PowerShell 2.0 (in Windows Server 2008 R2 enthalten) oder 3.0 (in Windows Server 2012 R2 und Windows Server 2012 enthalten)
- Visual C++ 2008 SP1 Redistributable Package

Datenbanken

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

- SQL Server 2014, Express, Standard und Enterprise Edition.
- SQL Server 2012 SP1 und SP2, Express, Standard und Enterprise Editions. Standardmäßig wird SQL Server 2012 SP2 Express zusammen mit dem Controller installiert, wenn keine unterstützte SQL Server-Installation erkannt wird.
- SQL Server 2008 R2 SP2, Express, Standard, Enterprise und Datacenter Edition

Die folgenden Datenbankfeatures werden unterstützt (außer bei SQL Server Express, das nur den eigenständigen Modus unterstützt):

- SQL Server-Cluster-Instanzen
- SQL Server-Spiegelung
- SQL Server 2012-AlwaysOn-Verfügbarkeitsgruppen

Die Windows-Authentifizierung ist für Verbindungen zwischen dem Controller und der SQL Server-Datenbank erforderlich.

Weitere Informationen finden Sie im Artikel Datenbanken.

Citrix Studio

Unterstützte Betriebssysteme:

- Windows 10, Enterprise Edition

- Windows 8.1, Professional und Enterprise Edition
- Windows 8, Professional und Enterprise Edition
- Windows 7, Professional, Enterprise und Ultimate Edition
- Windows Server 2012 R2, Standard und Datacenter Edition
- Windows Server 2012, Standard und Datacenter Edition
- Windows Server 2008 R2 SP1, Standard, Enterprise und Datacenter Edition

Anforderungen:

- Speicherplatz auf der Datenträger: 75 MB
- Microsoft .NET Framework 4.5.1 (4.5.2 und 4.6 werden auch unterstützt)
- Microsoft .NET Framework 3.5 SP1 (nur Windows Server 2008 R2 und Windows 7)
- Microsoft Management Console 3.0 (in allen unterstützten Betriebssystemen enthalten)
- Windows PowerShell 2.0 (in Windows 7 und Windows Server 2008 R2 enthalten) oder 3.0 (in Windows 10, Windows 8.1, Windows 8, Windows Server 2012 R2 und Windows Server 2012 enthalten)

Citrix Director

Unterstützte Betriebssysteme:

- Windows Server 2012 R2, Standard und Datacenter Edition
- Windows Server 2012, Standard und Datacenter Edition
- Windows Server 2008 R2 SP1, Standard, Enterprise und Datacenter Edition

System Center Operations Manager-Integration erfordert:

- Windows Server 2012 R2
- System Center 2012 R2 Operations Manager

Anforderungen:

- Speicherplatz auf dem Datenträger: 140 MB
- Microsoft .NET Framework 4.5.1 (4.5.2 und 4.6 werden auch unterstützt).
- Microsoft .NET Framework 3.5 SP1 (nur Windows Server 2008 R2)
- Microsoft Internetinformationsdienste (IIS) 7.0 und ASP.NET 2.0. Stellen Sie sicher, dass der Static-Content-Rollendienst für die IIS-Serverrolle installiert ist. Wenn diese Komponenten nicht auf Ihrem Server installiert sind, werden Sie möglicherweise aufgefordert, das Windows Server-Installationsmedium einzulegen. Sie werden dann installiert.
- Unterstützte Browser zum Anzeigen von Director:
  - Internet Explorer 11 oder 10 Der Kompatibilitätsmodus wird für Internet Explorer nicht unterstützt. Für den Zugriff auf Director müssen Sie die empfohlenen Webbrowsereinstellungen verwenden. Akzeptieren Sie bei der Installation von Internet Explorer die Standardeinstellung zur Verwendung der empfohlenen Sicherheits- und Kompatibilitätseinstellungen. Wenn der Browser bereits ohne die empfohlenen Einstellungen installiert ist, navigieren Sie auf "Extras > Internetoptionen > Erweitert" > Zurücksetzen" und folgen Sie den Anweisungen.
  - Microsoft Edge
  - Firefox ESR (Extended Support Release)
  - Chrome

Virtual Delivery Agent (VDA) für Windows-Desktopbetriebssysteme

Unterstützte Betriebssysteme:

- Windows 10 Enterprise Edition Die folgenden Features werden unter Windows 10 nicht unterstützt:
  - HDX 3D Pro
  - GPU-Beschleunigung
  - Desktopgestaltungsumleitung
  - Legacygrafikmodus
  - Sicherer Start
  - Veröffentlichen universeller Windows-Apps mit VM-gehosteten Apps
- Windows 8.1, Professional und Enterprise Edition
- Windows 8, Professional und Enterprise Edition
- Windows 7 SP1, Professional, Enterprise und Ultimate Edition

Für das Verwenden des Server-VDI-Features können Sie über die Befehlszeilenschnittstelle einen VDA für Windows-Desktopbetriebssysteme auf einem unterstützten Serverbetriebssystem installieren. Weitere Informationen finden Sie im Artikel Server VDI.

- Windows Server 2012 R2, Standard und Datacenter Edition
- Windows Server 2012, Standard und Datacenter Edition
- Windows Server 2008 R2 SP1, Standard, Enterprise und Datacenter Edition

Anforderungen:

- Microsoft .NET Framework 4.5.1 (4.5.2 und 4.6 werden auch unterstützt)
- Microsoft .NET Framework 3.5.1 (nur Windows 7)
- Microsoft Visual C++ 2008 SP1, 2010 SP1 und 2013 Runtimes (32-Bit und 64-Bit)

Remote-PC-Zugriff verwendet diesen VDA, den Sie auf physischen Büro-PCs installieren.

Mehrere Multimediabeschleunigungsfunktionen (z. B. HDX MediaStream-Windows Media-Umleitung) erfordern, dass Microsoft Media Foundation auf dem Computer installiert wird, auf dem der VDA installiert ist. Wenn Media Foundation nicht installiert ist, werden die Multimediabeschleunigungsfeatures nicht installiert und sind nicht funktionsfähig. Entfernen Sie Media Foundation nicht nach der Installation der Citrix Software von der Maschine, sonst können sich Benutzer nicht an der Maschine anmelden. Bei den meisten Editionen von Windows-Desktopbetriebssystemen ist Media Foundation bereits installiert und kann nicht entfernt werden. Bei N-Editionen sind bestimmte medienrelevante Technologien nicht enthalten; Sie können die Software von Microsoft oder einem Drittanbieter beziehen.

Bei der VDA-Installation können Sie entscheiden, ob Sie die HDX 3D Pro-Version des VDAs für Windows-Desktopbetriebssysteme installieren möchten. Diese Version eignet sich besonders für die Verwendung mit DirectX- und OpenGL-gesteuerten Anwendungen sowie mit Rich Media-Inhalten wie Video. Dies wird unter Windows 10 nicht unterstützt.

Sie können einen VDA der aktuellen Version nicht auf einer Maschine unter Windows XP oder Windows Vista installieren. Sie können bei diesen Betriebssystemen jedoch bei Bedarf eine Vorversion von Virtual Desktop Agent installieren. Einzelheiten

hierzu finden Sie unter CTX140941. Die Version von Remote-PC-Zugriff in diesem Release wird nicht auf Windows Vista-Betriebssystemen unterstützt.

Virtual Delivery Agent (VDA) für Windows-Serverbetriebssysteme

Unterstützte Betriebssysteme:

- Windows Server 2012 R2, Standard und Datacenter Edition
- Windows Server 2012, Standard und Datacenter Edition
- Windows Server 2008 R2 SP1, Standard, Enterprise und Datacenter Edition

Das Installationsprogramm stellt die folgenden Anforderungen automatisch bereit, die auch auf den Citrix Installationsmedien in den Ordnern \Support zur Verfügung stehen:

- Microsoft .NET Framework 4.5.1 (4.5.2 und 4.6 werden auch unterstützt)
- Microsoft .NET Framework 3.5.1 (nur Windows Server 2008 R2)
- Microsoft Visual C++ 2008 SP1, 2010 SP1 und 2013 Runtimes (32-Bit und 64-Bit)

Das Installationsprogramm installiert und aktiviert automatisch die Rollendienste für Remotedesktopdienste, wenn sie nicht bereits installiert und aktiviert sind.

Mehrere Multimediabeschleunigungsfunktionen (z. B. HDX MediaStream-Windows Media-Umleitung) erfordern, dass Microsoft Media Foundation auf dem Computer installiert wird, auf dem der VDA installiert ist. Wenn Media Foundation nicht installiert ist, werden die Multimediabeschleunigungsfeatures nicht installiert und sind nicht funktionsfähig. Entfernen Sie Media Foundation nicht nach der Installation der Citrix Software von der Maschine, sonst können sich Benutzer nicht an der Maschine anmelden. Bei den meisten Editionen von Windows Server 2012 R2, Windows Server 2012 und Windows Server 2008 R2 wird Media Foundation über den Server-Manager installiert (bei Windows Server 2012 R2 und Windows Server 2012: ServerMediaFoundation, bei Windows Server 2008 R2: DesktopExperience). Bei N-Editionen sind bestimmte medienrelevante Technologien nicht enthalten; Sie können die Software von Microsoft oder einem Drittanbieter beziehen.

Hosts/Virtualisierungsressourcen

Unterstützte Plattformen:

- XenServer:
  - XenServer 6.5 und SP1
  - XenServer 6.2 SP1 und Hotfixes (Sie müssen SP1 anwenden, damit die Anwendung zukünftiger Hotfixes möglich ist)
  - XenServer 6.1
- VMware vSphere: Der "Linked Mode"-Betrieb von vSphere vCenter wird nicht unterstützt.
  - VMware vSphere 6.0 und Update 1
  - VMware vSphere 5.5 und Update 1-3
  - VMware vSphere 5.1 Updates 2 und 3
  - VMware vSphere 5.0 Updates 2 und 3
  - VMware vCenter 5.5-/6-Gerät

- 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.
  - System Center Virtual Machine Manager 2012 R2
  - System Center Virtual Machine Manager 2012 SP1
  - System Center Virtual Machine Manager 2012
- Nutanix Acropolis 4.5. Wenn Sie diese Plattform verwenden, stehen verschiedene XenApp- und XenDesktop-Features nicht zur Verfügung; weitere Informationen finden Sie unter CTX202032. Weitere Informationen zur Verwendung des Produkts mit Acropolis finden Sie unter https://portal.nutanix.com/#/page/docs.

Sie können dieses Produkt auch in den folgenden Cloudumgebungen bereitstellen:

- Amazon Web Services (AWS)
  - Sie können Anwendungen und Desktops auf unterstützten Windows Server-Betriebssystemen bereitstellen.
  - SQL Server 2012 Enterprise ist für AWS nicht verfügbar.
  - AWS bietet keine Desktopbetriebssysteminstanzen.
  - Amazon Relational Database Service (RDS) wird nicht unterstützt.
  - Weitere Informationen finden Sie in der AWS-Dokumentation und unter CTX140427.
- Citrix CloudPlatform
  - Die unterstützte Mindestversion ist 4.2.1 mit Hotfixes 4.2.1-4.
  - Bereitstellungen wurden mit XenServer 6.2 (mit Service Pack 1 und Hotfix XS62ESP1003) und vSphere 5.1-Hypervisors getestet.
  - CloudPlatform unterstützt keine Hyper-V-Hypervisors.
  - CloudPlatform 4.3.0.1 unterstützt VMware vSphere 5.5.
  - Weitere Informationen sowie die Anforderungen für Linux-basierte Systeme finden Sie in der CloudPlatform-Dokumentation (einschließlich Versionshinweise für Ihre CloudPlatform-Version) und unter CTX140428.
- Microsoft Azure

Die folgenden Kombinationen aus Virtualisierungsressourcen- und Speichertechnologien werden für Maschinenerstellungsdienste und für das Hinzufügen von Active Directory-Konten in VMs zur Laufzeit unterstützt: Mit einem Sternchen (*) gekennzeichnete Kombinationen werden empfohlen.

Virtualisierungsressource	Lokale Datenträger	NFS	Blockspeicher	Speicherlink
XenServer	Ja	Ja *	Ja	Nein
VMware	Ja (nicht vMotion oder dynamische Platzierung)	Ja *	Ja	Nein
Hyper-V	Ja	Nein	Ja * (erfordert freigegebene Clustervolumes)	Nein

Das Wake-On-LAN-Feature von Remote-PC-Zugriff erfordert Microsoft System Center Configuration Manager 2012.

Funktionsebenen von Active Directory

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

- Natives Windows 2000 (auf Domänencontrollern nicht unterstützt)
- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

HDX

UDP-Audio für Multistream-ICA wird unter Citrix Receiver für Windows und Citrix Receiver für Linux 13 unterstützt.

Die Echounterdrückung wird unter Receiver für Windows unterstützt.

Siehe Informationen zu Unterstützung und Anforderungen für HDX unten.

Das Windows-Benutzergerät bzw. der Thin Client muss Folgendes unterstützen oder enthalten:

- DirectX 9
- Pixel Shader 2.0 (in Hardware unterstützt)
- 32 Bit pro Pixel
- 1,5 GHz Prozessor (32-Bit oder 64-Bit)
- 1 GB RAM
- 128 MB Videospeicher auf der Grafikkarte oder einem integrierten Grafikprozessor
  HDX überprüft das Windows-Gerät auf die erforderlichen GPU-Anforderungen und schaltet dann ggf. automatisch auf serverseitige Desktopgestaltung um. Geräte, die die erforderlichen GPU-Anforderungen erfüllen aber nicht die benötigte Prozessorgeschwindigkeit oder RAM-Spezifikationen haben, müssen in der GPO-Gruppe der Geräte erfasst werden, die von der Desktopgestaltungsumleitung ausgeschlossen sind.

Als Mindestausstattung ist eine verfügbare Bandbreite von 1,5 MBit/s erforderlich, empfohlen werden 5 MBit/s. Die Werte schließen End-to-End-Latenz ein.

Für den clientseitigen Abruf von Windows Media-Inhalten, die Windows Media-Umleitung und die Windows Media-Multimediatranscodierung in Echtzeit werden folgende Clients unterstützt: Citrix Receiver für Windows, Citrix Receiver für iOS und Citrix Receiver für Linux.

Zur Verwendung des clientseitigen Inhaltsabrufs von Windows Media auf Windows 8-Geräten 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 http://developer.nvidia.com/cuda/cuda-gpus.

Die folgenden Clients und Adobe Flash Player-Versionen werden unterstützt:

- Citrix Receiver für Windows: Die zweite Generation der Flash-Umleitungsfeatures erfordert Adobe Flash Player for Other Browsers, diese Version wird auch als NPAPI (Netscape Plugin Application Programming Interface) Flash Player bezeichnet.
- Citrix Receiver für Linux: Die zweite Generation der Flash-Umleitungsfeatures erfordert Adobe Flash Player for other Linux oder Adobe Flash Player for Ubuntu.
- Citrix Online Plug-In 12.1: Für Legacyfeatures der Flash-Umleitung wird Adobe Flash Player für Windows Internet Explorer benötigt (auch ActiveX Player genannt).

Die Hauptversionsnummer von Flash Player auf dem Benutzergerät muss größer oder gleich der Hauptversionsnummer von Flash Player auf dem Server sein. Wenn eine ältere Version oder gar keine Version von Flash Player auf dem Benutzergerät installiert ist, werden Flash-Inhalte auf dem Server wiedergegeben.

Die Maschinen, auf denen VDAs ausgeführt werden, erfordern Folgendes:

- Adobe Flash Player für Windows Internet Explorer (ActiveX Player)
- Internet Explorer Version 7, 8, 9, 10 und 11 (im Modus "Nicht-moderne-Oberfläche") Flash-Umleitung erfordert Internet Explorer auf dem Server; mit anderen Browsern werden Flash-Inhalte auf dem Server wiedergegeben.
- Der geschützte Modus muss in Internet Explorer deaktiviert sein (Extras > Internetoptionen > Registerkarte "Sicherheit" > Kontrollkästchen "Geschützten Modus aktivieren" deaktiviert). Starten Sie Internet Explorer neu, damit die Änderung wirksam wird.

Wenn Sie einen VDA für Windows-Desktopbetriebssysteme installieren, können Sie die Version HDX 3D Pro installieren (Ausnahme: Maschinen mit Windows 10).

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

- GPU-Passthrough steht mit Citrix XenServer zur Verfügung. GPU-Passthrough ist auch mit VMware vSphere und VMware ESX verfügbar und wird in diesem Zusammenhang als vDGA (virtual Direct Graphics Acceleration) bezeichnet.
- vGPU ist mit Citrix XenServer und VMware vSphere verfügbar. Weitere Informationen finden Sie unter www.citrix.com/go/vGPU (Anmeldeinformationen für Citrix My Account erforderlich).

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

Grafikprozessor (GPU):

- Im Hinblick auf CPU-basierte Komprimierung, einschließlich verlustfreier Komprimierung, unterstützt HDX 3D Pro alle Grafikkarten auf dem Hostcomputer, die mit der bereitgestellten Anwendung kompatibel sind.
- Für optimierten GPU-Framepufferzugriff mit NVIDIA GRID API erfordert HDX 3D Pro NVIDIA Quadro Smartcards mit den neuesten NVIDIA-Treibern. NVIDIA GRID liefert eine hohe Framerate und dadurch eine sehr interaktive Benutzererfahrung.
- Zu den Anforderungen für HDX 3D Pro zur Verwendung von vGPU mit XenServer gehören die Grafikkarten NVIDIA GRID K1 und K2.

Benutzergerät:

- HDX 3D Pro unterstützt alle Monitorauflösungen, die von dem GPU auf dem Hostcomputer unterstützt werden. Um mit den empfohlenen Minimalspezifikationen für Benutzergeräte und GPUs eine optimale Leistung zu erzielen, empfiehlt Citrix jedoch eine maximale Monitorauflösung für Benutzergeräte von 1920 x 1200 Pixeln für LAN-Verbindungen sowie von 1280 x 1024 Pixeln für WAN-Verbindungen.
- Als Mindestausstattung für Benutzergeräte empfiehlt Citrix mindestens 1 GB RAM und eine CPU mit einer Taktfrequenz von 1,6 GHz. Zur Verwendung des standardmäßigen Tiefenkomprimierungscodecs, der bei Verbindungen mit geringer Bandbreite erforderlich ist, ist eine leistungsfähigere CPU erforderlich, es sei denn, die Decodierung erfolgt in der Hardware. Zur Erzielung der optimalen Leistung empfiehlt Citrix die Ausstattung von Benutzergeräten mit mindestens 2 GB RAM und einer Dual-Core-CPU mit einer Taktfrequenz von mindestens 3 GHz.
- Bei Multimonitorzugriff empfiehlt Citrix Benutzergeräte mit Vierkern-CPUs.
- Benutzergeräte benötigen keinen dedizierten GPU für den Zugriff auf Desktops oder Anwendungen, die mit HDX 3D Pro bereitgestellt werden.
- Citrix Receiver muss installiert sein.

Unterstützte Clients: Citrix Receiver für Windows, Citrix Receiver für Mac und Citrix Receiver für Linux

Unterstützte Videokonferenzanwendungen:

- Citrix GoToMeeting HDFaces
- Adobe Connect
- Cisco WebEx
- IBM Sametime
- Microsoft Lync 2010 und 2013
- Für Microsoft Office Communicator:
- Google + Hangouts
- Media Foundation-basierte Videoanwendungen auf Windows 8.x, Windows Server 2012 und Windows Server 2012 R2
- Skype 6.7

Zum Verwenden von Skype auf einem Windows-Client bearbeiten Sie die Registrierung auf Client und Server folgendermaßen:

- Clientregistrierungsschlüssel HKEY_CURRENT_USER\Software\Citrix\HdxRealTime
  Name: DefaultHeight, Typ: REG_DWORD, Wert: 240
  Name: DefaultWidth, Typ: REG_DWORD, Wert: 320

- Serverregistrierungsschlüssel HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Vd3d\Kompatibilität
  Name: skype.exe, Typ: REG_DWORD, Wert: 0

Andere Anforderungen an Benutzergeräte:

- Geeignete Hardware für die Audiowiedergabe
- DirectShow-kompatible Webcam (Webcam-Standardeinstellungen verwenden). Hardware-verschlüsselungsfähige Webcams senken die clientseitige CPU-Nutzung.
- Webcam-Treiber (möglichst vom Kamerahersteller)

Sitzungsaufzeichnung

Die Verwaltungskomponenten der Sitzungsaufzeichnung (Datenbank für die Sitzungsaufzeichnung, Sitzungsaufzeichnungsserver und Richtlinienkonsole) können auf demselben oder mehreren Servern installiert werden.

Unterstützte Betriebssysteme:

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1

Datenbank für die Sitzungsaufzeichnung

Unterstützte Microsoft SQL Server-Versionen:

- Microsoft SQL Server 2014 (Enterprise und Express Edition)
- Microsoft SQL Server 2012 SP2 (Enterprise und Express Edition)
- Microsoft SQL Server 2008 R2 SP3 (Enterprise und Express Edition)

Voraussetzung: .NET Framework Version 3.5 SP1 (nur Windows Server 2008 R2) oder .NET Framework Version 4.5.1 oder 4.6.

Sitzungsaufzeichnungsserver

Sie müssen die Voraussetzungen vor dem Sitzungsaufzeichnungsserver installieren. Fügen Sie im Server-Manager die IIS-Rolle hinzu und wählen Sie folgende Optionen:

- Anwendungsentwicklung > ASP.NET 4.5 (Server 2012 und Server 2012 R2), ASP.NET (Server 2008 R2). Andere Komponenten werden automatisch ausgewählt; klicken Sie auf **Hinzufügen**, um die erforderlichen Rollen zu übernehmen.
- Sicherheit > Windows-Authentifizierung
- Verwaltungstools > Kompatibilität mit IIS 6
  - IIS 6-Metabasiskompatibilität
  - IIS 6-WMI-Kompatibilität
  - IIS 6-Skriptingtools
  - IIS 6-Verwaltungskonsole

Weitere Anforderungen:

- .NET Framework Version 3.5 SP1 (nur Windows Server 2008 R2) oder .NET Framework Version 4.5.1 oder 4.6.
- Wenn der Sitzungsaufzeichnungsserver HTTPS als Kommunikationsprotokoll verwendet, fügen Sie ein gültiges Zertifikat hinzu. Die Sitzungsaufzeichnung verwendet in der Standardeinstellung HTTPS; dies wird von Citrix empfohlen.
- Microsoft Message Queuing (MSMQ) mit deaktivierter Active Directory-Integration und aktivierter MSMQ-HTTP-Unterstützung.

Richtlinienkonsole für die Sitzungsaufzeichnung

Voraussetzung: .NET Framework Version 3.5 SP1 (nur Windows Server 2008 R2) oder .NET Framework Version 4.5.1 oder 4.6.

Installieren Sie den Sitzungsaufzeichnungsagent auf jedem XenApp-Server, auf dem Sie Sitzungen aufzeichnen möchten.

Unterstützte Betriebssysteme:

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1

Anforderungen:

- XenApp oder XenDesktop, Mindestversion 7.6 FP1
- .NET Framework Version 3.5 SP1, 4.5.1 oder 4.6 (müsste bereits installiert sein)
- Microsoft Message Queuing (MSMQ) mit deaktivierter Active Directory-Integration und aktivierter MSMQ-HTTP-Unterstützung

Unterstützte Betriebssysteme:

- Microsoft Windows 8,1
- Microsoft Windows 8
- Microsoft Windows 7 SP1

Voraussetzung: NET Framework Version 4.5.1 oder 4.6.

Für optimale Ergebnisse sollten Sie den Sitzungsaufzeichnungsplayer auf einer Arbeitsstation installieren, die folgende Anforderungen erfüllt:

- Eine Bildschirmauflösung von 1024 x 768
- Eine Farbtiefe von mindestens 32 Bit
- Mindestens 1GB RAM, größere RAM- und CPU-/GPU-Ressourcen können die Leistung bei der Wiedergabe grafikintensiver Aufzeichnungen verbessern, insbesondere, wenn die Aufzeichnungen viele Animationen enthalten.

Die Reaktionszeit bei der Suche hängt von der Größe der Aufzeichnung und der Computerhardware ab.

Die Sitzungsaufzeichnung ist in Englisch, Französisch, Deutsch, Japanisch, Spanisch und vereinfachtem Chinesisch erhältlich. Alle Sitzungsaufzeichnungskomponenten, die miteinander eine Verbindung herstellen, müssen in der gleichen Sprachversion vorliegen; Installationen mit unterschiedlichen Sprachen werden nicht unterstützt.

Die englische Sprachversion der Sitzungsaufzeichnung wird unter den folgenden Betriebssystemen unterstützt: Englisch, Russisch, Chinesisch (traditionell) und Koreanisch. Die Sprachversionen Französisch, Deutsch, Japanisch, Spanisch und Chinesisch (vereinfacht) der Sitzungsaufzeichnung werden unter den entsprechenden Sprachversionen des Betriebssystems unterstützt.

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 2012 R2 und 2012
- Windows Server 2008 R2 SP1
- Windows Server 2008 (32 Bit)

Voraussetzung: Microsoft Visual C++ 2013 Runtime

Für VDAs für Windows-Serverbetriebssysteme erfordert die Benutzerauthentifizierung bei Druckvorgängen, dass der universelle Druckserver in der gleichen Domäne ist wie der VDA.

Auch eigenständige Client- und Server-Komponentenpakete stehen zum Download zur Verfügung.

Weitere Informationen finden Sie im Artikel Bereitstellen von Druckern.

Sonstiges

- Citrix empfiehlt die Installation der Komponentensoftwareversionen auf dem Installationsmedium für dieses Release (bzw. ein Upgrade auf diese Versionen).
  - StoreFront erfordert 2 GB Arbeitsspeicher. Informationen zu Systemanforderungen finden Sie in der Dokumentation von StoreFront. StoreFront 2.6 ist die in diesem Release unterstützte Mindestversion.
  - Wenn Sie Provisioning Services mit diesem Release verwenden, wird als Mindestversion Provisioning Services 7.0 unterstützt.
  - Citrix Lizenzserver erfordert 40 MB Speicherplatz auf dem Datenträger. Informationen zu den Systemanforderungen finden Sie in der Dokumentation der Lizenzierung. Es wird nur Citrix Lizenzserver für Windows unterstützt. Die unterstützte Mindestversion ist 11.13.1.
- Die Microsoft-Gruppenrichtlinien-Verwaltungskonsole ist erforderlich, wenn Sie Citrix Richtlinieninformationen in Active Directory und nicht in der Sitekonfigurationsdatenbank speichern. Weitere Informationen finden Sie in der Dokumentation von Microsoft.
- Die Verwendung mehrerer Netzwerkkarten wird nicht unterstützt.
- Standardmäßig wird zusammen mit einem VDA Citrix Receiver für Windows installiert. Weitere Informationen finden Sie in der Dokumentation von Citrix Receiver für Windows.
- Wenn Sie Access Gateway-Versionen vor 10.0 mit diesem Release verwenden, werden Windows-Clients vor Version 7 nicht unterstützt.
- Unterstützte Versionen sind im App-V-Artikel aufgeführt.
- Clientordnerumleitung – unterstützte Betriebssysteme:
  - Server: Windows Server 2008 R2 SP1, Windows Server 2012 und Windows Server 2012 R2
  - Client (mit der aktuellen Version von Citrix Receiver für Windows): Windows 7, Windows 8, und Windows 8.1

Technische Übersicht

Feb 29, 2016

XenApp und XenDesktop sind Virtualisierungslösungen, die IT die Steuerung von virtuellen Maschinen, Anwendungen sowie von der Lizenzierung und Sicherheit ermöglichen und gleichzeitig Benutzern von überall Zugriff mit jedem Gerät bieten.

XenApp und XenDesktop ermöglichen Folgendes:

- Endbenutzer können Anwendungen und Desktops unabhängig vom Betriebssystem und von der Benutzeroberfläche eines Geräts ausführen.
- Administratoren können Netzwerke verwalten und Zugriff von ausgewählten Geräten oder allen Geräten gewähren oder einschränken.
- Administratoren können ein ganzes Netzwerk von einem Datencenter aus verwalten.

XenApp und XenDesktop haben eine einheitliche Architektur, die FlexCast Management Architecture (FMA) genannt wird. Die Hauptfunktion von FMA umfasst die Ausführung mehrerer Versionen von XenApp oder XenDesktop auf einer einzigen Site und die Bereitstellung von integriertem Provisioning.

Hauptkomponenten von FMA

Eine typische XenApp- oder XenDesktop-Umgebung besteht aus einigen technischen Hauptkomponenten, die interagieren, wenn Benutzer Verbindungen zu Anwendungen und Desktops herstellen, und Daten über die Siteaktivität erfassen.

Citrix Receiver: Softwareclient, der auf dem Benutzergerät installiert ist. Er stellt die Verbindung zur virtuellen Maschine über TCP-Port 80 oder 443 her und kommuniziert mit StoreFront über die StoreFront-Dienst-API.

Citrix StoreFront: Benutzeroberfläche, mit der Benutzer authentifiziert werden. Sie dient zur Verwaltung von Anwendungen und Desktops und zum Hosten des Anwendungsstores. StoreFront kommuniziert mit dem Delivery Controller mit XML.

Delivery Controller: zentrale Verwaltungskomponente einer XenApp- oder XenDesktop-Site. Sie besteht aus Diensten, die Ressourcen, Anwendungen und Desktops verwalten und die Last der Benutzerverbindungen optimieren und ausgleichen.

Virtual Delivery Agent (VDA): Agent, der auf Maschinen installiert ist, auf denen Windows Server- oder Windows-Desktopbetriebssysteme ausgeführt werden. Er gewährleistet, dass diese Maschinen und die von ihnen gehosteten Ressourcen Benutzern zur Verfügung gestellt werden können. Auf Windows-Serverbetriebssystemmaschinen ermöglichen VDAs das Hosten mehrerer Verbindungen für mehrere Benutzer und sind mit den Benutzern über einen der folgenden Ports verbunden:

- TCP-Port 80 oder Port 443, wenn TLS aktiviert ist
- TCP-Port 2598, wenn Citrix Gateway Protocol (CGP) aktiviert ist (für Sitzungszuverlässigkeit)
- TCP-Port 1494, wenn CGP deaktiviert ist oder wenn der Benutzer eine Verbindung über einen Legacyclient herstellt

Brokerdienst: Delivery Controller-Dienst, der protokolliert, welche Benutzer wo angemeldet sind, welche Sitzungsressourcen die Benutzer nutzen und ob Benutzer sich erneut mit vorhandenen Anwendungen verbinden müssen. Der Brokerdienst führt PowerShell aus und kommuniziert mit dem Broker Agent über TCP-Port 80. Er kann TCP-Port 443 nicht verwenden.

Broker-Agent: Agent, der mehrere Plug-Ins hostet und Echtzeitdaten sammelt. Der Broker Agent ist auf dem VDA und mit dem Controller über TCP-Port 80 verbunden. Er kann TCP-Port 443 nicht verwenden.

Überwachungsdienst: Komponente des Delivery Controllers, die historische Daten sammelt und diese standardmäßig in der Sitedatenbank speichert. Der Monitor Service kommuniziert über TCP-Port 80 oder 443.

ICA-Datei/Stack: gebündelte Benutzerinformationen, die für die Verbindung mit dem VDA erforderlich sind.

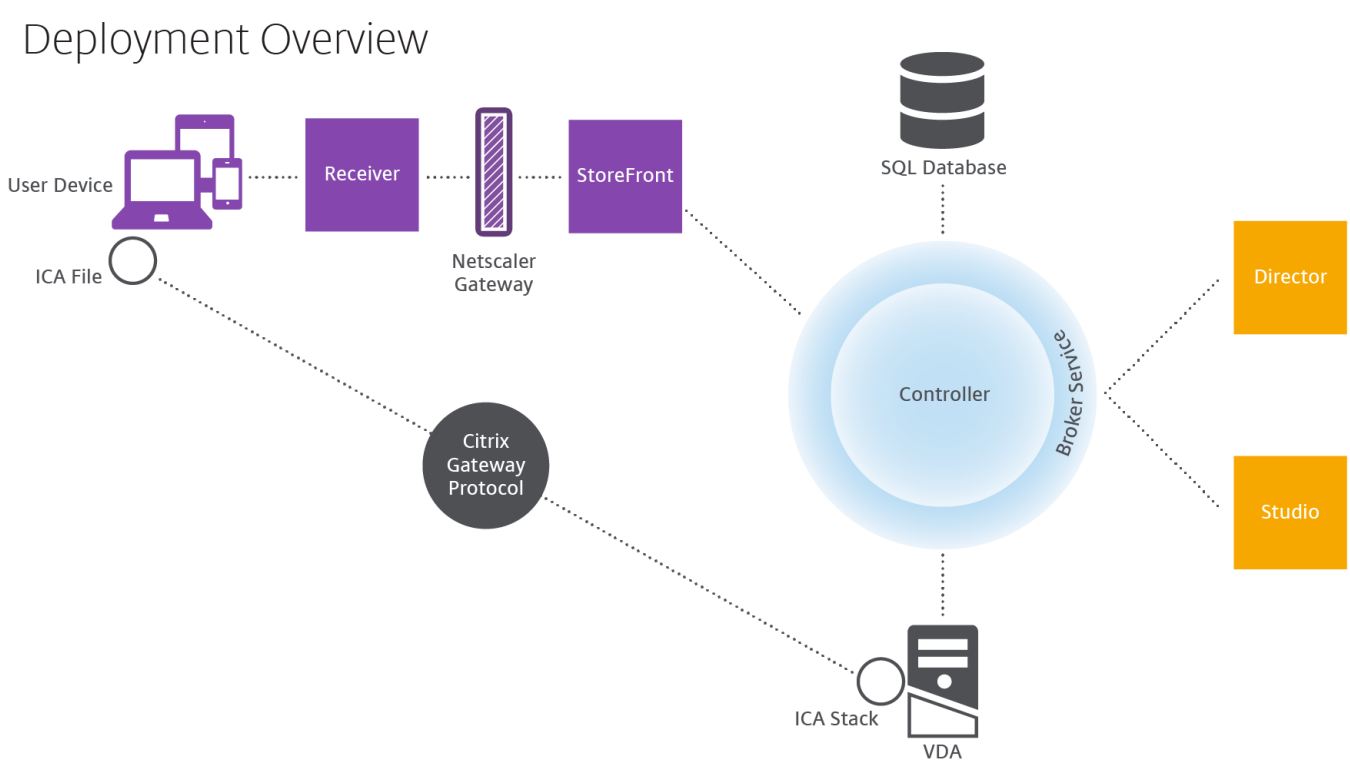
Sitedatenbank: Microsoft SQL-Datenbank, in der Daten für den Delivery Controller (Siterichtlinien, Maschinenkataloge, Bereitstellungsgruppen etc.) gespeichert werden.

NetScaler Gateway: Datenzugriffslösung, die sicheren Zugriff von innerhalb oder außerhalb der LAN-Firewall durch zusätzliche Anmeldeinformationen gewährleistet.

Citrix Director: webbasiertes Tool, das Administratoren und Helpdeskpersonal den Zugriff auf Echtzeitdaten vom Broker-Agent, historische Daten von der Sitedatenbank und HDX-Daten von NetScaler für die Problembehandlung und den Support bietet. Director kommuniziert mit dem Controller über TCP-Port 80 oder 443.

Citrix Studio: Verwaltungskonsole, mit der Administratoren Sites konfigurieren und verwalten und die Zugriff auf Echtzeitdaten vom Broker-Agent ermöglicht. Studio kommuniziert mit dem Controller über TCP-Port 80.

XenApp- und XenDesktop-Sites bestehen aus Maschinen mit dedizierten Rollen, die Skalierbarkeit, hohe Verfügbarkeit und Failover gewährleisten und auf diese Weise eine inhärent sichere Lösung bieten. Eine XenApp- oder XenDesktop-Site besteht aus Server- und Desktopmaschinen mit installierten VDAs und dem Delivery Controller, der den Zugriff verwaltet.



Durch den VDA können Benutzer Verbindungen mit Desktops und Anwendungen herstellen. Er ist auf Server- oder Desktopmaschinen im Datencenter für die meisten Bereitstellungsmethoden installiert, aber er kann auch auf physischen

PCs für Remote-PC-Zugriff installiert werden.

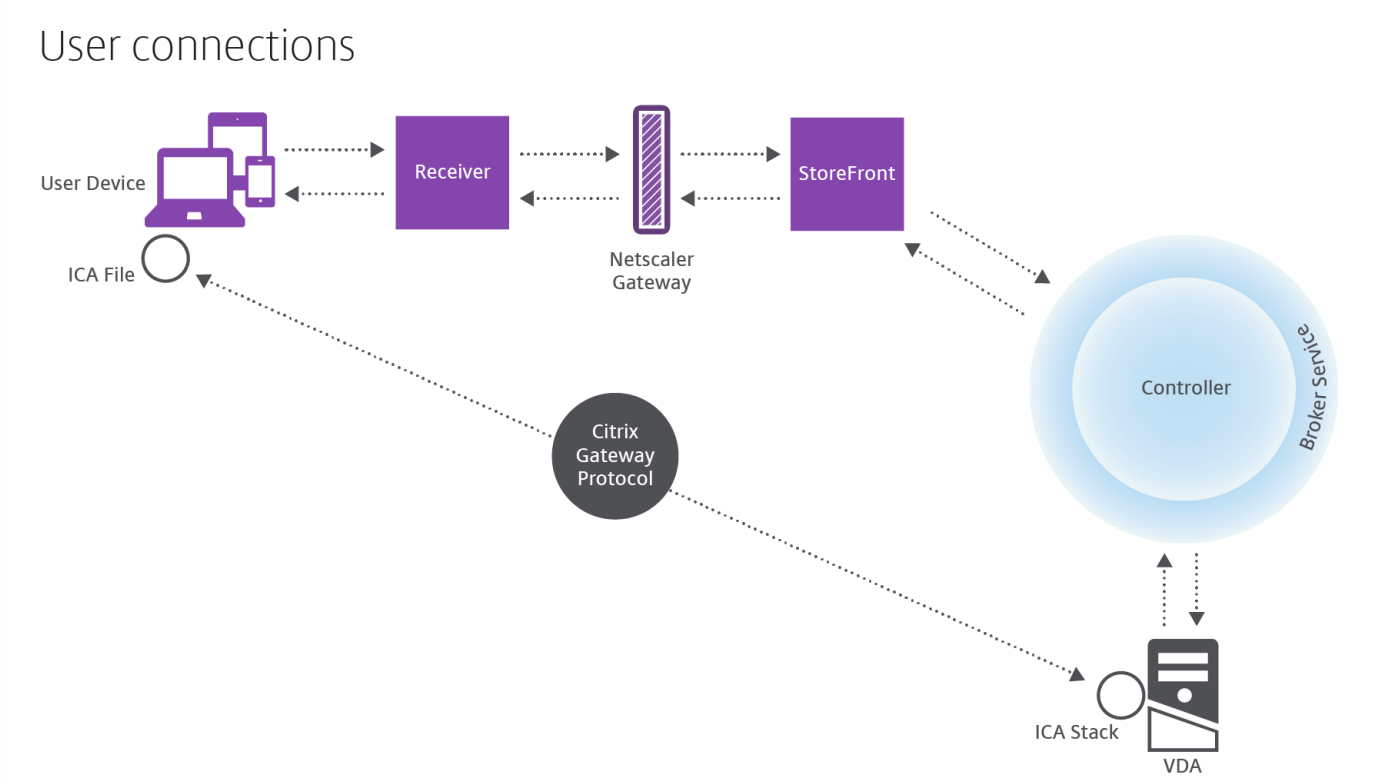
Der Controller besteht aus unabhängigen Windows-Diensten, die Ressourcen, Anwendungen und Desktops verwalten und die Last der Benutzerverbindungen optimieren und ausgleichen. Jede Site hat einen oder mehrere Controller. Da Sitzungen von der Latenz, Bandbreite und Netzwerkzuverlässigkeit abhängig sind, sollten alle Controller idealerweise im gleichen LAN sein.

Benutzer greifen niemals direkt auf den Controller zu. Der VDA dient als Vermittler zwischen den Benutzern und dem Controller. Wenn Benutzer sich über StoreFront an der Site anmelden, werden ihre Anmeldeinformationen an den Brokerdienst weitergeleitet. Dieser ruft, basierend auf den festgelegten Richtlinien, die Profile der Benutzer und die für sie verfügbaren Ressourcen ab.

Zum Starten einer XenApp- oder XenDesktop-Sitzung stellt der Benutzer eine Verbindung über Citrix Receiver her (auf dem Benutzergerät installiert), oder über Citrix Receiver für Web (RFW).

In Citrix Receiver wählt der Benutzer 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. Administratoren wird empfohlen, ein SSL-Zertifikat auf StoreFront zu installieren, sodass die von Receiver kommenden Anmeldeinformationen verschlüsselt werden.



Der Brokerdienst bestimmt, auf welche Desktops und Anwendungen der Benutzer zugreifen kann.

Wenn die Anmeldeinformationen geprüft wurden, werden die Informationen zu verfügbaren Apps und Desktops über die StoreFront-Citrix Receiver-Route an den Benutzer gesendet. Wenn der Benutzer Anwendungen oder Desktops aus dieser Liste auswählt, werden diese Informationen wieder an den Controller geleitet, der den richtigen VDA zum Hosten der

einzelnen Anwendungen oder Desktops bestimmt.

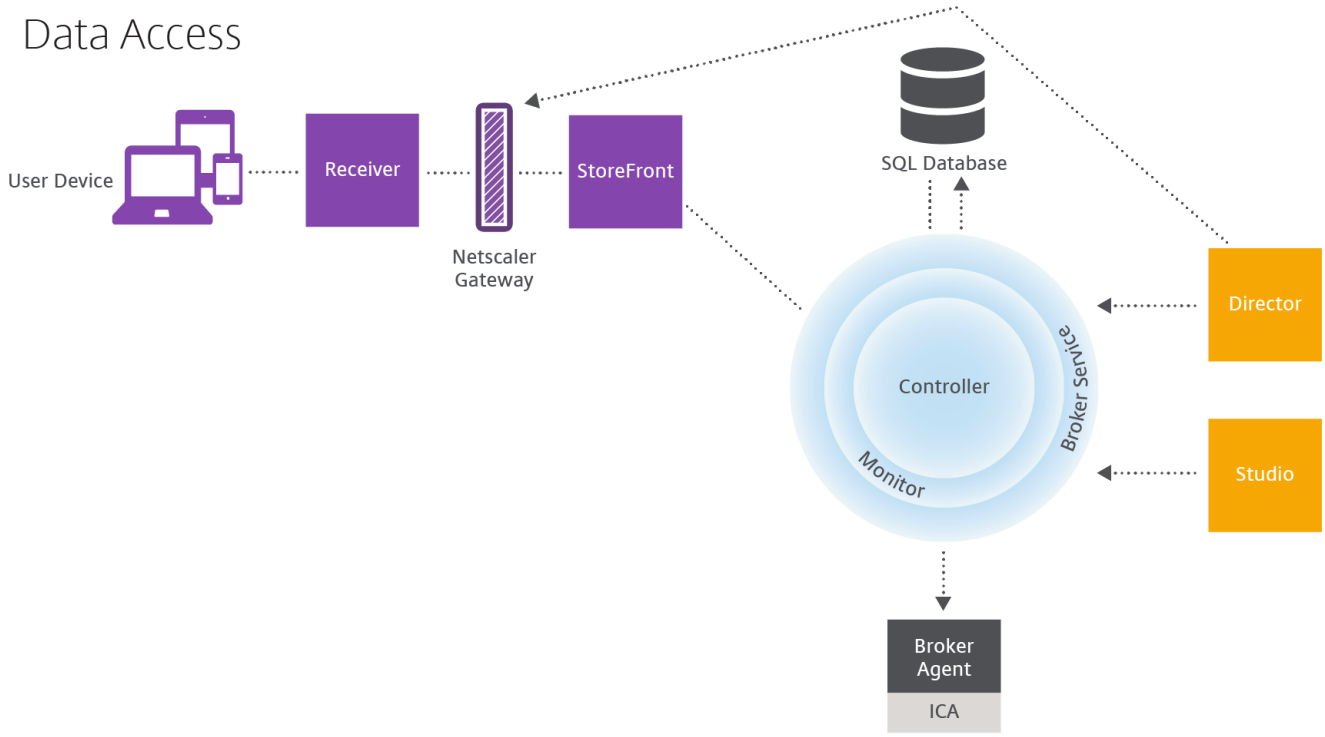
Der Controller sendet eine Nachricht mit den Anmeldeinformationen des Benutzers sowie alle Daten zu dem Benutzer und der Verbindung an den VDA. Der VDA akzeptiert die Verbindung und sendet die Informationen über die gleiche Route an Citrix Receiver zurück. Citrix Receiver bündelt die gesamten Informationen, die während der Sitzung generiert wurden, und erstellt eine ICA-Datei (Independent Computing Architecture) auf dem Benutzergerät, wenn Citrix Receiver lokal installiert ist, oder auf dem RFW, wenn der Zugriff über das Internet erfolgt. 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 von Citrix Receiver, StoreFront und Controller.

Die Verbindung zwischen Citrix Receiver und dem VDA verwendet das Citrix Gateway Protocol (CGP). Wenn eine Verbindung unterbrochen wird, kann der Benutzer bei aktivierter Sitzungszuverlässigkeit die Verbindung zum VDA wieder herstellen und muss sich nicht über die Verwaltungsinfrastruktur erneut anmelden. Die Sitzungszuverlässigkeit kann in Studio aktiviert oder deaktiviert werden.

Wenn der Client eine Verbindung zum VDA hergestellt hat, benachrichtigt der VDA den Controller, dass der Benutzer angemeldet ist, und der Controller sendet diese Informationen an die Sitedatenbank und beginnt mit der Protokollierung von Daten in der Überwachungsdatenbank.

Jede XenApp- oder XenDesktop-Sitzung produziert Daten, auf die die IT-Mitarbeiter über Studio oder Director zugreifen können. Mit Studio können Administratoren auf Echtzeitdaten aus dem Broker Agent zugreifen und damit Sites besser verwalten. Director bietet Zugriff auf dieselben Echtzeitdaten und historischen Daten, die in der Überwachungsdatenbank gespeichert sind, sowie auf HDX-Daten von NetScaler Gateway, die dem Helpdesk zum Support und zur Problembehandlung dienen.



Innerhalb des Controllers gibt der Brokerdienst Sitzungsdaten für jede Sitzung auf der virtuellen Maschine als Echtzeitdaten zurück. Der Überwachungsdienst erfasst ebenfalls die Echtzeitdaten und speichert sie als historische Daten in der Überwachungsdatenbank.

Studio kann nur mit dem Brokerdienst kommunizieren und hat daher lediglich Zugriff auf Echtzeitdaten. Director kommuniziert mit dem Brokerdienst (über ein Plug-In im Broker Agent), um auf die Sitedatenbank zuzugreifen.

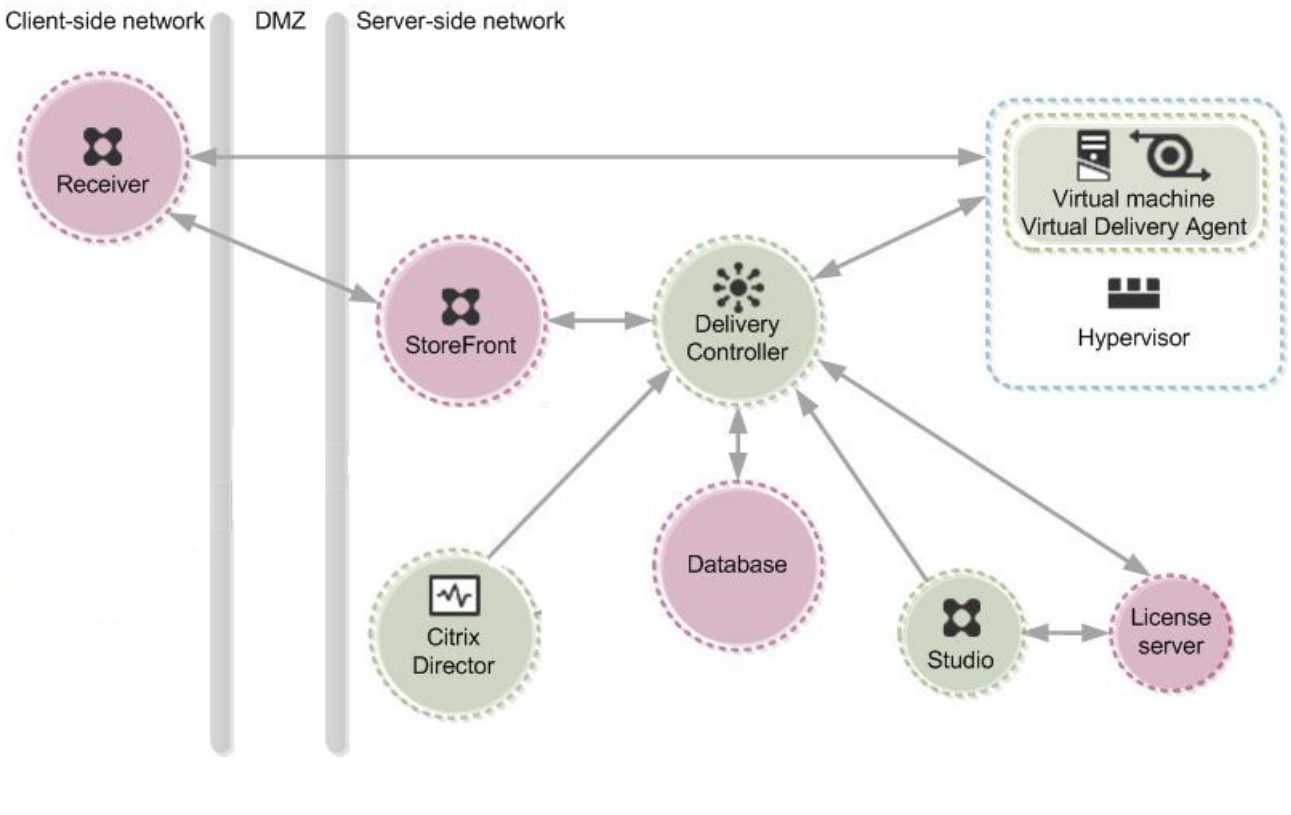
Director kann zudem auf NetScaler Gateway zugreifen und Informationen zu HDX-Daten abrufen.

- Konzepte und Komponenten
- Bereitstellungsmethoden

Konzepte und Komponenten

Jul 22, 2016

Diese Abbildung zeigt die wichtigsten Komponenten in einer typischen XenApp- oder XenDesktop-Bereitstellung, die als *Site* bezeichnet wird.



Die Abbildung enthält folgende Komponenten:

- **Delivery Controller**: Der Delivery Controller ist die zentrale Verwaltungskomponente einer XenApp- oder XenDesktop-Site. Jede Site hat einen oder mehrere Delivery Controller. Er muss auf mindestens einem Server im Datencenter installiert sein. (Um die Zuverlässigkeit und Verfügbarkeit der Site zu gewährleisten, installieren Sie den Controller auf mehreren Servern.) Wenn Ihre Bereitstellung virtuelle Maschinen auf einem Hypervisor oder in einem Clouddienst enthält, kommunizieren die Controller-Dienste mit dem Hypervisor, um Anwendungen und Desktops zu verteilen, den Benutzerzugriff zu authentifizieren und zu verwalten, Verbindungen zwischen Benutzern und ihren virtuellen Desktops und Anwendungen zu vermitteln, Benutzerverbindungen zu optimieren und einen Lastausgleich für die Verbindungen auszuführen.
  Die Daten dieser Dienste werden in der Sitedatenbank gespeichert.

  Der Controller verwaltet den Zustand der Desktops, startet und hält sie basierend auf dem Bedarf und der administrativen Konfiguration an. In bestimmten Editionen ermöglicht der Controller die Installation der Profilverwaltung, mit der Sie personalisierte Einstellungen in virtualisierten oder physischen Windows-Umgebungen verwalten.

- **Datenbank**: Mindestens eine Microsoft SQL Server-Datenbank ist pro XenApp- oder XenDesktop-Site zum Speichern der Konfigurations- und Sitzungsinformationen erforderlich. Diese Datenbank speichert die Daten, die von den Diensten des Controllers gesammelt und verwaltet werden. Installieren Sie die Datenbank in Ihrem Datencenter und stellen Sie eine persistente Verbindung mit dem Controller sicher.

- **Virtual Delivery Agent (VDA)**: Der VDA ist auf jeder physischen oder virtuellen Maschine der Site installiert, die Sie Benutzern zur Verfügung stellen möchten. Durch ihn kann sich die Maschine beim Controller registrieren, sodass die Maschine und die darauf gehosteten Ressourcen Benutzern verfügbar gemacht werden können. VDAs erstellen und verwalten die Verbindung zwischen der Maschine und dem Benutzergerät, prüfen, ob eine Citrix Lizenz für den Benutzer oder die Sitzung verfügbar ist und wenden die für die Sitzung konfigurierten Richtlinien an. Der VDA übermittelt über den Broker Agent Sitzungsinformationen an den Brokerdienst auf dem Controller.
  VDAs sind für Windows-Serverbetriebssysteme und Windows-Desktopbetriebssysteme verfügbar. Mit VDAs für Windows-Serverbetriebssysteme können mehrere Benutzer gleichzeitig eine Verbindung mit dem Server herstellen. Mit VDAs für Windows-Desktopbetriebssysteme kann jeweils nur ein Benutzer eine Verbindung zum Desktop herstellen.

- **Citrix StoreFront**: dient zur Authentifizierung von Benutzern für Sites mit Ressourcen und zur Verwaltung von Stores mit Desktops und Anwendungen für die Benutzer. StoreFront hostet den Unternehmensanwendungsstore, über den Sie Benutzern Self-Service-Zugriff auf Desktops und Anwendungen gewähren, die Sie verfügbar machen. Außerdem verfolgt es die Anwendungsabonnements von Benutzern sowie Verknüpfungsnamen und andere Daten, um eine konsistente Benutzererfahrung über mehrere Geräte sicherzustellen.
- **Citrix Receiver**: wird auf Benutzergeräten und anderen Endpunkten installiert, u. a. virtuellen Desktops, und bietet Benutzern schnellen, sicheren Self-Service-Zugriff auf Dokumente, Anwendungen und Desktops von allen Geräten (Smartphones, Tablets, PCs) aus. Citrix Receiver bietet bedarfsgesteuerten Zugriff auf Windows-, Web- und SaaS-Anwendungen. Bei Geräten, auf denen die Citrix Receiver-Software nicht installiert werden kann, ermöglicht Citrix Receiver für HTML5 eine Verbindung über einen HTML5-kompatiblen Webbrowser.
- **Citrix Studio**: Dies ist die Verwaltungskonsole, mit der Sie die Bereitstellung konfigurieren und verwalten, wobei keine separaten Verwaltungskonsolen für die Bereitstellung von Anwendungen und Desktops benötigt werden. Studio bietet zahlreiche Assistenten, die Ihnen bei der Einrichtung Ihrer Umgebung, dem Erstellen der Arbeitslast zum Hosten von Anwendungen und Desktops sowie beim Zuweisen von Anwendungen und Desktops zu Benutzern behilflich sind. Sie können mit Studio auch Citrix Lizenzen für die Site zuweisen und verfolgen.
  Studio erhält die Informationen, die es anzeigt, vom Brokerdienst auf dem Controller.

- **Citrix Director**: Director ist ein webbasiertes Tool, mit dem die Support- und Helpdesk-Teams eine XenDesktop-Umgebung überwachen, potenziell systembedrohende Probleme rechtzeitig behandeln und Unterstützung für Endbenutzer leisten können. Sie können eine Director-Bereitstellung zur Verbindungen mit und Überwachung von mehreren XenApp- bzw. XenDesktop-Sites verwenden. In Director werden folgende Sitzungs- und Siteinformationen angezeigt:

  - Echtzeit-Sitzungsdaten vom Brokerdienst auf dem Controller, einschließlich Daten, die der Brokerdienst vom Broker Agent auf dem VDA erhält.
  - Historische Daten für die Site vom Überwachungsdienst auf dem Controller.
  - Daten zum HDX-Datenverkehr (auch ICA-Datenverkehr genannt), die von HDX Insight auf dem NetScaler erfasst werden, wenn die Bereitstellung einen NetScaler und die XenApp- oder XenDesktop-Edition HDX Insights enthält.

  Zudem können Sie über Microsoft-Remoteunterstützung auch Benutzersitzungen anzeigen und steuern.

- **Citrix Lizenzserver**: Der Lizenzserver verwaltet die Produktlizenzen. Er kommuniziert mit dem Controller, um die Lizenzierung jeder Benutzersitzung zu verwalten, und mit Studio, um Lizenzdateien zuzuteilen. Sie müssen mindestens einen Lizenzserver zum Speichern und Verwalten Ihrer Lizenzdateien erstellen.
- **Hypervisor**: Der Hypervisor hostet die virtuellen Maschinen in der Site. Dies können virtuellen Maschinen sein, die Sie zum

Hosten von Anwendungen und Desktops verwenden, und auch virtuellen Maschinen, die Sie zum Hosten von XenApp- und XenDesktop-Komponenten verwenden. Ein Hypervisor wird auf einem Hostcomputer installiert, der nur zur Ausführung des Hypervisors und dem Hosten virtueller Maschinen bestimmt ist.
Der Citrix XenServer-Hypervisor ist in XenApp und XenDesktop enthalten. Sie können auch andere unterstützte Hypervisors verwenden, z. B. Microsoft Hyper-V oder VMware vSphere.

Obwohl für viele Implementierungen von XenApp und XenDesktop ein Hypervisor erforderlich ist, benötigen Sie keinen für Remote-PC-Zugriff oder wenn Sie Provisioning Services statt MCS zum Bereitstellen von virtuellen Maschinen verwenden. Provisioning Services ist in bestimmten XenApp-/XenDesktop-Editionen enthalten.

Diese zusätzlichen Komponenten, die nicht in der Abbildung oben enthalten sind, können auch in typischen XenApp- oder XenDesktop-Bereitstellungen enthalten sein:

- **Provisioning Services**: Provisioning Services ist eine optionale Komponente von XenApp und XenDesktop und steht in einigen Editionen zur Verfügung. Es bietet eine Alternative zu MCS für das Provisioning von virtuellen Maschinen. Während MCS Kopien eines Masterimages erstellt, streamt Provisioning Services das Masterimage zum Benutzergerät. Provisioning Services benötigen hierfür keinen Hypervisor, daher können Sie mit Provisioning Services physische Maschinen hosten. Wenn Provisioning Services in einer Site installiert ist, kommuniziert es mit dem Controller, um Benutzern Ressourcen bereitzustellen.
- **NetScaler Gateway**: Wenn Benutzer eine Verbindung von außerhalb der Unternehmensfirewall herstellen, können diese Verbindungen in diesem Release mit Citrix NetScaler Gateway (früher Access Gateway) mit TLS gesichert werden. NetScaler Gateway oder NetScaler VPX virtuelles Gerät ist ein SSL-VPN-Gerät, das in der DMZ (demilitarisierten Zone) bereitgestellt wird und sicheren, zentralen Zugriff über die Unternehmensfirewall bietet.
- **Citrix CloudBridge**: In Bereitstellungen, in denen virtuelle Desktops den Benutzern an Remotestandorten wie etwa Zweigstellen bereitgestellt werden, kann mit Citrix CloudBridge (früher Citrix Branch Repeater oder WANScaler) die Leistung optimiert werden. Repeater erhöhen die Leistung in WAN-Netzwerken. Mit Repeatern im Netzwerk erleben Benutzer in Zweigstellen eine LAN-ähnliche Leistung über das WAN. CloudBridge 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 mit CloudBridge bietet Komprimierung mit Token sowie Entfernung von Datenduplikaten, wodurch die Bandbreitenanforderungen drastisch reduziert werden und die Leistung verbessert wird. Weitere Informationen finden Sie in der Dokumentation für Citrix CloudBridge.

Einrichten und Zuweisen von Ressourcen: Maschinenkataloge und Bereitstellungsgruppen

Sie richten die Ressourcen, die Sie Benutzern bereitstellen möchten, mit Maschinenkatalogen ein; welche Benutzer Zugriff auf diese Ressourcen haben, wird mit Bereitstellungsgruppen festgelegt.

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 ist das gleiche Betriebssystem und der gleiche Virtual Desktop Agent (VDA) installiert.

Sie verfügen auch über dieselben Anwendungen oder virtuellen Desktops. Normalerweise erstellen Sie ein Masterimage und verwenden es zum Erstellen identischer virtueller Maschinen im Maschinenkatalog. Beim Erstellen eines Maschinenkatalogs geben Sie den Typ und die Bereitstellungsmethode für die Maschinen in dem Katalog an.

- **Serverbetriebssystemmaschinen**: virtuelle oder physische Maschinen, die auf einem Serverbetriebssystem basieren und dazu verwendet werden, mit XenApp veröffentlichte Apps (serverbasierte, gehostete Anwendungen) und mit XenApp veröffentlichte Desktops (servergehostete Desktops) bereitstellen. Mehrere Benutzer können gleichzeitig eine Verbindung mit diesen Maschinen herstellen.
- **Desktopbetriebssystemmaschinen**: virtuelle oder physische Maschinen, die auf einem Desktopbetriebssystem basieren und die VDI-Desktops (Desktops, auf denen Desktopbetriebssysteme ausgeführt werden, die abhängig von den ausgewählten Optionen vollständig personalisiert werden können), VM-gehostete Apps (Anwendungen von Desktopbetriebssystemen) und gehostete physische Desktops bereitstellen. Nur jeweils ein Benutzer kann eine Verbindung zu einem dieser Desktops herstellen.
- **Remote-PC-Zugriff**: Wenn Benutzergeräte auf einer Positivliste enthalten sind, können die Benutzer von einem beliebigen Gerät aus, auf dem Citrix Receiver ausgeführt wird, auf ihre Büro-PCs zugreifen. Remote-PC-Zugriff ermöglicht das Verwalten des Zugriffs auf Büro-PCs über die XenDesktop-Bereitstellung.

Provisioningmethoden

- **Maschinenerstellungsdienste (MCS)**: Sammlung von Diensten, die bei Bedarf virtuelle Server und Desktops von einem Masterimage erstellen, die Speichernutzung optimieren und den Benutzern bei jeder Anmeldung eine virtuelle Maschine bereitstellen. MCS ist vollständig in Citrix Studio integriert und wird dort verwaltet.
- **Provisioning Services**: ermöglicht Provisioning und erneutes Provisioning von Computern in Echtzeit von einem freigegebenen Datenträgerimage. Zielgeräte werden von Provisioning Services als eine Gerätesammlung verwaltet. Die Desktops und Anwendungen werden von einer Provisioning Services-vDisk bereitgestellt, deren Image von einem Masterzielgerät erstellt wurde. So können Sie die Verarbeitungsleistung der physischen Hardware oder der virtuellen Maschinen nutzen. Provisioning Services werden in einer eigenen Konsole verwaltet.
- **Vorhandene Images**: bezieht sich auf Desktops und Anwendungen, die Sie bereits auf virtuelle Maschinen im Datencenter migriert haben. Sie müssen die Zielgeräte individuell oder kollektiv mit ESD-Tools (Electronic Software Distribution) verwalten.

Bereitstellungsgruppen

Bereitstellungsgruppen sind Sammlungen von Benutzern, denen Zugriff auf eine gemeinsame Gruppe von Ressourcen erteilt wird. Bereitstellungsgruppen enthalten Maschinen von Ihren Maschinenkatalogen und Active Directory-Benutzer, die Zugriff auf die Site haben. Oft ist es sinnvoll, 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, aber eine Maschine kann jeweils nur zu einer Bereitstellungsgruppe gehören. Sie können Bereitstellungsgruppen für Anwendungen, Desktops oder beides einrichten. Dabei definieren Sie, auf welche Ressourcen Benutzer in der Bereitstellungsgruppe zugreifen können. Beispiel: Sie möchten verschiedene Anwendungen verschiedenen Benutzern bereitstellen. Eine Methode ist die Installation aller bereitzustellenden Anwendungen auf dem Masterimage für einen Maschinenkatalog. Dann erstellen Sie in diesem Katalog genug Maschinen, um sie auf mehrere Bereitstellungsgruppen zu verteilen. Anschließend konfigurieren Sie jede Bereitstellungsgruppe so, dass sie einen anderen Teil der auf den Maschinen installierten Anwendungen bereitstellt.

Unterschiede zwischen XenApp und XenDesktop 7.x

und XenApp-Versionen bis 6.5

Wenn Sie mit XenApp 6.5 und Vorversionen vertraut sind, kann es nützlich sein, sich die Unterschiede zwischen XenApp und XenDesktop 7.x und diesen älteren Versionen anzuschauen.

> **Hinweis:** In diesem Abschnitt bezieht sich die Angabe 7.x auf XenApp ab Version 7.5 und auf XenDesktop ab Version 7.

Obwohl die funktionellen Elemente nicht genau gleich sind, erleichtert die folgende Tabelle das Zuordnen der funktionellen Elemente von XenApp bis Version 6.5 zu jenen von XenApp und XenDesktop 7.x:

XenApp 6.5 und Vorversionen	XenApp und XenDesktop 7.x
Independent Management Architecture (IMA)	FlexCast Management Architecture (FMA)
Farm	Site
Workergruppe	Maschinenkatalog Bereitstellungsgruppe
Worker	Virtual Delivery Agent (VDA) Serverbetriebssystemmaschine, VDA für Serverbetriebssystem Desktopbetriebssystemmaschine, VDA für Desktopbetriebssystem
Remotedesktopdienste (RDS) oder Terminaldienste-Maschine	Serverbetriebssystemmaschine, VDA für Serverbetriebssystem
Zonen- und Datensammelpunkt	Delivery Controller
Delivery Services Console	Citrix Studio und Citrix Director
Veröffentlichen von Anwendungen	Bereitstellen von Anwendungen
Datenspeicher	Datenbank
Lastauswertungsprogramm	Lastverwaltungsrichtlinie
Administrator	Delegierter Administrator

	Rolle Geltungsbereich

XenApp und XenDesktop 7.x basieren auf der FlexCast Management Architecture (FMA). Die FMA ist eine dienstorientierte Architektur, die über Citrix Technologien übergreifend Interoperabilität und Verwaltungsmodularität ermöglicht Die FMA bietet eine Plattform für die Anwendungsbereitstellung, Mobilität, Dienste, flexible Bereitstellung und Cloudverwaltung.

Die FMA ersetzt die Independent Management Architecture (IMA) in XenApp 6.5 und Vorversionen.

Dies sind die Hauptelemente der FMA gegenüber den Elementen von XenApp 6.5 und Vorversionen:

- **Bereitstellungssites:** Farmen waren die Objekte der obersten Ebene in XenApp 6.5 und Vorversionen. In XenApp und XenDesktop 7.x ist dies die Site. Über Sites werden Benutzergruppen Anwendungen und Desktops angeboten. Die FMA erfordert, dass Sie in einer Domäne sind, um eine Site bereitzustellen. Beispiel: Zum Installieren der Server muss Ihr Konto lokale Administratorrechte haben und in Active Directory ein Domänenbenutzer sein.
- **Maschinenkataloge und Bereitstellungsgruppen:** Maschinen, auf denen Anwendungen gehostet werden, gehörten in XenApp 6.5 und Vorversionen zu Workergruppen, um eine effiziente Verwaltung von Anwendungen und Serversoftware zu ermöglichen. Administratoren konnten für die Anwendungsverwaltung und für den Lastausgleich alle Maschinen in einer Workergruppe als eine Einheit behandeln. Ordner wurden verwendet, um Anwendungen und Maschinen zu organisieren. In XenApp und XenDesktop 7.x verwenden Sie eine Kombination aus Maschinenkatalogen und Bereitstellungsgruppen, um Maschinen, den Lastausgleich und gehostete Anwendungen oder Desktops zu verwalten. Sie können auch Anwendungsordner verwenden.
- **Virtual Delivery Agents (VDAs):** In XenApp 6.5 und Vorversionen wurden auf Maschinen in Workergruppen Anwendungen für die Benutzer ausgeführt und die Maschinen kommunizierten mit Datensammelpunkten. In XenApp und XenDesktop 7.x kommuniziert der VDA mit Delivery Controllern, die die Benutzerverbindungen verwalten.
- **Delivery Controller:** In XenApp 6.5 und Vorversionen war ein Zonenmaster für Verbindungsanfragen von Benutzern und die Kommunikation mit Hypervisors zuständig. In XenApp und XenDesktop 7.x verteilen und handhaben Controller in der Site Verbindungsanfragen. In XenApp 6.5 und Vorversionen ermöglichten Zonen das Aggregieren von Servern und Replizieren von Daten über WAN-Verbindungen. Die Zonen in XenApp und XenDesktop 7.x sind zwar keine exakte Entsprechung, dennoch können Sie mit ihnen Benutzern an entfernten Standorten eine Verbindung mit Ressourcen ermöglichen, ohne dass diese große WAN-Segmente durchqueren muss.
- **Citrix Studio und Citrix Director:** Mit der Studio-Konsole können Sie Umgebungen konfigurieren und Benutzern Zugriff auf Anwendungen und Desktops gewähren. Studio ersetzt die Delivery Services Console in XenApp 6.5 und Vorversionen. Administratoren verwenden Director, um die Umgebung zu überwachen, Benutzergeräte zu spiegeln und IT-Probleme zu behandeln. Zum Spiegeln von Benutzern muss die Microsoft-Remoteunterstützung aktiviert sein; sie ist standardmäßig aktiviert, wenn der VDA installiert ist.
- **Anwendungsbereitstellung:** In XenApp 6.5 und Vorversionen wurden mit dem Assistenten zur Anwendungsveröffentlichung Anwendungen vorbereitet und für Benutzer bereitgestellt. In XenApp und XenDesktop 7.x erstellen Sie Anwendungen mit Studio und stellen Sie den Benutzern in einer Bereitstellungsgruppe zur Verfügung. In Studio konfigurieren Sie zunächst eine Site, erstellen und geben Maschinenkataloge an und dann erstellen Sie Bereitstellungsgruppen, die Maschinen aus diesen Maschinenkatalogen verwenden. Mit Bereitstellungsgruppen wird festgelegt, welche Benutzer Zugriff auf die bereitgestellten Anwendungen haben.
- **Datenbank:** In XenApp und XenDesktop 7.x werden die Konfigurationsinformationen nicht im IMA-Datenspeicher gespeichert. Stattdessen werden Konfigurations- und Sitzungsinformationen in einer Microsoft SQL Server-Datenbank gespeichert.

- **Lastverwaltungsrichtlinie:** In XenApp 6.5 und Vorversionen verwenden Lastauswertungsprogramme vordefinierte Messungen zur Bestimmung der Last auf einer Maschine. Benutzerverbindungen können weniger ausgelasteten Maschinen zugeordnet werden. In XenApp und XenDesktop 7.x erfolgt der Lastausgleich auf Maschinen mit Lastverwaltungsrichtlinien.
- **Delegierte Administration:** In XenApp 6.5 und Vorversionen wurden benutzerdefinierte Administratoren erstellt und ihnen wurden Berechtigungen auf der Basis von Ordnern und Objekten zugewiesen. In XenApp und XenDesktop 7.x basieren benutzerdefinierte Administratoren auf Rollen- und Geltungsbereichspaaren. Eine Rolle repräsentiert eine Stellenfunktion. Ihr sind definierte Berechtigungen zugewiesen, die eine Delegierung erlauben. Ein Geltungsbereich steht für eine Sammlung von Objekten. Vordefinierte Administratorrollen haben spezifische Berechtigungssätze, z. B. für Helpdesk, Anwendungen, Hosting und Kataloge. Beispiel: Helpdeskadministratoren können nur mit einzelnen Benutzern in bestimmten Sites arbeiten, während Volladministratoren die gesamte Bereitstellung überwachen und systemweite IT-Probleme behandeln können.

Der Übergang zu FMA bedeutet außerdem, dass einige in XenApp 6.5 und Vorversionen verwendete Features möglicherweise anders implementiert worden sind oder dass Sie sie eventuell durch andere Features, Komponenten oder Tools ersetzen müssen, um das gleiche Ziel zu erreichen.

XenApp 6.5 und Vorversionen	XenApp und XenDesktop 7.x
Sitzungsvorabstart und Sitzungsfortbestehen, die mit Richtlinieneinstellungen konfiguriert sind	Sitzungsvorabstart und Sitzungsfortbestehen, die durch Bearbeiten der Bereitstellungsgruppeneinstellungen konfiguriert sind. Wie in XenApp 6.5 ermöglichen diese Features Benutzern einen schnellen Zugriff auf Anwendungen, indem Sitzungen gestartet werden, bevor sie angefordert werden (Sitzungsvorabstart), und aktiv bleiben, nachdem ein Benutzer alle Anwendungen geschlossen hat (Sitzungsfortbestehen). In XenApp und XenDesktop 7.x aktivieren Sie die Features für bestimmte Benutzer, indem Sie diese Einstellungen für vorhandene Bereitstellungsgruppen konfigurieren. Siehe Konfigurieren des Vorabstarts und des Fortbestehens von Sitzungen.
Unterstützung für nicht authentifizierte (anonyme) Benutzer erfolgt durch Zuweisen von Rechten für anonyme Benutzer beim Festlegen der Eigenschaften für veröffentlichte Anwendungen	Unterstützung für nicht authentifizierte (anonyme) Benutzer erfolgt durch Konfigurieren dieser Option, wenn Sie die Benutzereigenschaften einer Bereitstellungsgruppe festlegen. Siehe Benutzer.
Lokaler Hostcache ermöglicht das Funktionieren eines Workerservers, selbst wenn eine Verbindung zum Datenspeicher nicht verfügbar ist	Verbindungsleasing ermöglicht Benutzern die Wiederverbindung mit den zuletzt verwendeten Anwendungen und Desktops, selbst wenn die Sitedatenbank nicht verfügbar ist. Das Feature für Verbindungsleasing ergänzt die bewährten Methoden zum Bereitstellen hoher Verfügbarkeit bei SQL Server. Siehe Verbindungsleasing.

Anwendungsstreaming	App-V stellt gestreamte Anwendungen bereit, die mit Studio verwaltet werden.
Webinterface	Citrix empfiehlt, dass Sie StoreFront einsetzen.
SmartAuditor	Verwenden Sie die Sitzungsaufzeichnung. Sie können auch alle Sitzungsaktivitäten aus einer administrativen Perspektive mit der Konfigurationsprotokollierung aufzeichnen.

Active Directory

Feb 29, 2016

Active Directory ist zum Authentifizieren und Autorisieren erforderlich. Mit der Kerberos-Infrastruktur in Active Directory wird die Authentizität und Vertraulichkeit der Kommunikation zwischen den Delivery Controllern garantiert. Informationen zu Kerberos finden Sie in der Dokumentation von Microsoft.

Der Artikel Systemanforderungen enthält die unterstützten Funktionsebenen für Gesamtstruktur und Domäne. Zur Verwendung der Richtlinienmodellierung muss der Controller unter Windows 2003 oder höher bis Windows Server 2012 R2 ausgeführt werden. Dies wirkt sich nicht auf die Domänenfunktionsebene aus.

Dieses Produkt unterstützt Folgendes:

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

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

Tipp: Ändern Sie weder den Computernamen noch die Domänenmitgliedschaft eines Controllers, nachdem Sie die Site konfiguriert haben.

Hinweis: Diese Informationen gelten für Versionen ab XenDesktop 7.1 und XenApp 7.5. Sie gelten nicht für ältere Versionen von XenDesktop und XenApp.
Bei einer Active Directory-Umgebung mit mehreren Gesamtstrukturen und unidirektionalen oder bidirektionalen Vertrauensstellungen können Sie DNS-Weiterleitungen zur Suche und Registrierung von Namen verwenden. Mit dem Assistenten zum Zuweisen der Objektverwaltung können Sie den entsprechenden Active Directory-Benutzern das Erstellen von Computerkonten ermöglichen. Weitere Informationen zu diesem Assistenten finden Sie in der Dokumentation von Microsoft.

In der DNS-Infrastruktur sind keine Reverse-DNS-Zonen erforderlich, wenn die entsprechenden DNS-Weiterleitungen zwischen Gesamtstrukturen eingerichtet sind.

Der SupportMultipleForest-Schlüssel ist erforderlich, wenn der VDA und der Controller in unterschiedlichen Gesamtstrukturen eingerichtet sind, unabhängig davon, ob sich die Active Directory- und NetBIOS-Namen voneinander unterscheiden. Der Schlüssel "SupportMultipleForest" ist nur auf dem VDA nötig. Mit den folgenden Informationen fügen Sie einen Registrierungsschlüssel hinzu:

Achtung: Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.

- HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\SupportMultipleForest
  - Name: SupportMultipleForest
  - Typ: REG_DWORD
  - Wert: 0x00000001 (1)

Sie müssen möglicherweise die DNS-Konfiguration umkehren, wenn sich der DNS-Namespace vom Active Directory-Namespace unterscheidet.

Wenn externe Vertrauensstellungen während des Setups vorhanden sind, ist der Registrierungsschlüssel "ListOfSIDs" erforderlich. Der Registrierungsschlüssel "ListOfSIDs" ist auch erforderlich, wenn der vollqualifizierte Domänenname (FQDN) für Active Directory sich vom DNS-FQDN unterscheidet oder die Domäne mit dem Domänencontroller einen anderen Netbios-Namen hat als der Active Directory-FQDN. Verwenden Sie zum Hinzufügen des Registrierungsschlüssels die folgenden Informationen:

- Für einen 32-Bit- oder 64-Bit-VDA verwenden Sie den Registrierungsschlüssel HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs.
  - Name: ListOfSIDs
  - Typ: REG_SZ
  - Daten: Sicherheits-ID (SID) der Controller

Wenn externe Vertrauensstellungen vorhanden sind, nehmen Sie die folgenden Änderungen auf dem VDA vor:

1. Navigieren Sie zur Datei: \Citrix\Virtual Desktop Agent\brokeragentconfig.exe.config.
2. Erstellen Sie eine Sicherungskopie der Datei.
3. Öffnen Sie die Datei in einem Textbearbeitungsprogramm, z. B. Editor.
4. Suchen Sie den Text allowNtlm="false" und ändern Sie den Text in allowNtlm="true".
5. Speichern Sie die Datei.

Nach dem Hinzufügen des Registrierungsschlüssels "ListOfSIDs" und der Bearbeitung der Datei brokeragent.exe.config starten Sie den Citrix Desktopdienst neu, um die Änderungen anzuwenden.

In der folgenden Tabelle werden die unterstützten Vertrauenstypen aufgeführt:

Vertrauenstyp	Transitivität	Richtung	In diesem Release unterstützt
Über-/untergeordnet	Transitiv	Bidirektional	Ja
Strukturstamm	Transitiv	Bidirektional	Ja
Extern	Nicht transitiv	Unidirektional oder bidirektional	Ja

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

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

Datenbanken

Jul 22, 2016

XenApp- bzw. XenDesktop-Sites verwenden drei SQL Server-Datenbanken:

- **Site:** (auch "Sitekonfiguration") enthält die Konfiguration der ausgeführten Site sowie den aktuellen Sitzungszustand und Verbindungsinformationen.
- **Konfigurationsprotokollierung**: (auch "Protokollierung") enthält Informationen über Änderungen an der Sitekonfiguration und Administratoraktivitäten. Diese Datenbank wird verwendet, wenn die Konfigurationsprotokollierung aktiviert ist (diese ist standardmäßig aktiviert).
- **Überwachung:** enthält von Director genutzte Daten, z. B. Sitzungs- und Verbindungsinformationen.

Jeder Delivery Controller kommuniziert mit der Sitedatenbank, zwischen Controller und Datenbank ist eine Windows-Authentifizierung 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. Neue Verbindungen können nicht hergestellt werden, wenn der Datenbankserver nicht verfügbar ist, außer in manchen Fällen, wenn das Verbindungsleasing konfiguriert ist.

Citrix empfiehlt, dass Sie regelmäßig ein Backup der Datenbanken durchführen, damit diese bei einem Ausfall des Datenbankservers von dem Backup wiederhergestellt werden können. Die Backupstrategie kann für jede Datenbank anders sein. Anweisung finden Sie unter CTX135207.

Wenn die Site mehr als eine Zone enthält, muss die Sitedatenbank in der primären Zone residieren. Controller in jeder Zone kommunizieren mit der Datenbank.

Hohe Verfügbarkeit

Es gibt einige Hochverfügbarkeitslösungen, die Sie in Betracht ziehen können, um automatisches Failover zu gewährleisten:

- **AlwaysOn-Verfügbarkeitsgruppen:** Dies ist eine Lösung für Hochverfügbarkeit 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 http://msdn.microsoft.com/en-us/library/hh510230.
- **Spiegelung der SQL Server-Datenbank:** Dies stellt sicher, dass ein automatische Failoverprozess in nur wenigen Sekunden stattfindet, falls der aktive Datenbankserver ausfällt. Benutzer werden in der Regel also nicht beeinträchtigt. Diese Methode ist teurer als andere Lösungen, da Volllizenzen für SQL Server auf jedem Datenbankserver erforderlich sind. In gespiegelten Umgebungen kann SQL Server Express nicht verwendet werden.
- **SQL-Clustering:** Mit dieser Technologie von Microsoft können Sie einem Server automatisch erlauben, die Aufgaben und Verantwortlichkeiten eines anderen, fehlgeschlagenen 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.

Hinweis: Die Installation eines Controllers auf einem Knoten in einer SQL-Clustering- oder SQL-Spiegelungsinstallation wird nicht unterstützt.

Das Feature für Verbindungsleasing ergänzt die bewährten Methoden zur hohen Verfügbarkeit bei SQL Server, da es Benutzern die Wiederverbindung mit den zuletzt verwendeten Anwendungen und Desktops ermöglicht, selbst wenn die Sitedatenbank nicht verfügbar ist. Weitere Informationen finden Sie im Artikel *Verbindungsleasing*.

Für den Fall, dass alle Controller einer Site ausfallen, können Sie den Virtual Delivery Agent so konfigurieren, dass er im Hochverfügbarkeitsmodus arbeitet, damit Benutzer weiterhin auf Desktops und Anwendungen zugreifen und diese verwenden können. Im Hochverfügbarkeitsmodus akzeptiert der VDA direkte ICA-Verbindungen von Benutzern anstelle von durch den Controller vermittelten Verbindungen. Dieses Feature ist nur zur Verwendung in dem seltenen Fall, dass die Kommunikation mit allen Controllern fehlschlägt, vorgesehen. Es ist keine Alternative zu anderen Hochverfügbarkeitslösungen. Weitere Informationen finden Sie unter CTX 127564.

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. Dies genügt normalerweise für Machbarkeitsstudien oder Testumgebungen. SQL Server Express unterstützt jedoch keine Microsoft-Features für hohe Verfügbarkeit.

Diese Installation verwendet die Standarddienstkonten und -privilegien von Windows. Informationen zu diesen Standards und dem Hinzufügen von Windows-Dienstkonten zur sysadmin-Rolle finden Sie in der Microsoft-Dokumentation. In dieser Konfiguration verwendet der Controller das Netzwerkdienstkonto. Der Controller erfordert keine weiteren SQL Server-Rollen oder -Berechtigungen.

Bei Bedarf können Sie zum Ausblenden der Datenbankinstanz die Option **Instanz ausblenden** wählen. Geben Sie beim Konfigurieren der Datenbankadresse in Studio die statische Portnummer statt des Namens ein. Informationen zum Ausblenden einer Instanz des SQL Server-Datenbankmoduls finden Sie in der Dokumentation von Microsoft.

In den meisten Produktionsbereitstellungen und in Bereitstellungen, in denen Microsoft-Features für hohe Verfügbarkeit verwendet werden, muss eine andere (unterstützte) SQL Server-Version als SQL Server Express auf den anderen Computern (als dem mit dem ersten Controller) installiert werden. In dem Artikel über die Systemanforderungen werden die unterstützten SQL Server-Versionen aufgeführt. Die Datenbanken können auf einem oder mehreren Computern residieren.

Stellen Sie sicher, dass die SQL Server-Software installiert ist, bevor Sie eine Site erstellen. Sie müssen keine Datenbank erstellen, wenn Sie es jedoch tun, muss sie leer sein. Außerdem empfiehlt sich das Konfigurieren von Microsoft-Features für hohe Verfügbarkeit.

Halten Sie die SQL Server-Installation mit Windows Update auf dem neuesten Stand.

Einrichten der Datenbanken mit dem Assistenten für die Siteerstellung

Legen Sie Namen und Speicherorte der Datenbanken auf der Seite **Datenbanken** des Assistenten für die Siteerstellung

fest (s. *Datenbankadressformate* weiter unten). Zur Vermeidung von Fehlern bei künftigen Abfragen von Monitor Service durch Director verwenden Sie keine Leerzeichen im Namen der Überwachungsdatenbank.

Die Seite **Datenbanken** bietet zwei Optionen zum Einrichten der Datenbanken: automatisch und Skriptverwendung. Normalerweise können Sie die automatische Erstellung wählen, wenn Sie die erforderlichen Berechtigungen für die Datenbank haben (Studio-Benutzer und Citrix Administrator). Weitere Informationen finden Sie unter "Für die Einrichtung von Datenbanken erforderliche Berechtigungen" weiter unten.

Sie können den Speicherort einer Datenbank nach Erstellen der Site ändern. Weitere Informationen finden Sie unter "Ändern des Datenbankspeicherorts" weiter unten.

Zum Konfigurieren einer Site für die Verwendung einer gespiegelten Datenbank führen Sie die folgenden Verfahren durch und fahren Sie dann mit der automatischen oder skriptbasierten Einrichtung fort:

1. Installieren Sie SQL Server auf zwei Servern, A und B.
2. Erstellen Sie auf Server A die Datenbank, die als Hauptdatenbank verwendet werden soll. Sichern Sie die Datenbank auf Server A und kopieren Sie sie anschließend auf Server B.
3. Stellen Sie auf Server B die Sicherungsdatei wieder her.
4. Starten Sie die Spiegelung auf Server A.

Tipp: 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.

Wenn Sie die erforderlichen Datenbankberechtigungen haben, wählen Sie auf der Seite **Datenbanken** des Assistenten für die Siteerstellung die Option "Datenbanken mit Studio erstellen und einrichten" und geben Sie die Namen und Adressen der Hauptdatenbanken ein.

Gibt es an einer von Ihnen angegebenen Adresse eine Datenbank, muss sie leer sein. Gibt es an der angegebenen Adresse keine Datenbank, wird eine entsprechende Meldung angezeigt und Sie werden gefragt, ob eine Datenbank erstellt werden soll. Wenn Sie dies bejahen, werden die Datenbanken erstellt und die Initialisierungsskripts für die Haupt- und Replikatdatenbanken ausgeführt.

Wenn Sie nicht die erforderlichen Datenbankberechtigungen haben, muss eine andere Person mit diesen Berechtigungen, z. B. ein Datenbankadministrator, helfen. Verfahren:

1. Wählen Sie im Assistenten für die Siteerstellung die Option **Skripts generieren**. Es werden insgesamt sechs Skripts für die drei Datenbanken erstellt, eines für jede Hauptdatenbank und eines für jedes Replikat. Sie können den Speicherort für die Skripts festlegen.
2. Geben Sie die Skripts Ihrem Datenbankadministrator. Der Assistent für die Siteerstellung hält an diesem Punkt automatisch an und wenn Sie später zurückkehren, werden Sie aufgefordert, die Siteerstellung fortzusetzen.

Der Datenbankadministrator erstellt dann die Datenbanken. Die Datenbanken müssen folgende Merkmale aufweisen:

- Sortierung, die in "_CI_AS_KS" endet. Citrix empfiehlt die Verwendung einer Sortierung, die in "_100_CI_AS_KS" endet.

- Zur Gewährleistung der optimalen Leistung aktivieren Sie den SQL Server-Read-Committed-Snapshot. Weitere Informationen finden Sie unter CTX 137161.
- Features für hohe Verfügbarkeit sollten nach Bedarf konfiguriert werden.
- Zum Konfigurieren der Spiegelung legen Sie für die Datenbank das vollständige Wiederherstellungsmodell fest (Standardeinstellung ist das einfache Wiederherstellungsmodell). Sichern Sie die Hauptdatenbank und kopieren Sie die Sicherungsdatei auf den Spiegelserver. Stellen Sie in der Spiegeldatenbank die Sicherungsdatei auf dem Spiegelserver wieder her. Starten Sie dann die Spiegelung auf dem Hauptserver.

Der Datenbankadministrator führt jedes xxx_Replica.sql-Skript mit dem SQLCMD-Befehlszeilenprogramm oder mit SQL Server Management Studio im SQLCMD-Modus in den SQL Server-Datenbankinstanzen mit hoher Verfügbarkeit (sofern konfiguriert) aus und dann jedes xxx_Principal.sql-Skript in den Hauptinstanzen der SQL Server-Datenbank. Weitere Informationen zu SQLCMD können Sie der Dokumentation von Microsoft entnehmen.

Wenn alle Skripts erfolgreich ausgeführt wurden, übergibt der Datenbankadministrator dem Citrix Administrator die drei Hauptdatenbankadressen.

In Studio werden Sie aufgefordert, die Siteerstellung fortzusetzen, und die Seite **Datenbanken** wird wieder angezeigt. Geben Sie die Adressen ein. Wenn einer der Server mit einer Datenbank nicht erreicht werden kann, wird eine Fehlermeldung angezeigt.

Für die Einrichtung von Datenbanken erforderliche Berechtigungen

Zum Erstellen und Initialisieren der Datenbanken (bzw. zum Ändern des Speicherorts einer Datenbank) müssen Sie lokaler Administrator und Domänenbenutzer sein. Sie benötigen zudem bestimmte SQL Server-Berechtigungen. Die nachfolgend aufgeführten Berechtigungen können über eine Active Directory-Gruppenmitgliedschaft explizit konfiguriert oder erworben werden. Wenn Ihre Studio-Anmeldeinformationen diese Berechtigungen nicht umfassen, werden Sie aufgefordert, Benutzeranmeldeinformationen für SQL Server einzugeben.

Vorgang	Zweck	Serverrolle	Datenbankrolle
Erstellen einer Datenbank	Erstellen einer geeigneten leeren Datenbank	dbcreator	
Erstellen eines Schemas	Erstellen aller dienstspezifischen Schemas und Hinzufügen des ersten Controllers zur Site	securityadmin *	db_owner
Hinzufügen eines Controllers	Hinzufügen eines weiteren Controllers (zusätzlich zum ersten) zur Site	securityadmin *	db_owner
Hinzufügen eines Controllers	Hinzufügen einer Controller-Anmeldung zu dem Datenbankserver, der derzeit die	securityadmin *	

(Spiegelungsserver)	Spiegelrolle einer gespiegelten Datenbank hat		
Aktualisieren eines Schemas	Anwenden von Aktualisierungen oder Hotfixes auf das Schema		db_owner

* Zwar ist die securityadmin-Serverrolle technisch restriktiver als die sysadmin-Serverrolle, aber in der Praxis ist sie als gleichwertig anzusehen.

Wenn Sie diese Vorgänge mit Studio ausführen, muss das Benutzerkonto Mitglied der sysadmin-Serverrolle sein.

Datenbankadressformate

Datenbankadressen können in einem der folgenden Formate angegeben werden:

- Servername
- Servername\Instanzname
- Servername,Portnummer

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 ändern. Berücksichtigen Sie Folgendes, wenn Sie den Speicherort einer Datenbank ändern:

- Die Daten werden nicht aus der bestehenden Datenbank in die neue Datenbank importiert.
- Die Protokolle beider Datenbanken können beim Abrufen von Protokollen nicht aggregiert werden.
- Der erste Protokolleintrag in der neuen Datenbank gibt an, dass eine Datenbankänderung stattfand, die vorherige Datenbank wird jedoch nicht angegeben.

Sie können den Speicherort der Konfigurationsprotokollierungsdatenbank nicht ändern, wenn die verbindliche Protokollierung aktiviert ist.

Ändern des Datenbankspeicherorts

1. Vergewissern Sie sich, dass eine unterstützte Version von Microsoft SQL Server auf dem Server installiert ist, auf dem die Datenbank residieren soll. Richten Sie Features für hohe Verfügbarkeit nach Bedarf ein.
2. Wählen Sie im Studio-Navigationsbereich **Konfiguration** aus.
3. Wählen Sie die Datenbank aus, für die Sie einen neuen Speicherort angeben möchten, und wählen Sie dann im Aktionsbereich **Datenbank ändern** aus.
4. Geben Sie den neuen Speicherort und den Datenbanknamen ein.
5. Wenn die Datenbank von Studio erstellt werden soll und Sie die notwendigen Berechtigungen haben, klicken Sie auf **OK**. Wenn Sie dazu aufgefordert werden, klicken Sie auf **OK**. Studio erstellt dann die Datenbank automatisch. Studio versucht, mit Ihren Anmeldeinformationen auf die Datenbank zuzugreifen; wenn dies fehlschlägt, werden Sie zur Eingabe der Anmeldeinformationen des Datenbankbenutzers aufgefordert. Das Datenbankschema wird dann von Studio in die

Datenbank hochgeladen. Die Anmeldeinformationen werden nur für den Zeitraum der Datenbankerstellung gespeichert.

6. Wenn die Datenbank nicht von Studio erstellt werden soll oder Sie die erforderliche Berechtigung nicht haben, klicken Sie auf **Skript generieren**. Die generierten Skripts enthalten Anweisungen, wie Sie die Datenbank und ggf. die Spiegeldatenbank manuell erstellen. Stellen Sie vor dem Hochladen des Schemas sicher, dass die Datenbank leer ist und dass mindestens ein Benutzer Zugriffs- bzw. Änderungsberechtigung für die Datenbank hat.

Bereitstellungsmethoden

Feb 29, 2016

Es ist eine Herausforderung, die Anforderungen aller Benutzer mit einer Virtualisierungsbereitstellung erfüllen. Mit XenApp und XenDesktop können Administratoren die Benutzererfahrungen mit verschiedenen Methoden, die auch als FlexCast-Modelle bezeichnet werden, anpassen.

Diese Bereitstellungsmethoden, von denen jede ihre Vor- und Nachteile hat, bieten die beste Benutzererfahrung für jeden Anwendungsfall.

Touchscreen-Geräte, wie Tablets und Smartphones, sind jetzt Standard in Mobilität. Wenn Windows-basierte Anwendungen auf ihnen ausgeführt werden, die normalerweise auf großen Bildschirmen angezeigt werden und für volle Funktionalität Klicken mit der rechten Maustaste erfordern, können diese Geräte Probleme verursachen.

XenApp mit Citrix Receiver bietet eine sichere Lösung, sodass die Benutzer von Mobilgeräten Zugriff auf alle Funktionen ihrer Windows-basierten Apps haben, ohne dass diese kostenaufwendig für native mobile Plattformen umgeschrieben werden müssen.

Die Bereitstellungsmethode der mit XenApp veröffentlichten Anwendungen verwendet die HDX-Mobiltechnologie, die die mit der Mobilisierung von Windows-Anwendungen assoziierten Probleme löst. Mit dieser Methode können Windows-Anwendungen für die Toucheingabe umgestaltet werden, während Features wie Mehrfingerbewegungen, native Menüsteuerung, Kamera und GPS-Funktionen erhalten bleiben. Viele Touchfeatures sind nativ in XenApp und XenDesktop und zu ihrer Aktivierung sind keine Änderungen am Anwendungsquellcode nötig.

Zu diesen Features gehören Folgende:

- Automatische Anzeige der Tastatur, wenn ein bearbeitbares Feld den Fokus erhält
- Größeres Auswahlsteuerelement ersetzt Windows-Kombinationsfeld-Steuerelement
- Mehrfingergesten, z. B. Vergrößern und Verkleinern mit zwei Fingern
- Trägheitssensitiver Bildlauf
- Touchpad oder direkte Cursornavigation

Das Aktualisieren von physischen Maschinen ist eine große Aufgabe, der sich viele Unternehmen alle drei bis fünf Jahre stellen müssen, besonders, wenn ein Unternehmen bei Betriebssystemen und Anwendungen immer auf dem neuesten Stand sein muss. Wachsende Unternehmen sehen sich zudem hohen Kosten für das Hinzufügen von neuen Maschinen zum Netzwerk gegenüber.

Mit der Bereitstellungsmethode eines VDI mit Personal vDisk können Einzelbenutzern vollständig personalisierte Desktopbetriebssysteme auf jeder Maschine oder jedem Thin Client mit Serverressourcen bereitgestellt werden. Administratoren können virtuelle Maschinen erstellen, deren Ressourcen, z. B. Verarbeitung, Arbeitsspeicher und Speicher, sich im Datencenter des Netzwerks befinden.

Dadurch kann das Leben älterer Maschinen verlängert werden, Software ist auf dem aktuellen Stand und Ausfallzeiten bei Upgrades werden minimiert.

Netzwerksicherheit ist ein wachsendes Problem, besonders bei der Arbeit mit Vertragsunternehmen, Partnern und gelegentlichen Mitarbeitern von Fremdfirmen, die Zugriff auf Unternehmensapps und Daten benötigen. Die Mitarbeiter benötigen möglicherweise auch leihweise Laptops oder andere Geräte, die zusätzliche Kosten verursachen.

Daten, Anwendungen und Desktops sind bei XenDesktop und XenApp hinter der Firewall des sicheren Netzwerks gespeichert, sodass Endbenutzer nur die Ein - und Ausgabevorgänge der Benutzergeräte wie Tastatureingaben, Mausklicks, Audio und Bildschirmaktualisierungen übermitteln. Durch die Verwaltung dieser Ressourcen in einem Datencenter bieten XenDesktop und XenApp eine sicherere Remotezugriffslösung als das übliche SSL VPN.

Bei einer VDI-Bereitstellung mit Personal vDisk können Administratoren Thin Clients oder die persönlichen Geräte von Benutzern nutzen, indem sie eine virtuelle Maschine auf einem Netzwerkserver erstellen und ein Betriebssystem für einzelne Benutzer anbieten. Auf diese Weise können IT-Abteilungen die Sicherheit gegenüber Mitarbeitern von Vertragsunternehmen aufrechterhalten, ohne zusätzliches teures Gerät kaufen zu müssen.

Beim Wechsel zu einem neuen Betriebssystem kann es eine Herausforderung sein, Legacy- und nicht kompatiblen Anwendungen bereitzustellen.

Mit VM-gehosteten Apps können Benutzer ältere Anwendungen über Citrix Receiver auf der aktualisierten virtuellen Maschine ohne Kompatibilitätsprobleme ausführen. Dadurch haben IT-Mitarbeiter mehr Zeit, Kompatibilitätsprobleme zu testen und zu beheben, Benutzern den Übergang zu erleichtern und die Effizienz bei Helpdeskanrufen zu erhöhen.

Zusätzliche Vorteile bei der Verwendung von XenDesktop während der Migration sind u. a.:
- Reduzierte Komplexität von Desktops
- Verbesserte Steuerung für IT-Mitarbeiter
- Erhöhte Flexibilität der Endbenutzer im Hinblick auf Geräte und Arbeitsplatz

Viele Designunternehmen und Herstellerfirmen sind stark auf professionelle 3-D-Grafikanwendungen angewiesen. Die Kosten der für diese Art Software erforderlichen leistungsfähigen Hardware sind für diese Unternehmen eine große finanzielle Belastung. Dazu kommen logistische Probleme durch die Freigabe großer Designdateien über FTP, E-Mail und andere Ad-hoc-Methoden.

Bei der XenDesktop-Bereitstellungsmethode für gehostete physische Desktops wird ein Desktopimage auf Arbeitsstationen und Bladeservern bereitgestellt, ohne dass Hypervisors benötigt werden, um grafikintensive 3-D-Anwendungen auf einem systemeigenen Betriebssystem auszuführen.

Alle Dateien werden in einem zentralen Datencenter im Netzwerk gespeichert und große Designdateien können schneller und sicherer für andere Benutzer im Netzwerk freigegeben werden, da die Dateien nicht zwischen Arbeitsstationen übertragen werden müssen.

Unternehmen mit großen Callcentern stehen vor der Herausforderung, zu Spitzenzeiten genügend Maschinen und zu anderen Zeiten nicht zu viele Maschinen im Einsatz zu haben.

Die gepoolte VDI-Bereitstellungsmethode bietet dynamischen Zugriff auf einen standardisierten Desktop für viele Benutzer zu minimalen Kosten. Die gepoolten Maschinen werden pro Sitzung nach dem Windhundprinzip zugeteilt.

Bei diesen virtuellen Maschinen fällt weniger alltägliche Verwaltung an, da während der Sitzung vorgenommene Änderungen

verworfen werden, wenn der Benutzer sich abmeldet. Dies erhöht auch die Sicherheit.

Von XenApp gehostete Desktops ist eine weitere Bereitstellungsmethode, die sich für Callcenter eignet. Bei dieser Methode werden mehrere Benutzerdesktops auf einem serverbasierten Betriebssystem gehostet.

Dies ist eine kosteneffizientere Methode als die gepoolte VDI-Bereitstellung, aber bei von XenApp gehosteten Desktops haben Benutzer keine Berechtigungen, um Anwendungen zu installieren, Systemeinstellungen zu ändern oder den Server neu zu starten.

Mit XenApp veröffentlichte Anwendungen und Desktops

Feb 29, 2016

Verwenden Sie Serverbetriebssystemmaschinen zum Bereitstellen von mit XenApp veröffentlichten Anwendungen und Desktops.

Anwendungsfall

- Gewünscht wird eine kostengünstige, serverbasierte Bereitstellung, um die Kosten für die Bereitstellung von Anwendungen für eine große Anzahl von Benutzern gering zu halten, und gleichzeitig eine sichere High-Definition-Benutzererfahrung zu bieten.
- Die Benutzer führen vordefinierte Aufgaben aus, es wird keine Personalisierung oder kein Offlinezugriff auf Anwendungen benötigt. Hierzu können aufgabenorientierte Mitarbeiter, wie z. B. Callcenter- und Einzelhandelsarbeitskräfte gehören, oder Benutzer, die Arbeitsstationen gemeinsam verwenden.
- Anwendungstypen: beliebig

Vorteile und Überlegungen

- Verwaltbare und skalierbare Lösung für das Datenzentrum.
- Kosteneffektivste Lösung für die Anwendungsbereitstellung.
- Gehostete Anwendungen werden zentral verwaltet und Benutzer können die Anwendung nicht ändern, wodurch eine konsistente, sichere und zuverlässige Benutzererfahrung bereitgestellt wird.
- Benutzer müssen online sein, um auf ihre Anwendungen zuzugreifen.

Benutzererfahrung

- Benutzer fordern eine oder mehrere Anwendungen von StoreFront über ihr Startmenü oder eine von Ihnen vorgegebene URL an.
- Anwendungen werden virtuell bereitgestellt und in High Definition auf Benutzergeräten angezeigt.
- Abhängig von den Profileinstellungen werden Benutzeränderungen gespeichert, wenn die Anwendungssitzung des Benutzers beendet wird. Andernfalls werden die Änderungen werden gelöscht.

Verarbeiten, Hosten und Bereitstellen von Anwendungen

- Die Anwendungsverarbeitung findet auf den Hostingmaschinen statt, nicht auf den Benutzergeräten. Die Hostingmaschine kann eine physische oder eine virtuelle Maschine sein.
- Anwendungen und Desktops sind auf einer Serverbetriebssystemmaschine gespeichert.
- Maschinen werden über Maschinenkataloge verfügbar gemacht.
- Maschinen aus Maschinenkatalogen sind in Bereitstellungsgruppen organisiert, die Benutzergruppen dieselben Anwendungen bereitstellen.
- Serverbetriebssystemmaschinen unterstützen Bereitstellungsgruppen, die Desktops oder Anwendungen oder beides hosten.

Sitzungsverwaltung und -zuweisung

- Auf Serverbetriebssystemmaschinen werden mehrere Sitzungen auf einer einzelnen Maschinen ausgeführt, über die mehrere Anwendungen und Desktops an mehrere, gleichzeitig verbundene Benutzer bereitgestellt werden. Jeder

Benutzer benötigt eine einzelne Sitzung, um die gehosteten Anwendungen auszuführen.

Beispiel: Ein Benutzer meldet sich an und fordert eine Anwendung an. Eine der Sitzungen auf dieser Maschine ist für die anderen Benutzer nicht mehr verfügbar. Ein zweiter Benutzer meldet sich an und fordert eine Anwendung an, die von dieser Maschine gehostet wird. Eine zweite Sitzung auf derselben Maschine ist damit jetzt nicht verfügbar. Wenn beide Benutzer weitere Anwendungen anfordern, werden keine zusätzlichen Sitzungen benötigt, da ein Benutzer mehrere Anwendungen in der gleichen Sitzung ausführen kann. Wenn zwei weitere Benutzer sich anmelden und Desktops anfordern, und zwei Sitzungen auf derselben Maschine verfügbar sind, hostet diese eine Maschine nun vier Sitzungen für vier verschiedene Benutzer.

- In der Bereitstellungsgruppe, der ein Benutzer zugewiesen ist, wird eine Maschine auf einem Server mit der geringsten Last ausgewählt. Ein Computer mit Sitzungsverfügbarkeit wird nach dem Zufallsprinzip zugewiesen und stellt einem Benutzer bei der Anmeldung Anwendungen bereit.

Bereitstellen mit XenApp veröffentlichter Anwendungen und Desktops

1. Installieren Sie die bereitzustellenden Anwendungen auf einem Masterimage mit einem unterstützten Windows-Serverbetriebssystem.
2. Erstellen Sie einen Maschinenkatalog für dieses Masterimage oder aktualisieren Sie einen vorhandenen Katalog mit dem Masterimage.
3. Erstellen Sie eine Bereitstellungsgruppe zum Bereitstellen von Desktops und Anwendungen. Wenn Sie Anwendungen bereitstellen, wählen Sie die gewünschten aus.

Einzelheiten finden Sie in den Artikeln zu Installation und Konfiguration.

VM-gehostete Apps

Feb 29, 2016

Bereitstellen VM-gehosteter Anwendungen über Desktopbetriebssystemmaschinen

Anwendungsfall

- Gewünscht wird eine clientbasierte Anwendungsbereitstellungslösung, die eine sichere, zentrale Verwaltung bietet und eine große Anzahl von Benutzern pro Hostserver (oder Hypervisor) unterstützt und Benutzern Anwendungen bereitstellt, die problemlos in High Definition angezeigt werden.
- Benutzer sind interne und externe Auftragnehmer, Partner aus Fremdunternehmen und andere vorläufige Teammitglieder. Sie benötigen keinen Offlinezugriff auf gehostete Anwendungen.
- Anwendungsarten: Anwendungen, die möglicherweise nicht gut mit anderen Anwendungen funktionieren oder mit dem Betriebssystem interagieren, z. B. .NET Framework. Dieser Typ von Anwendungen eignet sich gut für das Hosting auf virtuellen Maschinen.

  Anwendungen, die auf älteren Betriebssystemen (z. B. Windows XP oder Windows Vista) und älteren Architekturen (z. B. 32 Bit oder 16 Bit) ausgeführt werden. Durch Isolieren jeder Anwendung auf einer eigenen virtuellen Maschine werden die anderen Benutzer bei Ausfall einer Maschine nicht beeinträchtigt.

Vorteile und Überlegungen

- Anwendungen und Desktops auf dem Masterimage werden sicher verwaltet, gehostet und auf Maschinen im Datenzentrum ausgeführt, womit eine kosteneffektivere Lösung für die Anwendungsbereitstellung bereitgestellt wird.
- Die Benutzer können bei der Anmeldung willkürlich einer Maschine in einer Bereitstellungsgruppe zugewiesen werden, die für das Hosting einer Anwendung konfiguriert ist. Sie können auch einem einzelnen Benutzer eine einzelne Maschine für die Anwendungsbereitstellung jedes Mal statisch zuweisen, wenn sich der Benutzer anmeldet. Bei statisch zugewiesenen Maschinen kann der Benutzer eigene Anwendungen auf der virtuellen Maschine installieren und verwalten.
- Das Ausführen mehrerer Sitzungen auf Desktopbetriebssystemmaschinen wird nicht unterstützt. Daher beansprucht jeder Benutzer bei der Anmeldung eine einzelne Maschine innerhalb einer Bereitstellungsgruppe und der Zugriff auf die Anwendungen muss online erfolgen.
- Bei dieser Methode werden die Serverressourcen für die Verarbeitung von Anwendungen sowie der Speicher für die persönlichen vDisks der Benutzer erhöht.

Benutzererfahrung

Die gleiche nahtlose Anwendungserfahrung wie mit gehosteten, freigegebenen Anwendungen auf Serverbetriebssystemmaschinen.

Verarbeiten, Hosten und Bereitstellen von Anwendungen

Wie bei Serverbetriebssystemmaschinen, nur dass es sich um virtuelle Desktopbetriebssystemmaschinen handelt.

Sitzungsverwaltung und -zuweisung

- Desktopbetriebssystemmaschinen führen eine Desktopsitzung von einer Maschine aus. Nur beim Zugriff auf Anwendungen: Ein Benutzer kann mehrere Anwendungen verwenden (und ist nicht auf eine Anwendung eingeschränkt), da das Betriebssystem jede Anwendung als eine neue Sitzung ansieht.
- Innerhalb einer Bereitstellungsgruppe erhalten Benutzer bei der Anmeldung entweder statischen Zugriff auf eine

Maschine (d. h. bei jeder Anmeldung die gleiche Maschine) oder es wird ihnen eine Maschine nach Sitzungsverfügbarkeit zugewiesen.

Bereitstellen von VM-gehosteten Apps:

1. Installieren Sie die bereitzustellenden Anwendungen auf einem Masterimage mit einem unterstützten Windows-Desktopbetriebssystem.
2. Erstellen Sie einen Maschinenkatalog für dieses Masterimage oder aktualisieren Sie einen vorhandenen Katalog mit dem Masterimage.
3. Entscheiden Sie beim Definieren der Desktopdarstellung für den Maschinenkatalog, ob Benutzer bei jeder Anmeldung mit einer neuen VM oder mit derselben VM verbunden werden.
4. Erstellen Sie eine Bereitstellungsgruppe zum Bereitstellen der Anwendungen für Benutzer.
5. Wählen Sie in der Liste der installierten Anwendungen die Anwendung aus, die Sie bereitstellen möchten.

Einzelheiten finden Sie in den Artikeln zu Installation und Konfiguration.

VDI-Desktops

Feb 29, 2016

Verwenden Sie Desktopbetriebssystemmaschinen zum Bereitstellen von VDI-Desktops.

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

VDI-Desktops benötigen mehr Ressourcen als mit XenApp veröffentlichte Desktops, aber es ist nicht erforderlich, dass die auf ihnen installierten Anwendungen serverbasierte Betriebssysteme unterstützen. Abhängig vom ausgewählten Typ des VDI-Desktops kann der Desktop einzelnen Benutzern zugewiesen werden und von den Benutzern in hohem Maße personalisiert werden.

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

- Zufällige, nicht beständige Desktops (gepoolte VDI-Desktops): Jedes Mal, wenn ein Benutzer sich anmeldet, um einen dieser Desktops zu verwenden, wird eine Verbindung zu einem dynamisch ausgewählten Desktop in einem Pool von Desktops erstellt, die alle auf einem Masterimage basieren. Alle Änderungen an dem Desktop gehen verloren, wenn die Maschine neu gestartet wird.
- Statischer, nicht beständiger Desktop: Wenn sich ein Benutzer zum ersten Mal anmeldet, um einen dieser Desktops zu verwenden, wird ihm ein Desktop aus einem Pool von Desktops zugewiesen, die alle auf einem Masterimage basieren. Daraufhin wird dem Benutzer jedes Mal, wenn er sich anmeldet, um einen der Desktops zu verwenden, derselbe Desktop wie beim ersten Mal zugewiesen. Alle Änderungen an dem Desktop gehen verloren, wenn die Maschine neu gestartet wird.
- Statisch und permanent (VDI-Desktop mit persönlicher vDisk): Im Gegensatz zu anderen Typen der VDI-Desktops können diese Desktops vollständig personalisiert werden. Wenn sich ein Benutzer zum ersten Mal anmeldet, um einen dieser Desktops zu verwenden, wird ihm ein Desktop aus einem Pool von Desktops zugewiesen, die alle auf einem Masterimage basieren. Daraufhin wird dem Benutzer jedes Mal, wenn er sich anmeldet, um einen der Desktops zu verwenden, derselbe Desktop wie beim ersten Mal zugewiesen. Änderungen am Desktop bleiben beim Neustart der Maschine erhalten, da sie auf einer persönlichen vDisk gespeichert werden.

Bereitstellen von VDI-Desktops:

1. Erstellen Sie ein Masterimage mit einem unterstützten Windows-Desktopbetriebssystem.
2. Erstellen Sie einen Maschinenkatalog für dieses Masterimage oder aktualisieren Sie einen vorhandenen Katalog mit dem Masterimage. Entscheiden Sie beim Definieren der Desktopdarstellung für den Maschinenkatalog, ob Benutzer bei jeder Anmeldung mit einer neuen VM oder mit derselben VM verbunden werden, und legen Sie fest, ob Änderungen am Desktop beibehalten werden.
3. Erstellen Sie eine Bereitstellungsgruppe zum Bereitstellen der Desktops für Benutzer.

Einzelheiten finden Sie in den Artikeln zu Installation und Konfiguration.

Installation und Konfiguration

Feb 29, 2016

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

Befolgen Sie bei der Bereitstellung von XenApp bzw. XenDesktop nachfolgend aufgeführte Reihenfolge.

Vorbereiten

Lesen Sie den Artikel Vorbereiten der Installation und erledigen Sie alle erforderlichen Aufgaben. Dies umfasst:

- Kennenlernen von XenApp und XenDesktop – der Artikel enthält Quellen mit Informationen über Konzepte, Features, Unterschiede zu früheren Releases, Systemanforderungen und Datenbanken.
- Einrichten der Infrastruktur für Virtualisierung, Hosting und oder Support (falls verwendet)
- Einrichten der Maschinen, auf denen die Komponenten installiert werden
- Einrichten der Active Directory-Umgebung

Der Artikel enthält zudem Angaben zu den Informationen, die Sie bei der Installation der Komponenten und beim Aktivieren von Features auswählen oder angeben müssen.

Wenn Sie Linux-VDAs installieren möchten, lesen Sie vor der Installation die Artikel Installieren von VDAs unter Red Hat Linux und Installieren von VDAs unter SUSE Linux.

Installieren der Kernkomponenten

Installieren Sie Delivery Controller, Citrix Studio, Citrix Director, Citrix Lizenzserver und Citrix StoreFront. Sie können eine assistentengestützte grafische Oberfläche oder eine Befehlszeilenoberfläche für die skriptbasierte Installation verwenden. Bei beiden Methoden werden die meisten Voraussetzungen automatisch installiert.

Erstellen einer Site

Wenn Sie nach der Installation der Kernkomponenten Studio starten, führt Sie der Assistent für die Siteerstellung automatisch durch die Erstellung einer Site.

Installieren eines oder mehrerer Virtual Delivery Agents (VDAs)

Installieren Sie einen VDA auf einem Windows-Computer, entweder auf dem künftig zur Erstellung virtueller Maschinen genutzten Masterimage oder direkt auf jeder Maschine. Sie können eine grafische Benutzeroberfläche oder eine Befehlszeilenoberfläche verwenden. Beispielskripts werden bereitgestellt, wenn Sie die VDAs über Active Directory installieren möchten.

Bei Maschinen mit einem Linux-Betriebssystem befolgen Sie die Anweisungen für die Installation eines VDA unter Red Hat Linux bzw. unter SUSE Linux.

Für eine Remote-PC-Zugriff-Bereitstellung installieren Sie einen VDA für Desktopbetriebssysteme auf jedem Büro-PC. Verwenden Sie aus Effizienzzwecken die Befehlszeilenoberfläche des eigenständigen VDA-Installers und Ihre gewohnten Methoden zur elektronischen Softwareverteilung.

Installieren optionaler Komponenten

Wenn Sie den universellen Druckserver von Citrix verwenden möchten, installieren Sie dessen Serverkomponente auf Ihren Druckservern. Sie können eine grafische Benutzeroberfläche oder eine Befehlszeilenoberfläche verwenden.

Sie können auch zusätzlichen Citrix Komponenten in die XenApp- oder XenDesktop-Bereitstellung integrieren. Beispiel:

- Provisioning Services ist eine optionale Komponente von XenApp und XenDesktop, mit der Maschinen durch das Streaming eines Masterimages auf die Zielgeräte bereitgestellt werden. Weitere Informationen finden Sie in der Dokumentation zu Provisioning Services.
- Citrix NetScaler Gateway ist eine sichere Anwendungszugriffslösung, die Administratoren durch Richtlinien auf Anwendungsebene und durch Aktionssteuerung ermöglicht, den Zugriff auf Anwendungen und Daten zu sichern. Weitere Informationen finden Sie in der Dokumentation zu Citrix NetScaler Gateway.
- Citrix CloudBridge bietet eine Reihe von Geräten, die die WAN-Leistung optimieren. Weitere Informationen finden Sie in der Dokumentation zu Citrix CloudBridge.

Erstellen von Maschinenkatalogen

Nachdem Sie eine Site in Studio erstellt haben, werden Sie durch die Erstellung eines Maschinenkatalogs geführt.

Ein Katalog kann physische oder virtuelle Maschinen (VMs) enthalten. Virtuelle Maschinen können aus einem Masterimage erstellt werden. Wenn Sie einen unterstützten Hypervisor oder Clouddienst zum Bereitstellen von VMs verwenden möchten, müssen Sie zuerst ein Masterimage auf dem betreffenden Host erstellen. Bei der Erstellung des Katalogs geben Sie dann das Image an, das zum Erstellen von VMs verwendet werden soll.

Erstellen einer Bereitstellungsgruppe

Nachdem Sie den ersten Maschinenkatalog in Studio erstellt haben, werden Sie durch die Erstellung einer Bereitstellungsgruppe geführt.

Bereitstellungsgruppen steuern, welche Benutzer auf Maschinen in einem Maschinenkatalog zugreifen können und welche Anwendungen ihnen zur Verfügung stehen.

Vorbereiten der Installation

Feb 29, 2016

Dieser Abschnitt enthält folgende Themen:

Allgemeiner Installationsleitfaden

- Wenn Sie Produkt und Komponenten nicht ausreichend kennen, lesen Sie die Artikel unter Technische Übersicht. Wenn Sie derzeit XenApp 6.x oder eine Vorgängerversion ausführen, können Sie im Artikel Konzepte und Komponenten nachlesen, worin die Unterschiede zur 7.x-Version von XenApp und XenDesktop bestehen.
- Bei der Planung der Bereitstellung konsultieren Sie die Artikel unter Sicherheit.
- Informieren Sie sich über bekannte Probleme, die bei der Installation auftreten können.
- Wenn Sie einen unterstützten Hypervisor oder Clouddienst für virtuelle Maschinen zur Bereitstellung von Anwendungen und Desktops verwenden, richten Sie nach der Installation der Komponenten beim Erstellen einer Site die erste Verbindung mit diesem Host ein. Sie können die Virtualisierungsumgebung allerdings schon vorher konfigurieren. Konsultieren Sie dabei die hier aufgeführten Informationsquellen.
- Wenn Sie Microsoft System Center Configuration Manager zum Verwalten des Zugriffs auf Anwendungen und Desktops verwenden, lesen Sie diesen Artikel.
- Der Artikel Datenbanken enthält Informationen über die Systemdatenbanken und deren Konfiguration. Während der Installation des Controllers können Sie wählen, ob Microsoft SQL Server 2012 Express auf demselben Server installiert werden soll. Das Gros der Datenbankinformationen konfigurieren Sie beim Erstellen einer Site, nachdem Sie die Kernkomponenten installiert haben.
- Wenn Sie den Citrix Lizenzserver installieren, wird das Benutzerkonto automatisch zum Volladministrator auf dem Lizenzserver. Weitere Informationen finden Sie im Artikel Delegierte Administration.
- Beim Erstellen von Objekten vor, während und nach der Installation müssen Sie eindeutige Namen für jedes Objekt (Netzwerke, Gruppen, Kataloge und Ressourcen) eingeben.
- Bei Installationsproblemen wird der Prozess angehalten und eine Fehlermeldung angezeigt. Komponenten, die erfolgreich installiert werden, bleiben gespeichert; sie müssen nicht neu installiert werden.
- Citrix Studio wird nach dem Abschluss der Installation automatisch gestartet. Bei Verwendung der grafischen Oberfläche können Sie diese Aktion auf der letzten Seite des Assistenten deaktivieren.
- Sie können die Kernkomponenten und Virtual Delivery Agents (VDAs) mit dem im Produkt-ISO-Image enthaltenen Installationsprogramm (dem "Produktinstallationsprogramm") installieren. Zum Installieren von VDAs können Sie neben dem Produktinstallationsprogramm auch das eigenständige VDA-Installationsprogramm verwenden. Letzteres kann von der Produkt-Downloadseite im Internet heruntergeladen werden. Beide Programme bieten eine grafische Oberfläche und eine Befehlszeilenschnittstelle.
- Das Produktinstallationsmedium enthält Beispielskripts, um VDAs für Gruppen von Maschinen in Active Directory zu installieren, zu aktualisieren oder zu entfernen. Sie können die Skripts auch auf einzelne Maschinen anwenden und sie zum Verwalten von Masterimages einsetzen, die von den Maschinenerstellungsdiensten und Provisioning Services verwendet werden. Weitere Informationen finden Sie im Artikel Installieren von VDAs mit Skripts.
- Die Serverkomponente (UpsServer) des universellen Druckserver können Sie mit der grafischen Oberfläche oder der Befehlszeilenschnittstelle des Produktinstallationsprogramms auf den Druckservern installieren. Die Produktdownloadseite im Internet enthält ggf. UpsServer-Pakete zum Herunterladen.
- Citrix Receiver für Mac und Citrix Receiver für Linux sind nicht mehr im Produkt-ISO-Image enthalten. Sie oder die Benutzer können diese Citrix Receiver-Versionen von der Citrix Website herunterladen und installieren. Alternativ können Sie diese Citrix Receiver-Versionen auf dem StoreFront-Server zur Verfügung stellen. Informationen hierzu finden Sie im Abschnitt Verfügbarmachen von Citrix Receiver-Installationsdateien auf dem Server in der Dokumentation zu StoreFront 3.0.x bzw. in der Dokumentation zu der von Ihnen verwendeten StoreFront-Version.

Auf den Maschinen, auf denen Sie die Komponenten installieren, müssen Sie Domänenbenutzer und lokaler Administrator sein.

Für die Installation mit dem eigenständigen Installationsprogramm benötigen Sie erhöhte Administratorprivilegien oder verwenden Sie die Option **Als Administrator ausführen**.

Konfigurieren Sie die Active Directory-Domäne vor Beginn der Installation.

- Der Artikel Systemanforderungen enthält eine Liste der unterstützten Active Directory-Funktionsebenen. Der Artikel Active Directory enthält zusätzliche Informationen zu unterstützten Elementen.
- Sie müssen mindestens einen Domänencontroller mit Active Directory-Domänendiensten ausführen.
- Versuchen Sie nicht, Komponenten auf einem Domänencontroller zu installieren.
- Verwenden Sie keinen Schrägstrich (/), wenn Sie in Studio Namen für Organisationseinheiten festlegen.
- Weitere Informationen finden Sie in der Dokumentation von Microsoft zur Konfiguration von Active Directory.

Legen Sie fest, wo die Komponenten installiert werden, und bereiten Sie die Maschinen und Betriebssysteme vor.

- Der Artikel Systemanforderungen enthält Informationen über die unterstützten Betriebssysteme und Versionen für Controller, Studio, Citrix Director, Virtualisierungsressourcen (Hosts) und VDAs. Die meisten Komponentenvoraussetzungen werden automatisch installiert. Ausnahmen werden in dem Artikel aufgeführt. In den Dokumenten zu Citrix StoreFront und Citrix Lizenzserver finden Sie Angaben zu den unterstützten Plattformen.
- Sie können die Kernkomponenten auf dem gleichen Server oder auf unterschiedlichen Servern installieren. Um beispielsweise eine kleinere Bereitstellung remote zu verwalten, können Sie Studio auf einer anderen Maschine installieren als den Server, auf dem der Controller installiert wurde. Um zukünftige Erweiterungen zu ermöglichen, sollten Sie die Komponenten auf verschiedenen Servern installieren, z. B. den Lizenzserver und Director auf unterschiedlichen Servern.
- Sie können den Delivery Controller und den Virtual Delivery Agent für Windows-Serverbetriebssysteme auf demselben Server installieren. Starten Sie hierfür das Installationsprogramm und wählen Sie den Delivery Controller (sowie alle weiteren Kernkomponenten für diese Maschine). Starten Sie dann das Installationsprogramm erneut und wählen Sie den Virtual Delivery Agent für Windows-Serverbetriebssysteme.
- Installieren Sie keine Komponenten auf Domänencontrollern.
- Die Installation eines Controllers auf einem Knoten in einer SQL-Cluster- oder Spiegelungsinstallation oder auf einem Server mit Hyper-V wird nicht unterstützt.
- Installieren Sie Studio nicht auf einem Server, auf dem XenApp 6.5 Feature Pack 2 für Windows Server 2008 R2 oder eine frühere Version von XenApp ausgeführt wird.
- Stellen Sie sicher, dass für jedes Betriebssystem die neuesten Updates ausgeführt wurden.
- Stellen Sie sicher, dass bei allen Maschinen die Systemuhren synchronisiert sind. Die Synchronisierung wird für die Kerberos-Infrastruktur benötigt, die die Kommunikation zwischen den Maschinen sichert.

Angaben bei der Installation der Hauptkomponenten

In den folgenden Abschnitten werden die Parameter erläutert, die Sie bei der Installation festlegen. Die Beschreibung folgt den Schritten des Assistenten der grafischen Oberfläche; entsprechende Optionen für die Befehlszeilenschnittstelle werden ebenfalls aufgeführt. In den Artikeln zur Installation wird erläutert, wie Sie den Assistenten starten und Befehle mit Optionen eingeben.

Wählen Sie aus oder geben Sie an, ob Microsoft SQL Server Express installiert werden soll. Wenn Sie nicht mit den Datenbanken vertraut sind, lesen Sie den Artikel Datenbanken. (Befehlszeilenoption: /nosql zur Verhinderung der Installation)

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 und TCP-Port 3389 öffnen. Dieses Feature ist standardmäßig aktiviert. (Befehlszeilenoption: /no_remote_assistance)

Standardmäßig werden die folgenden Ports automatisch geöffnet, wenn der Windows-Firewalldienst ausgeführt wird, selbst wenn die Firewall nicht aktiviert ist. Sie können diese Standardaktion deaktivieren und die Ports manuell öffnen, wenn Sie die Firewall eines Drittanbieters oder keine Firewall verwenden, oder wenn Sie die Ports selbst öffnen möchten. Vollständige Portinformationen zu diesem und anderen Citrix Produkten finden Sie unter CTX101810. (Befehlszeilenoption: /configure_firewall)

- Controller: TCP 80, 443
- Director: TCP 80, 443
- Lizenzserver: TCP 7279, 8082, 8083, 27000
- StoreFront: TCP 80, 443

Leitfaden zur VDA-Installation

- Die VDA-Installationsprogramme bieten eine grafische Oberfläche und eine Befehlszeilenschnittstelle.
- Informationen zu den unterstützten Betriebssystemen und zu den VDA-Versionen enthält der Artikel Systemanforderungen. Die meisten Komponentenvoraussetzungen werden automatisch installiert. Ausnahmen werden in dem Artikel aufgeführt. Wenn Sie einen VDA für Windows-Serverbetriebssysteme installieren, werden die Rollendienste für die Remotedesktopdienste automatisch installiert und aktiviert, wenn sie nicht bereits installiert und aktiviert sind.
- Wenn Sie einen VDA auf einer Maschine mit Windows 7 oder Windows Server 2008 R2 installieren, vergewissern Sie sich vor der VDA-Installation, dass .NET 3.5.1 installiert ist. Der Abschnitt Neustarts unten enthält zusätzliche Tipps zu den Installationsvoraussetzungen.
- Der Druckspoolerdienst ist auf den unterstützten Windows-Servern standardmäßig aktiviert. Ist dieser Dienst deaktiviert, können Sie keinen VDA für Windows-Serverbetriebssysteme installieren. Stellen Sie daher vor der VDA-Installation sicher, dass der Dienst aktiviert ist.
- Die Profilverwaltung wird automatisch bei der Installation von Virtual Desktop Agent installiert. Sie können sie zwar ausschließen, wenn Sie die Befehlszeilenschnittstelle verwenden, ein solcher Ausschluss wirkt sich jedoch auf Überwachung und Problembehandlung von VDAs mit Director aus.
- Wenn Sie VDA installieren, wird automatisch eine neue lokale Benutzergruppe namens "Benutzer mit direktem Zugriff" erstellt. Bei VDA für Windows-Desktopbetriebssysteme gilt diese Gruppe nur für RDP-Verbindungen; bei VDA für Windows-Serverbetriebssysteme gilt sie für ICA- und RDP-Verbindungen.
- Für Remote-PC-Zugriff-Konfigurationen ist VDA für Windows-Desktopbetriebssystem auf jedem physischen Büro-PC zu installieren, auf den die Benutzer zugreifen. Aktivieren Sie das Feature zum Optimieren nicht.
- Wenn Sie einen VDA auf einem Computer mit einem unterstützten Linux- Betriebssystem installieren möchten, konsultieren Sie den Artikel Installieren von VDAs unter Red Hat Linux bzw. Installieren von VDAs unter SUSE Linux. Diese enthalten wichtige Informationen.

Sie können VDAs über das Produktinstallationsprogramm oder das eigenständige Installationsprogramm installieren. Beide bieten eine grafische Oberfläche und eine Befehlszeilenschnittstelle.

Das Produktinstallationsprogramm erkennt automatisch das Betriebssystem und erlaubt nur die Installation des für das System geeigneten Windows-VDA: VDA für Windows-Serverbetriebssysteme oder VDA für Windows-Desktopbetriebssysteme.

Eigenständiges VDA-Installationspaket

Das kleinere, eigenständige Paket ist besser für Bereitstellungen auf physischen Computern oder an Remotestandorten geeignet, da es über Electronic Software Distribution (ESD)-Pakete als limitierte Bereitstellung oder lokale Kopie bereitgestellt wird. Das eigenständige Paket ist in erster Linie für Bereitstellungen über die Befehlszeile (unbeaufsichtigte Installation) gedacht, da die gleichen Befehlszeilenparameter wie beim Produktinstallationsprogramm verwendet werden. Das Paket bietet zudem dieselbe grafische Oberfläche wie das Produktinstallationsprogramm.

Verwenden der grafischen Oberfläche des eigenständigen VDA-Installationsprogramms

Verwenden der Befehlszeilenschnittstelle des eigenständigen VDA-Installationsprogramms

Es gibt zwei selbstextrahierende eigenständige VDA-Installationspakete: eines zur Installation auf unterstützten Serverbetriebssystemmaschinen und eines für unterstützte Workstation- bzw. Desktopbetriebssystemmaschinen.

Standardmäßig werden die Dateien im Paket in den Ordner "Temp" extrahiert. Zum Extrahieren in den Ordner "Temp" wird auf der Maschine mehr Speicherplatz beansprucht, als wenn Sie das Produktinstallationsprogramm verwenden. Dateien, die in den Ordner "Temp" extrahiert wurden, werden nicht automatisch gelöscht, aber Sie können sie nach Abschluss der Installation manuell löschen (aus C:\Windows\Temp\Ctx-*, wobei * ein willkürlicher GUID ist). Alternativ können Sie den Befehl /extract mit einem absoluten Pfad verwenden.

Wenn in der Bereitstellung Microsoft System Center Configuration Manager verwendet wird, schlägt eine VDA-Installation u. U. scheinbar mit Exitcode 3 fehl, obwohl der VDA erfolgreich installiert wird. Sie können diese irreführende Meldung vermeiden, indem Sie die Installation mit einem CMD-Script umschließen oder die Erfolgscodes im Configuration Manager-Paket ändern. Weitere Informationen finden Sie in der Forumsdiskussion http://discussions.citrix.com/topic/350000-sccm-install-of-vda-71-fails-with-exit-code-3/.

Bei der VDA-Installation ist zum Abschluss ein Neustart erforderlich.

Wenn Sie die Zahl der Neustarts während der Installation auf ein Minimum begrenzen möchten, gehen Sie folgendermaßen vor:

- Stellen Sie vor der VDA-Installation sicher, dass eine unterstützte .NET Framework-Version installiert ist.
- Installieren und aktivieren Sie auf Windows-Serverbetriebssystemmaschinen vor der VDA-Installation die Rollendienste für Remotedesktopdienste.

Andere Voraussetzungen erfordern normalerweise keine Neustarts, daher können Sie das Installationsprogramm einfach laufen lassen.

Wenn Sie vor der VDA-Installation nicht die Voraussetzungen installieren und dann die Option /noreboot für die Befehlszeileninstallation festlegen, müssen Sie die Neustarts ausführen. Wenn Sie beispielsweise die Voraussetzungen automatisch bereitstellen, wartet das Installationsprogramm nach der Installation von RDS auf einen Neustart. Führen Sie nach dem Neustart den Befehl erneut aus, damit die Installation des VDAs fortgesetzt wird.

Die aktuellen VDAs werden unter Windows XP und Windows Vista nicht unterstützt. Außerdem können einige Features in diesem und anderen neueren Releases unter diesen Betriebssystemen nicht verwendet werden. Citrix empfiehlt, die Sie solche Systeme durch derzeit unterstützte Windows-Desktopbetriebssystemversionen ersetzen und dann einen VDA aus diesem Release installieren. Wenn Maschinen mit Windows XP oder Windows Vista weiter betrieben werden müssen, können Sie auch eine ältere Virtual Desktop Agent-Version (5.6 FP1 mit bestimmten Hotfixes) installieren. Einzelheiten hierzu finden Sie unter CTX140941. Beachten Sie Folgendes:

- Die Kernkomponenten (Controller, Studio Director, StoreFront, Lizenzserver) können nicht auf einem Windows XP- oder Windows Vista-System installiert werden.
- Remote-PC-Zugriff wird auf Windows Vista-Systemen nicht unterstützt.
- Citrix Support für Windows XP endete zusammen mit dem erweiterten Support von Microsoft am 8. April 2014.
- Die Verwendung älterer VDAs kann sich auf die Verfügbarkeit von Features und die Registrierung des VDAs beim Controller auswirken (siehe auch Hinweise zu heterogenen Umgebungen).

Angaben bei der VDA-Installation

In den folgenden Abschnitten werden die Parameter erläutert, die Sie bei der Installation festlegen. Die Beschreibung folgt den Schritten des Assistenten der grafischen Oberfläche; entsprechende Optionen für die Befehlszeilenschnittstelle werden ebenfalls aufgeführt. In den Artikeln zur Installation wird erläutert, wie Sie den Assistenten starten bzw. Befehle mit Optionen eingeben.

Die VDA-Umgebung gibt vor, wie der VDA verwendet wird:

- Die Standardoption "Masterimage" gibt an, dass Sie mit den Maschinenerstellungsdiensten (MCS) oder Provisioning Services virtuelle Maschinen basierend auf einem Masterimage in einem Hypervisor oder Clouddienst erstellen. Sie installieren den VDA auf dem Masterimage. (Befehlszeilenoption /masterimage)
- Die Option "Remote-PC-Zugriff" gibt an, dass Sie den VDA auf einer physischen Maschine oder auf einer VM ohne VDA installieren.

Wenn Sie einen VDA für Windows-Desktopbetriebssysteme installieren, können die Standardversion oder die HDX 3D Pro-Version des VDA auswählen.

- Die Standardversion wird für die meisten Desktops empfohlen, einschließlich solcher mit aktiviertem Microsoft RemoteFX. Diese Version wird standardmäßig installiert.
- Der VDA für HDX 3D Pro dient zur Optimierung der Leistung grafikintensiver Programme und Anwendungen und solcher mit hohem Multimedia-Anteil. Er wird empfohlen, wenn die Maschine zur 3D-Wiedergabe auf einen Grafikprozessor zugreift. (Befehlszeilenoption /enable_hdx_3d_pro)

Komponenten werden standardmäßig unter C:\Programme\Citrix installiert. Sie können einen anderen Speicherort während der Installation angeben. Stellen Sie jedoch sicher, dass dieser Speicherort den Netzwerkdienst ausführen kann. (Befehlszeilenoption: /installdir zum Festlegen eines nicht standardmäßigen Verzeichnisses)

Standardmäßig wird Citrix Receiver für Windows mit dem VDA installiert. Sie können diese Standardaktion deaktivieren.

(Befehlszeilenoption: /components vda, um die Installation von Citrix Receiver zu verhindern)

Sie können die Adressen (FQDNs) der installierten Controller bei der Installation des VDAs festlegen (empfohlen) oder zu einem späteren Zeitpunkt. Sie müssen zwar keine Controlleradressen bei der Installation eines VDAs angeben, ein VDA kann sich jedoch ohne diese Angabe nicht bei einem Controller registrieren. Wenn VDAs sich nicht registrieren können, können Benutzer auf Maschinen mit diesen VDAs nicht auf ihre Desktops und Anwendungen zugreifen. (Befehlszeilenoption: /controllers)

- Wenn Sie Controller-FQDNs bei der VDA-Installation angeben, wird versucht, eine Verbindung mit diesen Adressen herzustellen. Schlägt dies fehl, werden Informationsmeldungen angezeigt.
- Wenn Sie angeben, dass Sie Controlleradressen später festlegen möchten, werden Sie vom Installationsprogramm entsprechend erinnert. Wenn Sie einen VDA ohne Angabe einer Controlleradresse installieren, können Sie entweder das Installationsprogramm zu einem späteren Zeitpunkt erneut ausführen oder die Citrix Gruppenrichtlinie verwenden.

Wenn Sie Controlleradressen bei der VDA-Installation und in der Gruppenrichtlinie festlegen, haben die Richtlinieneinstellungen Vorrang vor den bei der Installation festgelegten Einstellungen.

Vergessen Sie nicht, dass zur VDA-Registrierung außerdem die Firewallports für die Kommunikation mit einem Controller geöffnet sein müssen.

Nach der ersten Angabe von Controlleradressen bei der VDA-Installation oder zu einem späteren Zeitpunkt können Sie das Feature für automatische Updates zum Aktualisieren von VDAs verwenden, wenn weitere Controller installiert werden.

Weitere Informationen dazu, wie VDAs Controller erkennen und sich dort registrieren, finden Sie im Artikel Delivery Controller.

Sie können folgende Features für VDAs aktivieren oder deaktivieren:

- **Leistung optimieren:** Wenn diese Funktion aktiviert ist, wird das Optimierungstool für VDAs verwendet, die auf einer VM auf einem Hypervisor ausgeführt werden. Die VM-Optimierung umfasst das Deaktivieren von Offlinedateien, das Deaktivieren der Hintergrunddefragmentierung und die Verkleinerung der Ereignisprotokollgröße. Weitere Informationen finden Sie unter CTX125874. Aktivieren Sie diese Option nicht, wenn Sie Remote-PC-Zugriff verwenden möchten. (Befehlszeilenoption: /optimize)
- **Microsoft-Remoteunterstützung:** Wenn dieses Feature aktiviert ist, wird die Microsoft-Remoteunterstützung mit dem Feature zur Benutzerspiegelung von Director verwendet, und Windows öffnet automatisch TCP-Port 3389 in der Firewall, selbst wenn Sie die Firewallports normalerweise manuell öffnen. Die Funktion ist standardmäßig aktiviert. (Befehlszeilenoption: /enable_remote_assistance)
- **Echtzeitaudioübertragung für Audio:** Wenn diese Funktion aktiviert ist, wird UDP für Audiopakete verwendet, wodurch die Audioleistung verbessert werden kann. Die Funktion ist standardmäßig aktiviert. (Befehlszeilenoption: /enable_real_time_transport)
- **Personal vDisk:** Wenn dieses Feature aktiviert ist, können persönliche vDisks mit einem Masterimage verwendet werden. Die Funktion ist standardmäßig deaktiviert und steht bei Installation eines VDAs für Windows-Desktopbetriebssysteme auf einer VM zur Verfügung. Weitere Informationen finden Sie im Artikel Personal vDisks. (Befehlszeilenoption: /baseimage)

Standardmäßig werden die folgenden Ports automatisch geöffnet, wenn der Windows-Firewalldienst ausgeführt wird, selbst wenn die Firewall nicht aktiviert ist. Sie können diese Standardaktion deaktivieren und die Ports manuell öffnen, wenn Sie die Firewall eines Drittanbieters oder keine Firewall verwenden, oder wenn Sie die Ports selbst öffnen möchten. Vollständige Portinformationen finden Sie unter CTX101810. (Befehlszeilenoption: /enable_hdx_ports)

- Controller: TCP 80, 1494, 2598, 8008

  Für die Kommunikation zwischen Benutzergeräten und virtuellen Desktops müssen Sie eingehendes TCP auf Ports 1494 und 2598 als Portausnahmen konfigurieren. Aus Sicherheitsgründen empfiehlt Citrix, diese registrierten Ports ausschließlich für das ICA-Protokoll und das Common Gateway Protocol zu verwenden.

  Für die Kommunikation zwischen Controller und virtuellen Desktops müssen Sie den eingehenden Port 80 als Portausnahme konfigurieren.

- Windows-Remoteunterstützung: TCP 3389

  Wenn das Feature aktiviert ist, öffnet Windows diesen Port automatisch, selbst wenn Sie die Ports normalerweise manuell öffnen.

- Echtzeitaudioübertragung: UDP 16500-16509

VMware-Virtualisierungsumgebungen

Feb 29, 2016

Folgen Sie diesen Anweisungen, wenn Sie zur Bereitstellung von virtuellen Maschinen VMware verwenden.

1. Installieren Sie vCenter Server und die Verwaltungstools. (Der "Linked Mode"-Betrieb von vSphere vCenter wird nicht unterstützt.)
2. Erstellen Sie ein VMware-Benutzerkonto mit den folgenden Mindestberechtigungen auf DataCenter-Ebene. Dieses Konto verfügt über Berechtigungen zum Erstellen neuer VMs und wird verwendet, um mit vCenter zu kommunizieren.

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
System.Anonymous, System.Read und System.View	Automatisch hinzugefügt.
Task.Create	Tasks > Create task
VirtualMachine.Config.AddRemoveDevice	Virtual machine > Configuration > Add or remove device
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.CPUCount	Virtual machine > Configuration > Change CPU Count
VirtualMachine.Config.Memory	Virtual machine > Configuration > Memory

SDK	Benutzeroberfläche
VirtualMachine.Config.RemoveDisk	Virtual machine > Configuration > Remove disk
VirtualMachine.Config.Resource	Virtual machine > Configuration > Change resource
VirtualMachine.Config.Settings	Virtual machine > Configuration > Settings
VirtualMachine.Interact.PowerOff	Virtual machine > Interaction > Power Off
VirtualMachine.Interact.PowerOn	Virtual machine > Interaction > Power On
VirtualMachine.Interact.Reset	Virtual machine > Interaction > Reset
VirtualMachine.Interact.Suspend	Virtual machine > Interaction > Suspend
VirtualMachine.Inventory.Create	Virtual machine > Inventory > Create new
VirtualMachine.Inventory.CreateFromExisting	Virtual machine > Inventory > Create from existing
VirtualMachine.Inventory.Delete	Virtual machine > Inventory > Remove
VirtualMachine.Inventory.Register	Virtual machine > Inventory > Register
VirtualMachine.Provisioning.Clone	Virtual machine > Provisioning > Clone template
VirtualMachine.Provisioning.DiskRandomAccess	Virtual machine > Provisioning > Allow disk access
VirtualMachine.Provisioning.GetVmFiles	Virtual machine > Provisioning > Allow virtual machine download
VirtualMachine.Provisioning.PutVmFiles	Virtual machine > Provisioning > Allow virtual machine files upload
VirtualMachine.Provisioning.DeployTemplate	Virtual machine > Provisioning > Deploy template
VirtualMachine.Provisioning.MarkAsVM	Virtual machine > Provisioning > Mark as virtual machine
VirtualMachine.State.CreateSnapshot	vSphere 5.0, Update 2 und vSphere 5.1, Update 1: Virtual machine > State > Create snapshot vSphere 5.5: Virtual machine > Snapshot management > Create snapshot

SDK	Benutzeroberfläche
VirtualMachine.State.RemoveSnapshot	vSphere 5.0, Update 2 und vSphere 5.1, Update 1: Virtual machine > State > Remove snapshot vSphere 5.5: Virtual machine > Snapshot management > Remove snapshot
VirtualMachine.State.RevertToSnapshot	vSphere 5.0, Update 2 und vSphere 5.1, Update 1: Virtual machine > State > Revert to snapshot vSphere 5.5: Virtual machine > Snapshot management > Revert to snapshot

3. Wenn Sie die erstellten VMs mit Tags kennzeichnen wollen, fügen Sie die folgenden Berechtigungen dem Benutzerkonto hinzu:

SDK	Benutzeroberfläche
Global.ManageCustomFields	Global > Manage custom attributes
Global.SetCustomField	Global > Set custom attribute

Um sicherzustellen, dass Sie ein sauberes Basisimage zum Erstellen neuer VMs verwenden, fügen Sie Tags den VMs hinzu, die mit den Maschinenerstellungsdiensten erstellt wurden. Damit schließen Sie sie aus der Liste der für Basisimages verfügbaren virtuellen Maschinen aus.

Um die vSphere-Kommunikation zu schützen, empfiehlt Citrix die Verwendung von HTTPS statt HTTP. HTTPS benötigt digitale Zertifikate. Citrix empfiehlt die Verwendung eines digitalen Zertifikats, das von einer Zertifizierungsstelle unter Berücksichtigung der Sicherheitsrichtlinie Ihrer Organisation erstellt wurde.

Wenn Sie kein digitales Zertifikat verwenden können, das von einer Zertifizierungsstelle ausgestellt wurde, können Sie das mit VMware installierte selbstsignierte Zertifikat verwenden, vorausgesetzt, die Sicherheitsrichtlinie Ihrer Organisation lässt dies zu. Fügen Sie das VMware vCenter-Zertifikat jedem Controller hinzu. Führen Sie diese Schritte aus:

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 Methoden ab:
   - Führen Sie auf dem vCenter-Server folgende Schritte aus:
     1. Kopieren Sie die Datei rui.crt vom vCenter-Server zu einem Speicherort, auf den Ihre Delivery Controller zugreifen können.
     2. Navigieren Sie auf dem Controller zu dem Speicherort des exportierten Zertifikats und öffnen Sie die Datei rui.crt.
   - Laden Sie das Zertifikat über einen Webbrowser herunter. Bei Verwendung von Internet Explorer müssen Sie (abhängig von Ihrem Benutzerkonto) ggf. in Internet Explorer mit der rechten Maustaste klicken und "Als Administrator ausführen" wählen, um das Zertifikat herunterzuladen und zu installieren.

1. Öffnen Sie einen Webbrowser und stellen Sie eine sichere Webverbindung zu dem vCenter-Server her, z. B. https://server1.domain1.com
2. Akzeptieren Sie die Sicherheitswarnungen.
3. Klicken Sie auf die Adressleiste, in der der Zertifikatfehler angezeigt wird.
4. Zeigen Sie das Zertifikat an und klicken Sie auf die Registerkarte Details.
5. Wählen Sie In Datei kopieren und exportieren Sie im CER-Format; geben Sie an entsprechender Stelle einen Namen an.
6. Speichern Sie das exportierte Zertifikat.
7. Navigieren Sie auf den Speicherort des exportierten Zertifikats und öffnen Sie die CER-Datei.

- Direkter Import von Internet Explorer, der als Administrator ausgeführt wird:
  1. Öffnen Sie einen Webbrowser und stellen Sie eine sichere Webverbindung mit dem vCenter-Server her, z. B. https://server1.domain1.com.
  2. Akzeptieren Sie die Sicherheitswarnungen.
  3. Klicken Sie auf die Adressleiste, in der der Zertifikatfehler angezeigt wird.
  4. Zeigen Sie das Zertifikat an.
- Importieren des Zertifikats auf jedem Controller in den Zertifikatspeicher:
  1. Klicken Sie auf Zertifikat installieren, wählen Sie Lokaler Computer aus und klicken Sie dann auf Weiter.
  2. Wählen Sie Alle Zertifikate in folgendem Speicher speichern aus und klicken Sie dann auf Durchsuchen.
  3. Bei Verwendung von Windows Server 2008 R2:
     1. Aktivieren Sie das Kontrollkästchen Physischen Speicher anzeigen.
     2. Erweitern Sie Vertrauenswürdige Personen.
     3. Wählen Sie Lokaler Computer.
     4. Klicken Sie auf Weiter und dann auf Fertig stellen.

     Bei Verwendung von Windows Server 2012 oder Windows Server 2012 R2:
     1. Wählen Sie Vertrauenswürdige Personen und klicken Sie auf OK.
     2. Klicken Sie auf Weiter und dann auf Fertig stellen.

  Wichtig: Wenn Sie den Namen des vSphere-Servers nach der Installation ändern, müssen Sie ein neues selbstsigniertes Zertifikat auf diesem Server erstellen, bevor Sie das neue Zertifikat importieren.

Verwenden Sie eine Master-VM zur Bereitstellung von Benutzerdesktops und Anwendungen. 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 Sicherungskopie zu verwenden.

Wenn Sie VM mit Studio erstellen statt einen vorhandenen Maschinenkatalog auszuwählen, geben Sie beim Einrichten der Hostinginfrastruktur für die Erstellung virtueller Desktops die folgenden Informationen ein:

1. Wählen Sie den VMware vSphere-Hosttyp aus.
2. Geben Sie die Adresse des Zugriffspunkts für das vCenter SDK ein.
3. Geben Sie die Anmeldeinformationen für das zuvor eingerichtete VMware-Konto ein, das Berechtigungen zum Erstellen neuer VMs hat. Geben Sie den Benutzernamen im Format Domäne/Benutzername ein.

Microsoft System Center Virtual Machine Manager-Umgebungen

Feb 29, 2016

Befolgen Sie die nachfolgenden Anweisungen, wenn Sie Hyper-V mit Microsoft System Center Virtual Machine Manager (VMM) zur Bereitstellung von virtuellen Maschinen verwenden.

Dieses Release unterstützt Folgendes:

- VMM 2012: Bietet bessere Verwaltungsfunktionen und ermöglicht die Verwaltung des gesamten virtualisierten Datencenters sowie der virtuellen Maschinen. Dieses Release organisiert das Patchen von Clusterhosts sowie die Integration mit Windows Server Update Services und ermöglicht somit das Erstellen eines Basisplans für Patches, die jeder Host benötigt.
- VMM 2012 SP1: Bietet Leistungsverbesserungen für Maschinenerstellungsdienste (MCS), wenn Sie SMB 3.0 auf Dateiservern mit freigegebenen Clustervolumes und Storage Area Networks (SANs) verwenden. Diese Dateifreigaben bieten kostengünstiges Zwischenspeichern und reduzierte E/A im SAN-Speicher mit verbesserter Leistung.
- VMM 2012 R2: Ermöglicht die angemessene Verwaltung von wichtigen Windows Server 2012 R2-Funktionen, wie das Ausführen von VM-Snapshots, dynamische VHDX-Größenanpassung und Speicherplätze.

Dieses Release unterstützt nur virtuelle Maschinen der ersten Generation mit VMM 2012 R2. Virtuelle Maschinen der zweiten Generation werden weder für Bereitstellungen mit Maschinenerstellungsdiensten (MCS) noch mit Provisioning Services unterstützt. Mit MCS oder Provisioning Services erstellte VM der zweiten Generation erscheinen nicht in der Auswahlliste für eine Master-VM. Auf ihnen ist der sichere Start standardmäßig aktiviert, wodurch eine richtige Funktionsweise des VDAs verhindert wird.

- Upgrade von VMM 2012 auf VMM 2012 SP1 oder VMM 2012 R2
  Informationen zu den Anforderungen von VMM- und Hyper-V-Hosts finden Sie unter http://technet.microsoft.com/en-us/library/gg610649.aspx. Informationen zu den Anforderungen für die VMM-Konsole finden Sie unter http://technet.microsoft.com/en-us/library/gg610640.aspx.

  Ein gemischter Hyper-V-Cluster wird nicht unterstützt. Ein gemischter Cluster ist beispielsweise einer, bei dem eine Hälfte des Clusters Hyper-V 2008 und die andere Hälfte Hyper-V 2012 ausführen.

- Upgrade von VMM 2008 R2 auf VMM 2012 SP1
  Wenn Sie ein Upgrade von XenDesktop 5.6 unter VMM 2008 R2 ausführen, halten Sie folgende Reihenfolge ein, um die Ausfallzeit von XenDesktop möglichst kurz zu halten:
  1. Upgrade von VMM auf 2012 (jetzt XenDesktop 5,6 und VMM 2012)
  2. Upgrade von XenDesktop auf die aktuelle Version (jetzt aktuelle XenDesktop-Version und VMM 2012)
  3. Upgrade von VMM von 2012 auf 2012 SP1 (jetzt aktuelle XenDesktop-Version und VMM 2012 SP1)
- Upgrade von VMM 2012 SP1 auf VMM 2012 R2
  Wenn Sie ein Upgrade von XenDesktop oder XenApp 7 unter VMM 2012 SP1 ausführen, halten Sie folgende Reihenfolge ein, um die Ausfallzeit von XenDesktop möglichst kurz zu halten:
  1. Upgrade von XenDesktop oder XenApp auf die aktuelle Version (jetzt aktuelle XenDesktop-/XenApp-Version und VMM 2012 SP1)
  2. Upgrade von VMM 2012 SP1 auf 2012 R2 (jetzt aktuelle XenDesktop- oder XenApp-Version und VMM 2012 R2)

1. Installieren und konfigurieren Sie einen Hypervisor.
   1. Installieren Sie Microsoft Hyper-V Server und VMM auf Ihren Servern. Alle Delivery Controller müssen in derselben Gesamtstruktur sein wie die VMM-Server.
   2. Installieren Sie die System Center VMM-Konsole auf allen Controllern.
   3. Überprüfen Sie die folgenden Kontoinformationen:
      - Das Konto, das Sie zum Festlegen von Hosts in Studio verwenden, ist ein VMM-Administrator oder delegierter VMM-Administrator für die relevanten Hyper-V-Maschinen. Wenn dieses Konto nur über die delegierte Administratorrolle in VMM verfügt, werden die Speicherdaten in Studio beim Erstellen des Hosts nicht aufgeführt.
      - Das Benutzerkonto, das für die Studio-Integration verwendet wird, muss auch Mitglied der lokalen Administratorsicherheitsgruppe auf

jedem Hyper-V-Server sein, um zur Lebenszyklusverwaltung von VM (z. B. VM erstellen, aktualisieren und löschen) berechtigt zu sein.

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

2. Erstellen Sie eine Master-VM.
   1. Installieren Sie einen Virtual Delivery Agent auf der Master-VM und wählen Sie die Option zur Desktopoptimierung aus. Dies verbessert die Leistung.
   2. Erstellen Sie einen Snapshot der Master-VM, um diesen als Sicherungskopie zu verwenden.
3. Erstellen Sie virtuelle Desktops. Bei Verwendung von MCS zum Erstellen von VM beim Erstellen einer Site oder einer Verbindung:
   1. Wählen Sie den Typ des Microsoft-Virtualisierungshosts aus.
   2. Geben Sie die Adresse als vollqualifizierten Domänennamen des Hostservers ein.
   3. Geben Sie die Anmeldeinformationen für das zuvor erstellte Administratorkonto ein, das Berechtigungen zum Erstellen von neuen VMs enthält.
   4. Wählen Sie im Dialogfeld Hostdetails den Cluster oder eigenständigen Host aus, der beim Erstellen der neuen VMs verwendet werden soll. Wichtig: Sie müssen auch dann zu einem Cluster oder eigenständigen Host navigieren und diesen auswählen, wenn Sie eine Bereitstellung mit einem einzelnen Hyper-V-Host verwenden.

Bei Maschinenkatalogen, die mit MSC auf SMB 3-Dateifreigaben für VM-Speicher erstellt wurden, müssen Sie darauf achten, dass die Anmeldeinformationen die nachfolgenden Anforderungen erfüllen, damit Aufrufe von der Hypervisor Communications Library (HCL) des Controllers die Verbindung mit dem SMB-Speicher herstellen:

- Die VMM-Benutzeranmeldeinformationen müssen vollständigen Lese-/Schreibzugriff auf den SMB-Speicher umfassen.
- Speichervorgänge auf dem virtuellen Datenträger werden bei Vorgängen im Lebenszyklus der VM über den Hyper-V-Server mit den VMM-Anmeldeinformationen durchgeführt.

Wenn Sie SMB als Speicher verwenden, aktivieren Sie das Feature "CredSSP" (Credential Security Support Provider) vom Controller auf den einzelnen Hyper-V-Maschinen, wenn Sie VMM 2012 SP1 mit Hyper-V unter Windows Server 2012 verwenden. Weitere Informationen finden Sie unter CTX137465.

Über eine standardmäßige Remote-PowerShell V3-Sitzung verwendet die HCL CredSSP zum Öffnen einer Verbindung mit der Hyper-V-Maschine. Dieses Feature übergibt mit Kerberos verschlüsselte Benutzeranmeldeinformationen an die Hyper-V-Maschine. Die PowerShell-Befehle in dieser Sitzung auf der Remotemaschine mit Hyper-V werden dann unter Verwendung der angegebenen Anmeldeinformationen (in diesem Fall, derer des VMM-Benutzers) ausgeführt, sodass eine ordnungsgemäße Kommunikation mit dem Speicher gewährleistet wird.

Die folgenden Tasks verwenden PowerShell-Skripts der HCL, die an die Hyper-V-Maschine zur Verwendung mit SMB 3.0-Speicher gesendet werden.

- **Konsolidieren des Masterimages**: Ein Masterimage erstellt ein neues MCS-Provisioningschema (Maschinenkatalog). Die Master-VM wird durch dieses Schema geklont und vereinfacht, damit sie zum Erstellen neuer VM aus dem neu erstellten Datenträger bereit ist (die Abhängigkeit zur ursprünglichen Master-VM wird entfernt).
  ConvertVirtualHardDisk im Namespace root\virtualization\v2

  Beispiel:
  $ims = Get-WmiObject -class $class -namespace "root\virtualization\v2"; $result = $ims.ConvertVirtualHardDisk($diskName, $vhdastext) $result
- **Erstellen eines differenzierenden Datenträgers**: erstellt einen differenzierenden Datenträger aus dem Masterimage, das durch Konsolidierung des Masterimages generiert wurde. Der differenzierende Datenträger wird dann an eine neue VM angeschlossen.
  CreateVirtualHardDisk im Namespace root\virtualization\v2

  Beispiel:
  $ims = Get-WmiObject -class $class -namespace "root\virtualization\v2"; $result = $ims.CreateVirtualHardDisk($vhdastext); $result
- **Upload von Identitätsdisks**: Von der HCL kann die Identitätsdisk nicht direkt in den SMB-Speicher hochgeladen werden. Daher muss die Identitätsdisk 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. Die Disk 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 Identitätsdisk-Upload durch die HCL auf die Hyper-V-Maschine abgeschlossen ist, werden die Identitätsdisks von der Remote-PowerShell-Sitzung in den SMB-Speicher kopiert und dann aus der Hyper-V-Maschine gelöscht.
   Falls der Ordner der Identitätsdisk gelöscht wird, wird er neu erstellt, damit er zur Wiederverwendung verfügbar ist.

- **Download von Identitätsdisks**: Wie beim Upload wird die Identitätsdisk über die Hyper-V-Maschine an die HCL übergeben. Beim folgenden Prozess wird, falls noch nicht vorhanden, ein Ordner erstellt, der nur VMM-Benutzerbenutzerberechtigungen auf dem Hyper-V-Server hat.
  1. Die Disk wird von der Hyper-V-Maschine aus dem SMB-Speicher in den lokalen Hyper-V-Speicher kopiert, und zwar über ein PowerShell-Skript, das in der Remote-PowerShell V3-Sitzung ausgeführt wird.
  2. Die HCL liest die Disk aus der Administratorfreigabe der Hyper-V-Maschine in den Speicher.
  3. Die HCL löscht die Datei aus der Administratorfreigabe.
- **Erstellen einer persönlichen vDisk**: Wenn der Administrator die VM in einem Personal vDisk-Maschinenkatalog erstellt, muss eine leere Disk (PvD) erstellt werden.
  Der Aufruf zum Erstellen einer leeren Disk erfordert keinen direkten Zugriff auf den Speicher. Wenn Sie PvDs auf anderen Speichern als dem Haupt- oder dem Betriebssystemdatenträger haben, verwenden Sie Remote-PowerShell zum Erstellen der PvD in einem Ordner mit dem gleichen Namen wie die VM, aus dem sie erstellt wurde. Verwenden Sie Remote-PowerShell nicht mit CSV oder LocalStorage. VMM-Befehlsfehler werden vermieden, wenn zuerst das Verzeichnis und dann die leere Disk erstellt werden.

  Führen Sie auf der Hyper-V-Maschine mkdir an dem Speicher aus.

Microsoft Azure-Virtualisierungsumgebungen

Feb 29, 2016

Verbindungskonfiguration

Wenn Sie Studio zum Erstellen einer Microsoft Azure-Verbindung verwenden, benötigen Sie Informationen aus der Datei mit den Veröffentlichungseinstellungen von Microsoft Azure. Die Informationen in dieser XML-Datei für die einzelnen Abonnements sehen in etwa folgendermaßen aus (das tatsächliche Verwaltungszertifikat ist viel länger):

```
ServiceManagementUrl="https://management.core.windows.net"
Id="o1455234-0r10-nb93-at53-21zx6b87aabb7p"
Name="Test1"
ManagementCertificate=";alkjdflaksdjfl;akjsdfl;akjsdfl; sdjfklasdfilaskjdfkluqweiopruaiopdfaklsdjfjsdilfasdkl;fjerioup" />
```

Bei dem folgenden Verfahren wird davon ausgegangen, dass Sie eine Verbindung mithilfe von Studio erstellen und entweder den Assistenten für die Siteerstellung oder den Assistenten für die Verbindungserstellung gestartet haben.

1. Rufen Sie in einem Browser https://manage.windowsazure.com/publishsettings/index auf.
2. Laden Sie die Datei mit den Veröffentlichungseinstellungen herunter.
3. Klicken Sie in Studio auf der Seite **Verbindung** des Assistenten nach Auswahl des Verbindungstyps "Microsoft Azure" auf "Importieren".
4. Wenn Sie mehrere Abonnements haben, werden Sie zur Auswahl des gewünschten Abonnements aufgefordert.

ID und Zertifikat werden automatisch und ohne Benutzereingriff in Studio importiert.

Energieaktionen, für die eine Verbindung verwendet wird, unterliegen Schwellenwerten. Im Allgemeinen sind die Standardwerte geeignet und sollten nicht geändert werden. Sie können sie jedoch beim Bearbeiten einer Verbindung ändern (beim Erstellen von Verbindungen können diese Werte nicht geändert werden). Weitere Informationen finden Sie unter Bearbeiten einer Verbindung.

Virtuelle Maschinen

Die Auswahl der Größe einzelner virtueller Maschine beim Erstellen eines Maschinenkatalogs in Studio hängt von den angezeigten Optionen, den Kosten und der Leistung des jeweiligen VM-Instanztyps und der Skalierbarkeit ab.

In Studio werden alle VM-Instanzoptionen angezeigt, die von Microsoft Azure in der jeweiligen Region angeboten werden. Diese Auswahl kann von Citrix nicht geändert werden. Daher sollten Sie mit Ihren Anwendungen und deren CPU-, Arbeitsspeicher- und E/A- Bedarf vertraut sein. Es stehen diverse Optionen zu verschiedenen Preis- und Leistungsstufen zur Auswahl. Einzelheiten zu den Optionen finden Sie in den nachfolgend aufgeführten Microsoft-Artikeln.

- Größen virtueller Computer und Cloud-Dienste für Azure: https://msdn.microsoft.com/en-us/library/azure/dn197896.aspx
- Virtual Machines – Preise: http://azure.microsoft.com/en-us/pricing/details/virtual-machines

Basic-VMs: VMs der Klasse "Basic" sind Basisfestplatten. Sie unterliegen primär der von Microsoft unterstützten IOPS-Stufe 300. Solche VMs werden für die Arbeitslast von Desktopbetriebssystemen (VDI) und Serverbetriebssystem-RDSHs

(Remotedesktop-Sitzungshost) nicht empfohlen.

Standard-VMs: VMs der Klasse "Standard" sind in vier Reihen eingeteilt: A, B, DS und G

Reihe	Anzeige in Studio
A	Sehr klein, klein, mittel, groß, sehr groß, A5, A6, A7, A8, A9, A10, A11. Mittel und Groß werden für Tests mit Arbeitslasten der Kategorie Desktopbetriebssystem (VDI) oder Serverbetriebssystem-RDSH empfohlen.
D	Standard_D1, D2, D3, D4, D11, D12, D13, D14. Diese VMs bieten SSDs für die temporäre Speicherung.
DS	Standard_DS1, DS2, DS3, DS4, DS11, DS12, DS13, DS14. Diese VMs bieten einen lokalen SSD-Speicher für alle Datenträger.
G	Standard_G1 – G5. Diese VMs sind für High Performance Computing geeignet.

Die US-Listenpreise der einzelnen VM-Instanztypen pro Stunde sind auf http://azure.microsoft.com/en-us/pricing/details/virtual-machines/ aufgeführt.

Bei der Arbeit mit Cloudumgebungen spielen die tatsächlichen Computing-Anforderungen eine wichtige Rolle. Für Machbarkeitsstudien oder anderen Tests werden gerne Hochleistungs-Instanztypen verwendet. Zur Einsparung von Kosten kann es hingegen verlockend sein, die VMs mit der niedrigsten Leistung zu wählen. Allerdings sollte idealerweise die für die jeweilige Aufgabe am besten geeignete VM verwendet werden. Die VMs der höchsten Leistungsklasse erzielen möglicherweise nicht das gewünschte Ergebnis und werden mit der Zeit sehr teuer – manchmal schon innerhalb einer Woche. Weniger teure VMs einer niedrigen Leistungsklasse sind der jeweiligen Aufgabe u. U. nicht gewachsen.

Tests mit Login VSI bei mittlerer Arbeitslast haben ergeben, dass für Desktopbetriebssysteme (VDI) und Serverbetriebssystem-RDSH Instanzen des Typs "Mittel" (A2) und "Groß" (A3) das beste Preis-/Leistungsverhältnis bieten.

Die Reihen Mittel (A2) und Groß (A3 oder A5) bieten das beste Preis-/Leistungsverhältnis für die Arbeitslastanalyse. Alles darunter wird nicht empfohlen. Leistungsfähigere VM-Reihen bieten ggf. die von Anwendungen und Benutzern geforderte Leistung und Benutzerfreundlichkeit. Es empfiehlt sich jedoch, die drei o. g. Instanztypen als Grundwert anzusetzen, um zu ermitteln, ob die höheren Kosten einer leistungsstärkeren VM einen echten Mehrwert bringen.

Die Skalierbarkeit von Katalogen in einer Hostingeinheit unterliegt einigen Schranken. Einige davon, z. B. die Zahl der CPU-Kerne des Azure-Abonnements, können ausgeräumt werden, indem beim Support von Microsoft Azure eine Erhöhung des Standardwerts (20) angefordert wird. Andere, etwa die Zahl der VMs in einem virtuellen Netzwerk pro Abonnement (2048), können nicht geändert werden.

Derzeit unterstützt Citrix 40 Maschinen pro Katalog.

Zur Erhöhung der Zahl der virtuellen Maschinen in einem Katalog oder Host wenden Sie sich an den Microsoft Azure-Support. Die Standardskalierungslimits von Microsoft Azure verhindern die Überschreitung einer bestimmten Zahl VMs. Diese

Limits ändern sich jedoch häufig. Die aktuellen Limits finden Sie unter http://azure.microsoft.com/en-us/documentation/articles/azure-subscription-service-limits/

Ein Microsoft Azure Virtual Network unterstützt bis zu 2048 VMs.

Microsoft empfiehlt ein Limit von 40 Standarddatenträger-VM-Images pro Clouddienst. Berücksichtigen Sie beim Skalieren die Zahl der Clouddienste, die für die VMs der gesamten Verbindung benötigt werden. Ziehen Sie darüber hinaus die VMs in Betracht, die für gehostete Anwendungen benötigt werden.

Wenden Sie sich an den Support von Microsoft Azure, um in Erfahrung zu bringen, ob die Standardzahl der CPU-Kerne für Ihre Arbeitslasten erhöht werden muss.

Microsoft System Center Configuration Manager-Umgebungen

Feb 29, 2016

Bei Sites, in denen der Zugriff auf Anwendungen und Desktops auf physischen Geräten mit System Center Configuration Manager (Configuration Manager) 2012 verwaltet wird, kann diese Verwendung über die Integrationsoptionen auf XenApp bzw. XenDesktop ausgeweitet werden.

- **Citrix Connector 7.5 für Configuration Manager 2012:** Citrix Connector bildet eine Brücke zwischen Configuration Manager und XenApp bzw. XenDesktop. Mit Citrix Connector können Sie alltägliche Vorgänge in den mit Configuration Manager verwalteten physischen Umgebungen und den mit XenApp bzw. XenDesktop verwalteten virtuellen Umgebungen übergreifend vereinheitlichen. Weitere Informationen zum Connector finden Sie unter Citrix Connector 7.5 für System Center Configuration Manager 2012.
- **Configuration Manager Wake Proxy-Feature:** Unabhängig davon, ob in der Umgebung Citrix Connector verwendet wird, wird für das Wake-On-LAN-Feature für den Remote-PC-Zugriff Configuration Manager benötigt. Weitere Informationen finden Sie weiter unten.
- **XenApp- und XenDesktop-Eigenschaften:** XenApp- und XenDesktop-Eigenschaften ermöglichen die Identifizierung virtueller Citrix Desktops für die Verwaltung durch Configuration Manager. Diese Eigenschaften werden automatisch von Citrix Connector verwendet, sie können aber auch manuell konfiguriert werden, wie im folgenden Abschnitt beschrieben.

Properties

Eigenschaften stehen Microsoft System Center Configuration Manager 2012 und 2012 R2 für die Verwaltung virtueller Desktops zur Verfügung.

Boolesche Eigenschaften in Configuration Manager 2012 können als 1 oder 0 statt True oder False angezeigt werden.

Die Eigenschaften stehen in der Klasse Citrix_virtualDesktopInfo im Namespace Root\Citrix\DesktopInformation zur Verfügung. Die Namen der Eigenschaften stammen vom Anbieter für Windows-Verwaltungsinstrumentation (WMI).

Eigenschaft	Beschreibung
AssignmentType	Legt den Wert auf IsAssigned fest. Gültige Werte: • ClientIP • ClientName • Keine • User: legt IsAssigned auf True fest.
BrokerSiteName	Site, gibt den gleichen Wert wie HostIdentifier zurück.
DesktopCatalogName	Dem Desktop zugewiesener Maschinenkatalog
DesktopGroupName	Dem Desktop zugewiesene Bereitstellungsgruppe
HostIdentifier	Site, gibt den gleichen Wert wie BrokerSiteName zurück.

Eigenschaft	Beschreibung
IsAssigned	True = ordnet den Desktop einem Benutzer zu; False = zufälliger Desktop.
IsMasterImage	Ermöglicht Entscheidungen bezüglich der Umgebung. Beispielsweise können Sie Anwendungen auf dem Masterimage und nicht auf den bereitgestellten Maschinen installieren, besonders dann, wenn diese Maschinen auf Bootmaschinen in einem fehlerfreien Zustand sind. Gültige Werte: • True auf einer VM, die als Masterimage verwendet wird (dieser Wert wird während der Installation basierend auf einer Auswahl festgelegt). • Cleared auf einer VM, die von diesem Image bereitgestellt wird.
IsVirtualMachine	True für eine virtuelle Maschine, False für eine physische Maschine
OSChangesPersist	False, wenn das Betriebssystemimage des Desktops bei jedem Neustart in einen fehlerfreien Zustand versetzt wird, andernfalls True
PersistentDataLocation	Der Speicherort, an dem Configuration Manager persistente Daten speichert. Benutzer haben hierauf keinen Zugriff.
PersonalvDiskDriveLetter	Bei einem Desktop mit einer persönlichen vDisk ist dies der Laufwerksbuchstabe, den Sie der persönlichen vDisk zuweisen.
BrokerSiteName, DesktopCatalogName, DesktopGroupName, HostIdentifier	Festgelegt, wenn der Desktop sich beim Controller registriert; bei Desktops, die noch nicht vollständig registriert sind, NULL

Zum Sammeln der Eigenschaften führen Sie eine Hardwareinventur in Configuration Manager durch. Zum Anzeigen der Eigenschaften verwenden Sie den Ressourcen-Explorer von Configuration Manager. In diesen Fällen können die Namen Leerzeichen enthalten oder vom Eigenschaftsnamen etwas abweichen. **BrokerSiteName** kann z. B. als "Broker Site Name" angezeigt werden. Weitere Informationen über die nachfolgend aufgeführten Aufgaben finden Sie unter http://support.citrix.com/article/ctx140905.

- Konfigurieren von Configuration Manager zum Sammeln von Citrix WMI-Eigenschaften vom Citrix VDA
- Erstellen abfragebasierter Gerätesammlungen mit Citrix WMI-Eigenschaften
- Erstellen globaler Bedingungen basierend auf Citrix WMI-Eigenschaften
- Verwenden globaler Bedingungen zum Definieren von Anforderungen für Anwendungsbereitstellungstypen

Sie können in der Microsoft-Klasse CCM_DesktopMachine im Namespace Root\ccm_vdi auch Microsoft-Eigenschaften verwenden. Weitere Informationen finden Sie in der Dokumentation von Microsoft.

Configuration Manager und Wake-On-LAN-Feature für den Remote-PC-Zugriff

Zum Konfigurieren des Wake-On-LAN-Features von Remote-PC-Zugriff führen Sie die folgenden Schritte aus, bevor Sie einen VDA auf den Büro-PCs installieren und mit Studio die Remote-PC-Zugriff-Bereitstellung erstellen oder aktualisieren:

- Konfigurieren Sie Configuration Manager 2012 im Unternehmen und stellen Sie dann den Configuration Manager-Client auf allen Remote-PC-Zugriff-Maschinen bereit. Warten Sie, bis der geplante SCCM-Bestandszyklus ausgeführt wurde (oder erzingen Sie manuell eine Ausführung). Die Zugriffsanmeldeinformationen, die Sie in Studio zum Konfigurieren der Verbindung mit Configuration Manager angeben, müssen Sammlungen im Geltungsbereich und die Rolle "Remotetoolsverantwortlicher" umfassen.
- Für die Unterstützung von Intel Active Management Technology (AMT) gilt Folgendes:
  - Die unterstützte Mindestversion auf dem PC ist AMT 3.2.1.
  - Stellen Sie den PC für die Verwendung von AMT mit Zertifikaten und zugehörigen Provisioningvorgängen bereit.
- Für die Unterstützung von Configuration Manager Wake-Proxy bzw. von Magic Packet:
  - Konfigurieren Sie Wake-On-LAN in den BIOS-Einstellungen aller PCs.
  - Zur Unterstützung von Configuration Manager Wake Proxy aktivieren Sie die entsprechende Option in Configuration Manager. Stellen Sie für jedes Subnetz des Unternehmens mit PCs, auf denen das Wake-On-LAN-Feature von Remote-PC-Zugriff verwendet wird, sicher, dass mindestens drei Maschinen als Sentinelmaschinen fungieren können.
  - Zur Unterstützung von Magic Packet konfigurieren Sie Netzwerkrouter und Firewalls so, dass Magic Packets entweder per subnetzgesteuertem Broadcast oder Unicast gesendet werden können.

Nach der Installation des VDAs auf Büro-PCs aktivieren oder deaktivieren Sie die Energieverwaltung beim Erstellen der Remote-PC-Zugriff-Bereitstellung in Studio.

- Wenn Sie die Energieverwaltung aktivieren, geben Sie Verbindungsdetails an, d. h. Adresse und Anmeldeinformationen von Configuration Manager sowie einen Namen.
- Wenn Sie die Energieverwaltung nicht aktivieren, können Sie eine Energieverwaltungsverbindung (Configuration Manager) später hinzufügen und dann einen Remote-PC-Zugriff-Maschinenkatalog zur Aktivierung der Energieverwaltung bearbeiten und die neue Energieverwaltungsverbindung angeben.

Sie können eine Energieverwaltungsverbindung bearbeiten, um die Verwendung von Configuration Manager Wake Proxy und Magic Packets zu konfigurieren und die Paketübertragungsmethode zu ändern.

Weitere Informationen finden Sie im Artikel Remote-PC-Zugriff.

Installieren über die grafische Oberfläche

Feb 29, 2016

Hinweis: Dieser Artikel gilt für die Installation von Komponenten auf Maschinen mit Windows-Betriebssystem. Informationen über die VDAs für Linux finden Sie unter VDAs unter Red Hat Linux sowie VDAs unter SUSE Linux.

Dieser Abschnitt enthält folgende Themen:

Einführung

Wichtig: Lesen Sie vor Beginn jeglicher Installation den Artikel Vorbereiten der Installation. Er enthält eine Beschreibung der Installationsprogramme und wichtige Informationen, mit denen Sie sich vor der Installation vertraut machen müssen. Er enthält zudem einen Leitfaden für die Elemente, die Sie im Assistenten festlegen müssen. In diesem Abschnitt wird beschrieben, wie Sie die grafische Oberfläche in einem Produktinstallationsprogramm starten.

Die grafische Oberfläche ermöglicht Folgendes:

- Installieren einer oder mehrerer der Kernkomponenten: Delivery Controller, Citrix Studio, Citrix Director, Lizenzserver und StoreFront.
- Installieren von Virtual Delivery Agent (VDA) auf einem Masterimage bzw. auf einer virtuellen oder physischen Maschine. Sie können auch die Skripts anpassen, die auf dem Medium sind, und sie zum Installieren und Entfernen von VDAs in Active Directory verwenden.
- Anpassen bereits installierter VDAs.
- Installieren eines universellen Druckservers. Der Controller hat bereits die Clientfunktionen des universellen Druckerservers; Sie müssen nur die Serverkomponente auf den Druckservern installieren. Nach der Installation der Komponente folgen Sie den Anweisungen im Artikel zum Konfigurieren von Druckern.
- Aktualisieren von Komponenten; Informationen hierzu finden Sie unter Upgrade einer Bereitstellung.

Das Produktinstallationsprogramm und das dedizierte VDA-Installationsprogramm haben beide eine grafische Benutzeroberfläche.

Verwenden des Produktinstallationsprogramms

Sie können Kernkomponenten, VDAs und die Komponenten des universellen Druckservers mit dem Produktinstallationsprogramm installieren.

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. Doppelklicken Sie auf **Automatische Auswahl**, wenn das Installationsprogramm nicht automatisch gestartet wird, oder klicken Sie auf das bereitgestellte

Laufwerk.

5. Wählen Sie aus, ob XenApp oder XenDesktop installiert werden soll.
6. Wählen Sie die Komponente aus, die Sie installieren möchten:

- Wenn Sie ganz zu Beginn der Installation stehen, wählen Sie in der linken Spalte **Delivery Controller**. Im Lauf der Installation mit dem Assistenten können Sie auswählen, welche Komponenten (Delivery Controller, Studio, Director, Lizenzserver und StoreFront) auf dem Computer, auf dem Sie das Installationsprogramm ausführen, installiert werden sollen.
- Wenn Sie bereits einige Komponenten installiert haben und Ihre Bereitstellung erweitern möchten, klicken Sie in der rechten Spalte auf die zu installierende Komponente. Diese Spalte enthält Kernkomponenten und den universellen Druckserver.
- Klicken Sie zum Installieren eines VDA auf den VDA-Eintrag in der mittleren Spalte. Es stehen nur die VDAs zur Verfügung, die für das Betriebssystem, unter dem Sie das Installationsprogramm ausführen, geeignet sind.

Folgen Sie die Anweisungen des Assistenten. Informationen zu den Elementen, die Sie im Assistenten sehen und konfigurieren, finden Sie unter Vorbereiten der Installation. Für die Installation eines VDA ist standardmäßig ein automatischer Neustart nach Installationsabschluss aktiviert; dieser ist erforderlich, bevor der VDA in einer Site verwendet werden kann.

Verwenden des dedizierten VDA-Installationsprogramms

Wichtig: Informationen zu Elementen der Installation mit dem dedizierten VDA-Installationsprogramm, insbesondere zu Neustarts und dem für die Extraktion benötigen Speicherplatz, finden Sie unter Vorbereiten der Installation.

Zum Zugriff auf die Downloadsite benötigen Sie Citrix Kontoanmeldeinformationen. Für die Installation benötigen Sie erhöhte Administratorprivilegien oder verwenden Sie die Option **Als Administrator ausführen**. Deaktivieren Sie die Benutzerkontensteuerung (UAC).

1. Laden Sie das benötigte Paket von Citrix herunter: **VDAServerSetup.exe** für Serverbetriebssystemmaschinen oder **VDAWorkstationSetup.exe** für Desktopbetriebssystemmaschinen Verwenden Sie für Einzelbenutzer-Einzelserverbereitstellungen (z. B. beim Bereitstellen von Windows Server 2012 für einen Benutzer zur Webentwicklung) das Paket VDAWorkstationSetup.exe. Weitere Informationen finden Sie im Artikel "Server-VDI".
2. Klicken Sie mit der rechten Maustaste auf das Paket und wählen Sie **Als Administrator ausführen**.
3. Folgen Sie die Anweisungen des Assistenten. Ein automatischer Neustart nach Installationsabschluss ist standardmäßig aktiviert; dieser ist erforderlich, bevor der VDA in einer Site verwendet werden kann.

Anpassen eines VDA

Einen installierten VDA können Sie auf folgende Weise anpassen:

1. Klicken Sie in Windows im Dialogfeld zum Hinzufügen oder Entfernen von Programmen mit der rechten Maustaste auf **Citrix Virtual Delivery Agent <*Version*>** und wählen Sie **Ändern**.
2. Wählen Sie **Virtual Delivery Agent-Einstellungen anpassen**. Wenn das Installationsprogramm startet, können Sie die Controlleradressen ändern sowie den TCP/IP-Port für die Registrierung beim Controller (Standard = 80) festlegen und ob

Portausnahmen für die Windows-Firewall automatisch geöffnet werden sollen.

Installieren über die Befehlszeile

Feb 29, 2016

Hinweis: Dieser Artikel gilt für die Installation von Komponenten auf Maschinen mit Windows-Betriebssystem. Informationen über die VDAs für Linux finden Sie unter VDAs unter Red Hat Linux sowie VDAs unter SUSE Linux.

Dieser Abschnitt enthält folgende Themen:

Einführung

Wichtig: Lesen Sie vor Beginn jeglicher Installation den Artikel Vorbereiten der Installation. Er enthält eine Beschreibung der Installationsprogramme und wichtige Informationen, mit denen Sie sich vor der Installation vertraut machen müssen. Außerdem werden die Optionen für die einzelnen Befehle erläutert. In diesem Abschnitt wird beschrieben, wie Sie die Befehlszeilenschnittstelle in einem Produktinstallationsprogramm starten.

Mit der Befehlszeilenschnittstelle können Sie folgende Aufgaben erledigen:

- Installieren einer oder mehrerer der Kernkomponenten: Delivery Controller, Citrix Studio, Citrix Director, Lizenzserver und StoreFront.
- Installieren von Virtual Delivery Agent (VDA) auf einem Masterimage bzw. auf einer virtuellen oder physischen Maschine. Sie können auch die Skripts anpassen, die auf dem Medium sind, und sie zum Installieren und Entfernen von VDAs in Active Directory verwenden.
- Anpassen bereits installierter VDAs.
- Installieren eines universellen Druckservers, der Netzwerksitzungsdrucker bereitstellt. Der Controller hat bereits die universelle Druckerserverfunktionalität; Sie müssen nur den universellen Druckserver auf den Druckservern in der Umgebung installieren.
- Aktualisieren von Komponenten; Informationen hierzu finden Sie unter Upgrade einer Bereitstellung.

Mit den Optionen /remove oder /removeall können Sie zudem zuvor installierte Komponenten aus dieser Version entfernen. Weitere Informationen finden Sie im Artikel Entfernen von Komponenten.

Sie müssen der ursprüngliche Administrator sein oder **Als Administrator ausführen** verwenden, um den Fortschritt der Befehlsausführung und die Rückgabewerte anzuzeigen. Weitere Informationen finden Sie in der Microsoft-Befehlsdokumentation.

Das Produktinstallationsprogramm und das dedizierte VDA-Installationsprogramm haben beide eine Befehlszeilenschnittstelle.

Wenn Sie VDA-Maschinen mit den Beispielskripts installieren, aktualisieren oder aus Active Directory entfernen, können Sie die unten aufgeführten VDA-Konfigurationsoptionen im VDA-Abschnitt angeben. Weitere Informationen zu den Beispielskripts finden Sie im Artikel Installieren von VDAs mit Skripts.

Verwenden des Produktinstallationsprogramms

Sie können Kernkomponenten und VDAs mit dem Produktinstallationsprogramm installieren.

- Laden Sie das Produktpaket von Citrix herunter. Zum Zugriff auf die Downloadsite benötigen Sie Citrix Kontoanmeldeinformationen.
- Entpacken Sie die Datei. Optional können Sie die ISO-Datei auch auf DVD brennen.
- Melden Sie sich mit einem lokalen Administratorkonto am Server an, auf dem Sie die Komponenten installieren.
- Legen Sie die DVD in das Laufwerk ein oder stellen Sie die ISO-Datei bereit.
- Führen Sie im Setupverzeichnis \x64\XenDesktop auf dem Medium folgenden Befehl aus:

  XenDesktopServerSetup.exe zum Installieren der Kernkomponenten. Verwenden Sie die unten im Abschnitt Befehlszeilenoptionen zur Installation der Kernkomponenten aufgeführten Optionen.

  XenDesktopVDASetup.exe zum Installieren eines VDAs. Verwenden Sie die unten im Abschnitt Befehlszeilenoptionen zur VDA-Installation aufgeführten Optionen.

Beispiele der Installation der Kernkomponenten mit dem Produktinstallationsprogramm

Beispiel 1: Mit dem folgenden Befehl werden ein XenDesktop-Controller, Studio, die Citrix Lizenzierung und SQL Server Express auf dem Server installiert. Für die Komponentenkommunikation erforderliche Ports werden automatisch geöffnet.

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /components controller,desktopstudio,licenseserver
/configure_firewall
```

Beispiel 2: Mit dem folgenden Befehl werden ein XenApp-Controller, Studio und SQL Server Express auf dem Server installiert. Für die Komponentenkommunikation erforderliche Ports werden automatisch geöffnet.

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /xenapp /components controller,desktopstudio
/configure_firewall
```

Beispiele der VDA-Installation mit dem Produktinstallationsprogramm

Beispiel 1: Mit dem folgenden Befehl wird ein VDA für Windows-Desktopbetriebssysteme und Citrix Receiver am Standardspeicherort auf einer VM installiert. VDA wird als Masterimage verwendet. Der VDA registriert sich anfänglich am Controller auf dem "Contr-Main" genannten Server in der Domäne "mydomain" und verwendet Personal vDisks, das Optimierungsfeature und die Windows-Remoteunterstützung.

```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /components vda,plugins /controllers "Contr-
Main.mydomain.local" /enable_hdx_ports /optimize /masterimage /baseimage /enable_remote_assistance
```

Beispiel 2: Mit dem folgenden Befehl wird ein VDA für Windows-Desktopbetriebssysteme und Citrix Receiver am Standardspeicherort eines Büro-PCs installiert, der mit Remote-PC-Zugriff verwendet wird. Nach der Installation von VDA wird die Maschine nicht neu gestartet. Ein Neustart ist jedoch erforderlich, bevor VDA verwendet werden kann. Der VDA registriert sich anfänglich am Controller auf dem "Contr-East" genannten Server in der Domäne "mydomain" und verwendet UDP für Audiopakete. HDX-Ports werden geöffnet, wenn der Windows-Firewalldienst erkannt wird.

```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /components vda,plugins /controllers "Contr-
East.mydomain.local" /enable_hdx_ports /enable_real_time_transport /noreboot
```

Verwenden des dedizierten VDA-Installationsprogramms

Wichtig: Informationen zu Elementen der Installation mit dem dedizierten VDA-Installationsprogramm, insbesondere zu Neustarts und dem für die Extraktion benötigen Speicherplatz, finden Sie unter Vorbereiten der Installation.

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: **VDAServerSetup.exe** für Serverbetriebssystemmaschinen oder **VDAWorkstationSetup.exe** für Desktopbetriebssystemmaschinen Verwenden Sie für Einzelbenutzer-Einzelserverbereitstellungen (z. B. beim Bereitstellen von Windows Server 2012 für einen Benutzer zur Webentwicklung) das Paket VDAWorkstationSetup.exe. Weitere Informationen finden Sie im Artikel Server-VDI.
2. Extrahieren Sie entweder zunächst die Dateien aus dem Paket 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. .\VDAWorkstationSetup.exe /extract %temp%\CitrixVDAInstallMedia. Führen Sie dann mit einem separaten Befehl **XenDesktopVdaSetup.exe** in dem Verzeichnis mit dem extrahierten Inhalt aus (im Beispiel oben wäre dies CitrixVDAInstallMedia). Verwenden Sie die unten im Abschnitt Befehlszeilenoptionen zur VDA-Installation aufgeführten Optionen.

   Zu Ausführen des heruntergeladenen Pakets führen Sie dessen Namen **VDAServerSetup.exe** oder **VDAWorkstationSetup.exe** aus. Verwenden Sie die unten im Abschnitt Befehlszeilenoptionen zur VDA-Installation aufgeführten Optionen. Hinweis für Personen, die mit dem Produktinstallationsprogramm vertraut sind: Die Ausführung des heruntergeladenen eigenständigen Pakets ist mit dem Befehl "XenDesktopVdaSetup.exe" mit Ausnahme des Namens identisch.

Beispiel der VDA-Installation mit dem eigenständigen VDA-Installationsprogramm

Der nachfolgende Installationsbefehl wird oft für Remote-PC-Zugriff verwendet. Mit ihm wird ein VDA auf einem physischen Computer ohne Citrix Receiver oder Citrix Profile Manager installiert. Nach der Installation des VDA wird die Maschine nicht automatisch neu gestartet. Ein Neustart ist jedoch erforderlich, bevor der VDA verwendet werden kann. Zu Beginn wird der VDA auf dem Server 'Contr-East' beim Controller registriert. Wenn der Windows-Firewalldienst erkannt wird, werden Ports geöffnet.

```
VDAWorkstationSetup.exe /quiet /components vda /exclude "Citrix User Profile Manager" /controllers "Contr-East.domain.com" /enable_hdx_ports /noreboot
```

> **Hinweis**
>
> Ausschließen von Citrix User Profile Manager aus der Installation hat Auswirkungen auf die Überwachung und Problembehandlung von VDAs mit Citrix Director. Auf den Seiten "Benutzerdetails" und "Endpunkte" treten Fehler in den Bereichen "Personalisierung" und "Anmeldedauer" auf. Auf den Seiten "Dashboard" und "Trends" werden im Bereich "Durchschnittliche Anmeldedauer" nur Daten für Maschinen angezeigt, auf denen Profilverwaltung installiert ist.

Anpassen eines VDAs über die Befehlszeile

Nachdem VDA installiert wurde, können Sie einige Einstellungen anpassen. Führen Sie auf dem Produktmedium im Setupverzeichnis \x64\XenDesktop den Befehl **XenDesktopVdaSetup.exe** aus und legen Sie dabei eine oder mehrere der folgenden, im Abschnitt Befehlszeilenoptionen zur VDA-Installation unten beschriebenen Optionen fest:

- /reconfigure: Diese Option ist zum Anpassen von VDA erforderlich
- /h oder /help
- /quiet
- /noreboot
- /controller
- /portnumber port
- /enable_hdx_ports

Befehlszeilenoptionen zur Installation der Kernkomponenten

In der folgenden Tabelle werden die für den Befehl **XenDesktopServerSetup.exe** verfügbaren Optionen aufgeführt.

Option	**Beschreibung**
/components component [,component] ...	Durch Trennzeichen getrennte Liste der zu installierenden oder zu entfernenden Komponenten. Gültige Werte: • CONTROLLER – Controller • DESKTOPSTUDIO – Studio • DESKTOPDIRECTOR – Director • LICENSESERVER – Citrix Lizenzserver • STOREFRONT – StoreFront Wenn diese Option ausgelassen wird, werden alle Komponenten installiert (bzw. entfernt, wenn die Option /remove ebenfalls angegeben ist).
/configure_firewall	Öffnet alle Ports in der Windows-Firewall, die für die installierten Komponenten erforderlich sind, 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.
/help oder/h	Zeigt die Hilfe für Befehle an.
/installdir Verzeichnis	Vorhandenes leeres Verzeichnis, in dem die Komponenten installiert werden.

	Standard: C:\Programme\Citrix
/logpath Pfad	Speicherort der Protokolldateien. Der angegebene Ordner muss bereits vorhanden sein. Er wird nicht vom Installationsprogramm erstellt. Standard = "%TEMP%\Citrix\XenDesktop Installer"
/no_remote_assistance	(Gilt nur für die Installation von Director.) Deaktiviert das Feature zur Benutzerspiegelung, welches Microsoft-Remoteunterstützung verwendet.
/noreboot	Verhindert einen Neustart nach der Installation. (Bei den meisten Kernkomponenten ist ein Neustart in der Standardeinstellung nicht aktiviert).
/nosql	Verhindert die Installation von Microsoft SQL Server Express auf dem Server, auf dem Sie den Controller installieren. Wenn diese Option ausgelassen wird, wird SQL Server Express installiert.
/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.
/tempdir Verzeichnis	Das Verzeichnis, das die temporären Dateien während der Installation enthält. Standard = C:\Windows\Temp.
/xenapp	Installiert XenApp. Wenn diese Option ausgelassen wird, wird XenDesktop installiert.

Befehlszeilenoptionen zur VDA-Installation

In der folgenden Tabelle werden die für den Befehl **XenDesktopVDASetup.exe** verfügbaren Optionen aufgeführt.

Bei der Installation von VDA für die Verwendung mit Remote-PC-Zugriff geben Sie nur Optionen ein, die auf physischen Maschinen (nicht VMs oder Masterimages) gültig und für VDAs für Windows-Desktopbetriebssysteme relevant sind.

Wenn nicht anders angegeben, gelten die Optionen für physische und virtuelle Maschinen sowie für VDAs für Windows-Desktopbetriebssysteme und VDAs für Windows-Serverbetriebssysteme.

Option	**Beschreibung**

/baseimage	(Gilt nur für die Installation von VDA für Windows-Desktopbetriebssysteme auf einer VM.) Ermöglicht das Verwenden von persönlichen vDisks mit einem Masterimage. Weitere Informationen finden Sie im Artikel Personal vDisks.
/components component[,component]	Durch Trennzeichen getrennte Liste der zu installierenden oder zu entfernenden Komponenten. Gültige Werte: • VDA: Installation von VDA • PLUGINS: Installation von Citrix Receiver für Windows (CitrixReceiver.exe) Verwenden Sie zum Beispiel zum Installieren des VDAs ohne Citrix Receiver "/components vda". Wenn diese Option ausgelassen wird, werden alle Komponenten installiert.
/controllers "controller [controller] [...]"	Durch Leerzeichen getrennte, vollqualifizierte Domänennamen (FQDNs) der Controller, mit denen VDA kommunizieren kann; von Anführungszeichen umschlossen. Geben Sie nicht beide Optionen, /site_guid und /controllers, an.
/enable_hdx_3d_pro	Installiert VDA für HDX 3D Pro. Weitere Informationen finden Sie im Artikel HDX 3D Pro.
/enable_hdx_ports	Öffnet die erforderlichen Ports für den Controller und die angegebenen Features (Windows-Remoteunterstützung, Echtzeitübertragung und Optimieren) 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.
/enable_real_time_transport	Aktiviert oder deaktiviert die Verwendung von UDP für Audiopakete (Echtzeittransport 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, wird der TCP-Port 3389 durch Windows in der Firewall geöffnet, selbst wenn die Option /enable_hdx_ports ausgelassen wird.
/exclude "component"[,"component"]	Verhindert die Installation der in Anführungszeichen angegebenen (durch Kommas getrennten) optionalen Komponenten. Beispiel: Installieren oder Aktualisieren eines VDAs auf einem nicht mit Maschinenerstellungsdiensten verwalteten Image erfordert keine Personal vDisk- oder Maschinenidentitätsdienstkomponenten. Gültige Werte: • Personal vDisk • Maschinenidentitätsdienst • Citrix User Profile Manager Das Ausschließen von Citrix User Profile Manager aus der VDA-Installation hat Auswirkungen auf die Überwachung und Problembehandlung von VDAs mit Citrix Director. Auf den Seiten "Benutzerdetails" und "Endpunkte" treten Fehler in den Bereichen "Personalisierung" und "Anmeldedauer" auf. Auf den Seiten "Dashboard" und "Trends" werden im Bereich "Durchschnittliche Anmeldedauer" nur Daten für Maschinen angezeigt, auf denen Profilverwaltung installiert ist.
/h oder /help	Zeigt die Hilfe für Befehle an.
/installdir Verzeichnis	Vorhandenes leeres Verzeichnis, in dem die Komponenten installiert werden. Standard: C:\Programme\Citrix

/installwithsecurebootenabled	Ermöglicht die VDA-Installation, wenn der sichere Start aktiviert ist. Wenn diese Option ausgelassen wird, gibt eine Warnung an, dass der sichere Start für eine erfolgreiche VDA-Installation deaktiviert werden muss. (Diese Option ist bei der grafischen Oberfläche nicht verfügbar)
/logpath Pfad	Speicherort der Protokolldateien. Der angegebene Ordner muss bereits vorhanden sein. Er wird nicht vom Installationsprogramm erstellt. (Diese Option ist bei der grafischen Oberfläche nicht verfügbar.) Standard = "%TEMP%\Citrix\XenDesktop Installer"
/masterimage	(Gilt nur für die Installation von VDA auf einer VM.) Richtet den VDA als Masterimage ein.
/nocitrixwddm	(Gilt nur für Windows 7-Maschinen, die keine WDDM-Treiber enthalten.) Deaktiviert die Installation des Citrix WDDM-Treibers.
/nodesktopexperience	(Gilt nur für die Installation von VDA für Windows-Serverbetriebssysteme.) Verhindert das Aktivieren von Enhanced Desktop Experience. Dieses Feature wird auch über die Citrix Richtlinieneinstellung "Enhanced Desktop Experience" gesteuert.
/noreboot	Verhindert einen Neustart nach der Installation. VDA steht erst nach einem Neustart vollständig zur Verfügung.
/optimize	Aktiviert die Optimierung für VDAs, die auf einer VM auf einem Hypervisor ausgeführt werden. Die VM-Optimierung umfasst das Deaktivieren von Offlinedateien, das Deaktivieren der Hintergrunddefragmentierung und die Verkleinerung der Ereignisprotokollgröße. Geben Sie diese Option für Remote-PC-Zugriff nicht an. Weitere Informationen zum Optimierungstool finden Sie unter CTX125874.
/portnumber port	(Gilt nur, wenn die Option /reconfig angegeben wurde.) Portnummer für die Kommunikation zwischen VDA und dem Controller. Der zuvor konfigurierte Port wird deaktiviert, es sei denn, es handelt sich um Port 80.
/quiet oder /passive	Während der Installation wird keine Benutzeroberfläche angezeigt. Der einzige Hinweis auf den Installations- und Konfigurationsvorgang ist im Windows Task-Manager. Wenn diese Option ausgelassen wird, wird die grafische Oberfläche gestartet.
/reconfig	Passt die zuvor konfigurierten VDA-Einstellungen an, wenn der Befehl mit den Optionen /portnumber, /Controller oder /enable_hdx_ports verwendet wird. Wenn Sie diese Option ohne die Option /quiet angeben, wird die grafische Oberfläche zum Anpassen von VDA gestartet.
/remove	Entfernt die mit /components angegebenen Komponenten.
/removeall	Entfernt alle installierten VDA-Komponenten.
/servervdi	Installiert einen VDA für Windows-Desktopbetriebssysteme auf einem unterstützten Windows Server. Lassen Sie diese Option aus, wenn Sie einen VDA für Windows-Serverbetriebssysteme auf einem Windows Server installieren. Lesen Sie vor dem Verwenden dieser Option den Artikel Server-VDI. (Diese Option ist bei der grafischen Oberfläche nicht verfügbar)
/site_guid guid	GUID (Globally Unique Identifier) der Website Active Directory Organisationseinheit (OU). Dabei wird ein virtueller Desktop einer Site zugeordnet, wenn Active Directory für die Discovery verwendet wird (das

	Feature für automatische Updates ist die empfohlene und Discovery-Standardmethode). Die Site-GUID ist eine Site-Eigenschaft, die in Studio angezeigt wird. Geben Sie nicht beide Optionen, /site_guid und /controllers, an.
/tempdir Verzeichnis	Das Verzeichnis für die temporären Dateien während der Installation. (Diese Option ist bei der grafischen Oberfläche nicht verfügbar.) Standard = C:\Windows\Temp.
/virtualmachine	(Gilt nur für die Installation von VDA 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.
/xa_server_location url	URL des Servers für Windows Serveranwendungen.

Installieren des universellen Druckservers über die Befehlszeile

Hinweis: Wenn Sie die UpsServer-Komponente auf einem Server mit der 32-Bit-Version von Windows 2008 installieren, lesen Sie zunächst diesen Artikel.

Führen Sie einen der folgenden Befehle auf jedem Druckserver aus:

- Unterstütztes 32-Bit-Betriebssystem: Führen Sie die Datei **UpsServer_x86.msi** aus, die sich auf dem Citrix Installationsmedium im Verzeichnis \x86\Universal Print Server\ befindet.
- Unterstütztes 64-Bit-Betriebssystem: Führen Sie die Datei **UpsServer_x64.msi** aus, die sich auf dem Citrix Installationsmedium im Verzeichnis \x64\Universal Print Server\ befindet.

Citrix empfiehlt, die Befehlsoption /ENABLE_CEIP mit der Einstellung 1 zu verwenden, um am Citrix Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) teilzunehmen. Beispiel:

```
msiexec /i UpsServer.msi ENABLE_CEIP=1
```

Wenn Sie an dem Programm teilnehmen, werden anonyme Statistiken und Nutzungsinformationen an Citrix gesendet, um die Qualität und Leistung der Citrix Produkte zu verbessern.

Nach der Installation des universellen Druckservers auf den Druckservern konfigurieren Sie diesen anhand der Anweisungen im Artikel Bereitstellen von Druckern.

Vorbereiten der Installation des universellen Druckservers unter Windows 2008 Server (32-Bit)

Zum Bereitstellen von UpsServer_x86.msi auf einer Windows 2008-32-Bit-Maschine müssen Sie die Mindestversion für Windows Installer für cdf_x86.msi und UpsServer_x86.msi mit Visual Basic-Skripts oder einem Tool wie Orca anpassen.

1. Kopieren Sie die 32-Bit-Version des CDF- und des UPS-Installationspakets (**cdf_x86.msi** und **UpsServer_x86.msi**) in einen temporären Ordner.
2. Installieren Sie das WiSumInf.vbs-Skript oder Orca. Beides ist in dem Paket Windows SDK Components for Windows Installer Developers enthalten. Informationen zu dem Skript finden Sie in dem MSDN-Artikel Manage Summary

Information.

3. Ändern Sie die Mindestversion für Windows Installer mit einer der folgenden Methoden:

   WiSumInf.vbs-Skript: Kopieren Sie die Datei WiSumInf.vbs in denselben temporären Ordner wie die beiden Citrix MSI-Pakete. Führen Sie dann das Skript für jedes Pakets mit den Parametern **WiSumInf.vbs cdf_x86.msi Pages=405** und **WiSumInf.vbs UpsServer_x86.msi Pages=405** aus.

   Orca: Öffnen Sie jeweils das Paket cdf_x86.msi und UpsServer_x86.msi, wählen Sie im Menü "View" die Option "Summary Information" aus und ändern Sie den Wert im Textfeld **Schema** in **405**.

Nach Abschluss des oben beschriebenen Verfahrens installieren Sie den universellen Druckserver auf dem Druckserver.

Installieren von VDAs mit Skripts

Feb 29, 2016

Hinweis: Dieser Artikel gilt für die Installation von Komponenten auf Maschinen mit Windows-Betriebssystem. Informationen über die VDAs für Linux finden Sie unter VDAs unter Red Hat Linux sowie VDAs unter SUSE Linux.

Das Installationsmedium enthält Beispielskripts, um Virtual Delivery Agents (VDAs) für Gruppen von Maschinen in Active Directory zu installieren, zu aktualisieren oder zu entfernen. Sie können die Skripts auch auf einzelne Maschinen anwenden und sie zum Verwalten von Masterimages einsetzen, die von den Maschinenerstellungsdiensten und Provisioning Services verwendet werden.

Erforderliche Zugriffsberechtigungen:

- Für die Skripts ist Lesezugriff für "Jeder" auf der Netzwerkfreigabe erforderlich, auf der der VDA-Installationsbefehl ist. Der Installationsbefehl ist beim vollständigen Produkt-ISO-Image "XenDesktopVdaSetup.exe" und beim eigenständigen Installationsprogramm "VDAWorkstationSetup.exe" bzw. "VDAServerSetup.exe".
- Die Protokolldetails werden auf jeder lokalen Maschine gespeichert. Sollen die Ergebnisse auch 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 ersichtlich, ob der Vorgang erfolgreich war oder nicht. Sie können herkömmliche Verzeichnissuchprogramme verwenden, um schnell eine fehlerhafte Installation oder Deinstallation im zentralen Protokoll zu finden, statt lokal auf den Zielmaschinen zu suchen.

Wichtig: Vor Beginn einer Installation führen Sie die im Artikel Vorbereiten der Installation beschriebenen Schritte durch.

Installieren oder Aktualisieren von VDAs mit dem Skript

1. Besorgen Sie sich das Beispielskript InstallVDA.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 installierenden VDA an: SET DESIREDVERSION. Beispielsweise kann die Version 7 als 7.0 angegeben werden. Der vollständige Wert befindet sich auf dem Installationsmedium in der Datei ProductVersion.txt (z. B. 7.0.0.3018); eine vollständige Übereinstimmung ist jedoch nicht erforderlich.
   - Geben Sie die Netzwerkfreigabe an, von der das Installationsprogramm aufgerufen wird Verweisen Sie auf den Stamm des Layouts (der höchste 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 wie im Artikel Installieren über die Befehlszeile beschrieben ein. 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 in Active Directory zu, in der die Maschinen sind. Diese Organisationseinheit sollte nur Maschinen enthalten, auf denen Sie VDA installieren möchten. Wenn die Maschinen in der Organisationseinheit neu gestartet werden, wird das Skript auf allen ausgeführt und VDA auf jeder Maschine installiert, deren Betriebssystem unterstützt wird.

Entfernen von VDAs mit dem Skript

1. Besorgen Sie sich das Beispielskript UninstallVDA.bat aus \Support\AdDeploy\ auf dem Installationsmedium. Citrix empfiehlt, dass Sie ein Backup der ursprünglichen Skriptdatei anlegen, bevor Sie sie ändern.
2. Bearbeiten Sie das Skript.
   - Geben Sie die Version des zu entfernenden VDA an: SET CHECK_VDA_VERSION. Beispielsweise kann die Version 7 als 7.0 angegeben werden. Der vollständige Wert befindet 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 in Active Directory zu, in der die Maschinen sind. Diese Organisationseinheit sollte nur Maschinen enthalten, von denen Sie VDA entfernen möchten. Wenn die Maschinen in der Organisationseinheit neu gestartet werden, wird das Skript auf allen ausgeführt und VDA auf jeder Maschine entfernt.

Problembehandlung

Das Skript generiert interne Protokolldateien, die den Skriptausführungsverlauf beschreiben. Das Skript kopiert das Protokoll Kickoff_VDA_Startup_Skript innerhalb von Sekunden nachdem die Bereitstellung auf der Maschine gestartet wurde in die zentrale Protokollfreigabe, sodass Sie den Gesamtvorgang überprüfen können. Wenn dieses Protokoll nicht wie vorgesehen in die Protokollfreigabe kopiert wird, können Sie zur weiteren Fehlerbehebung die lokale Maschine untersuchen, denn durch das Skript werden zwei Debugging-Protokolldateien im Ordner %temp% auf jeder Maschine gespeichert:

- Kickoff_VDA_Startup_Script_.log
- VDA_Install_ProcessLog_.log

Überprüfen Sie den Inhalt dieser Protokolle, um Folgendes für das Skript sicherzustellen:

- Es wird wie erwartet ausgeführt.
- Das Zielbetriebssystem wird korrekt erkannt.
- Der Verweis auf ROOT von DEPLOYSHARE ist korrekt konfiguriert (enthält die Datei "AutoSelect.exe").
- Die Authentifizierung bei den Freigaben DEPLOYSHARE und LOG ist möglich.

Installieren von VDAs unter Red Hat Linux

Feb 29, 2016

Sie können virtuelle Linux-Desktops auf der Basis einer Red Hat-Distribution erstellen. Bereiten Sie die Linux-VMs vor, installieren Sie die neue Linux-VDA-Software darauf, konfigurieren Sie den Delivery Controller und stellen Sie die Desktops den Benutzern mit Studio zur Verfügung.

Weitere Informationen finden Sie im folgenden Dokument:

PDF **Linux Virtual Desktop Installation Guide for Red Had Linux**

PDF der Anweisungen zu Installation und Einrichtung von Red Hat Linux-VDAs

Installieren von VDAs mit SUSE Linux

Feb 29, 2016

Sie können virtuelle Linux-Desktops auf der Basis einer SUSE-Distribution erstellen. Bereiten Sie die Linux-VMs vor, installieren Sie die neue Linux-VDA-Software darauf, konfigurieren Sie den Delivery Controller und stellen Sie die Desktops den Benutzern mit Studio zur Verfügung.

Weitere Informationen finden Sie im folgenden Dokument:

PDF

Installieren von VDAs mit SUSE Linux

PDF der Anweisungen zu Installation und Einrichtung von SUSE Linux-VDAs

Erstellen einer Site

Feb 29, 2016

Unter der *Site* versteht man die XenApp- bzw XenDesktop-Bereitstellung. Sie umfasst die Delivery Controller und andere Kernkomponenten, Virtual Delivery Agents (VDAs), Verbindungen mit Hosts (falls verwendet) sowie die Maschinenkataloge und Bereitstellungsgruppen, die Sie erstellen und verwalten. Sie erstellen die Site nach der Installation der Kernkomponenten und bevor Sie den ersten Maschinenkatalog und die erste Bereitstellungsgruppe erstellen.

Lesen Sie diesen Artikel über die vor der Siteerstellung zu treffenden Vorbereitungen und Entscheidungen, bevor Sie den Assistenten für die Siteerstellung starten.

Assistent für die Siteerstellung

Öffnen Sie Studio, falls es nicht geöffnet ist. Sie werden automatisch zu der Aktion zum Starten des Assistenten für die Siteerstellung geführt. Die Seiten des Assistenten decken folgende Konfigurationsbereiche ab:

Name und Typ der Site

Es stehen zwei Sitetypen zur Auswahl:

- **Anwendungs- und Desktopbereitstellungssite**: Wenn Sie eine Anwendungs- und Desktopbereitstellungssite erstellen, haben Sie die Wahl zwischen einer vollständigen Bereitstellung (empfohlen) oder einer leeren Site. Leere Sites sind nur teilweise konfiguriert und werden normalerweise von erfahrenen Administratoren erstellt.
- **Remote-PC-Zugriff-Site**: Sites dieses Typs ermöglichen Benutzern den Remotezugriff auf ihre Büro-PCs über eine sichere Verbindung.

Wenn Sie zu diesem Zeitpunkt eine Bereitstellung für die Anwendungs- und Desktopbereitstellung erstellen, können Sie eine Remote-PC-Zugriff-Bereitstellung später hinzufügen. Ebenso können Sie einer Remote-PC-Zugriff-Bereitstellung später eine vollständige Bereitstellung hinzufügen.

Geben Sie einen Namen für die Site ein. Nachdem die Site erstellt wurde, wird der Name oben im Studio-Navigationsbereich angezeigt: **Citrix Studio** (*Sitename*).

Datenbanken

Die Seite **Datenbanken** enthält Einstellungen zur Einrichtung der Site-, Überwachungs- und Konfigurationsprotokollierungsdatenbank. Informationen zu Anforderungen für die Datenbanken und zu deren Einrichtung finden Sie im Artikel Datenbanken.

Wenn Sie keine standardmäßige SQL Server Express-Installation verwenden möchten, installieren Sie vor Erstellen der Site SQL Server auf den Maschinen. Die unterstützten Versionen werden im Artikel "Systemanforderungen" aufgeführt.

Wenn Sie bereits die Controller-Software auf anderen Servern installiert haben und der Site weitere Delivery Controller hinzufügen möchten, können Sie dies über diese Seite im Assistenten für die Siteerstellung tun. Wenn Sie Skripts für die Einrichtung der Datenbanken generieren möchten, fügen Sie die Controller vor dem Generieren der Skripts hinzu.

Lizenzierung

Überlegen Sie, ob Sie vorhandene Lizenzen verwenden möchten oder das 30-tägige kostenlose Probeabo, bei dem die

Lizenzdateien später hinzugefügt werden können. Sie können Lizenzdateien auch über den Assistenten für die Siteerstellung hinzufügen oder herunterladen. Weitere Informationen finden Sie in der Dokumentation zur Lizenzierung.

Geben Sie die Adresse des Lizenzservers im Format *Name*:[*Port*] an. Der Name muss ein vollqualifizierter Domänenname (FQDN), ein NetBIOS-Name oder eine IP-Adresse sein, empfohlen wird die Verwendung eines FQDN. Wenn Sie die Portnummer auslassen, ist der Standardport 27000. Klicken Sie auf **Connect**. Sie können erst mit der nächsten Seite des Assistenten fortfahren, wenn eine Verbindung zum Lizenzserver hergestellt wurde.

Energieverwaltung (nur Remote-PC-Zugriff)

Informationen finden Sie im Abschnitt Remote-PC-Zugriff unten.

Hostverbindung, Netzwerk und Speicher

Wenn Sie VMs auf einem Hypervisor oder in einer Cloud zum Bereitstellen von Anwendungen und Desktops verwenden möchten, richten Sie diese Hostumgebung vor dem Erstellen der Site ein. (Informationen finden Sie in den unten aufgeführten Informationsquellen.)

Sie erstellen die erste Verbindung mit einem Host im Assistenten für die Siteerstellung; Sie können diese später modifizieren und weitere Verbindungen erstellen. Wenn Sie keinen Virtualisierungshost verwenden oder Studio für die Verwaltung von Benutzerdesktops nutzen, die auf dedizierten Blade-PCs gehostet werden, wählen Sie den Verbindungstyp **Keine**.

Wenn Sie eine Remote-PC-Zugriff-Site konfigurieren und Wake-On-LAN verwenden möchten, wählen Sie als Hosttyp Microsoft System Center Configuration Manager.

Geben Sie an, ob Sie Maschinenerstellungsdienste (MCS) oder andere Tools zum Erstellen von VMs auf dem Host verwenden möchten.

Nachdem Sie Verbindungstyp und Tools ausgewählt haben, geben Sie auf den folgenden Seiten des Assistenten Informationen zu Speicher und Netzwerk für die Verbindung, d. h. ihren *Ressourcen*, ein. Nach dem Erstellen der Site identifiziert der Ressourcenname in Studio die Kombination aus Speicher und Netzwerk für die Verbindung.

- Geben Sie an, ob Sie freigegebenen oder lokalen Speicher auf dem Host verwenden möchten. Freigegebener Speicher ist über die von Ihnen ausgewählten Netzwerke verfügbar. Wenn Sie einen freigegebenen Speicher mit XenServer verwenden, können Sie die Verwendung von IntelliCache aktivieren, um die Last auf dem Speichergerät zu reduzieren (siehe Verbindungen).
- Wenn Sie Desktopbetriebssystemmaschinen erstellen möchten, geben Sie an, ob Sie persönliche vDisks verwenden möchten, und wählen Sie den von diesen genutzten Speicher an. Persönliche vDisks können den gleichen Speicher wie die VMs oder einen anderen Speicher nutzen. Weitere Informationen finden Sie im Artikel Personal vDisks.
- Wählen Sie die verfügbaren Netzwerke, die die VMs verwenden sollen.

Informationsquellen zum Verbindungstyp

VMware

- Artikel VMware-Virtualisierungsumgebungen
- VMware-Produktdokumentation

Microsoft Hyper-V

- Artikel Microsoft System Center Virtual Machine Manager-Virtualisierungsumgebungen
- Microsoft-Dokumentation

Microsoft Azure

- Artikel Microsoft Azure-Virtualisierungsumgebungen
- Microsoft-Dokumentation
- Beim Erstellen einer Verbindung in Studio können Sie automatisch Informationen aus einer Datei mit Veröffentlichungseinstellungen importieren, die Sie von https://manage.windowsazure.com/publishsettings/index heruntergeladen haben.

Amazon Web Services (AWS)

- CTX140427
- AWS-Dokumentation
- Beim Erstellen einer Verbindung in Studio müssen Sie den API-Schlüssel und die Werte des geheimen Schlüssels angeben. Sie können die Schlüsseldatei mit diesen Werten aus AWS oder CloudPlatform exportieren und anschließend importieren. Sie müssen auch die Werte für Region, Availability Zone, 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 von Studio nicht zum Ausfüllen der Felder "API-Schlüssel" und "Geheimer Schlüssel" verwendet werden. Verwenden Sie AWS IAM-Anmeldeinformationsdateien.

Citrix CloudPlatform

- CTX140428.
- Citrix CloudPlatform-Dokumentation
- Beim Erstellen einer Verbindung in Studio müssen Sie den API-Schlüssel und die Werte des geheimen Schlüssels angeben. Sie können die Schlüsseldatei mit diesen Werten aus CloudPlatform exportieren und anschließend importieren.

Citrix XenServer

- Citrix XenServer-Dokumentation
- Beim Erstellen einer Verbindung müssen Sie die Anmeldeinformationen eines VM-Hauptadministrators oder eines höherrangigen Benutzers eingeben.
- Citrix empfiehlt die Verwendung von HTTPS zur Sicherung der Kommunikation mit XenServer. Um HTTPS zu verwenden, müssen Sie das standardmäßig mit XenServer installierte SSL-Zertifikat ersetzen (siehe CTX128656).
- Sie können hohe Verfügbarkeit konfigurieren, wenn diese auf XenServer aktiviert ist. Citrix empfiehlt, dass Sie alle Server im Pool (über "Server mit hoher Verfügbarkeit bearbeiten") auswählen, um die Kommunikation mit XenServer zu ermöglichen, wenn der Poolmaster ausfällt.
- Sie können einen GPU-Typ und eine GPU-Gruppe oder die Passthrough-Authentifizierung auswählen, wenn der XenServer vGPU unterstützt. Es wird angezeigt, ob die Auswahl dedizierte GPU-Ressourcen umfasst.

App-V

Wenn Sie Anwendungen aus Microsoft App-V-Paketen bereitstellen möchten, geben Sie die URL des Microsoft App-V-Verwaltungsservers und die URL und Portnummer des App-V- Veröffentlichungsservers an. Sie können diese Informationen auch später noch konfigurieren. Weitere Informationen finden Sie im Artikel App-V.

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 in dem Artikel zu Microsoft System Center Configuration Manager.

Für das Erstellen einer Remote-PC-Zugriff-Site gilt Folgendes:

- Wenn Sie Wake-On-LAN verwenden, geben Sie die Adresse, Anmeldeinformationen und Verbindungsinformationen für Microsoft System Center Configuration Manager auf der Seite **Energieverwaltung** an.
- Geben Sie Benutzer bzw. Benutzergruppen auf der Seite "Benutzer" an, denn es gibt keine Standardaktion zum automatischen Hinzufügen aller Benutzer. Geben Sie außerdem Maschinenkonten (Domänen- oder OU-Konten) auf der Seite **Maschinenkonten** des Assistenten an.

  Zum Hinzufügen von Benutzerinformationen klicken Sie auf **Benutzer hinzufügen**. Wählen Sie Benutzer und Benutzergruppen aus und klicken Sie dann auf **Benutzer hinzufügen**.

  Zum Hinzufügen von Maschinenkonten klicken Sie auf **Maschinenkonten hinzufügen**. Wählen Sie die

Maschinenkonten aus und klicken Sie dann auf **Maschinenkonten hinzufügen**. Klicken Sie auf **Organisationseinheiten hinzufügen**. Wählen Sie die Domäne und die Organisationseinheiten und geben Sie an, ob Elemente in Unterordnern eingeschlossen werden. Klicken Sie auf **Organisationseinheiten hinzufügen**.

Hinweis: Beim Erstellen einer Remote-PC-Zugriff-Site wird automatisch ein Maschinenkatalog erstellt, der alle Maschinenkonten, die Sie über den Assistenten für die Siteerstellung hinzugefügt haben, enthält. Es wird automatisch eine Bereitstellungsgruppe mit allen von Ihnen hinzugefügten Benutzern und Gruppen erstellt.

Gut zu wissen

- Sie werden von dem Assistenten für die Siteerstellung gefragt, ob Sie sich an dem Programm zur Verbesserung der Benutzerfreundlichkeit von Citrix beteiligen möchten. Wenn Sie diesem Programm beitreten, werden anonyme Statistik- und Nutzungsinformationen an Citrix gesendet (Informationen finden Sie unter http://more.citrix.com/XD-CEIP).
- Auf der letzten Seite des Assistenten für die Siteerstellung wird eine Zusammenfassung der von Ihnen angegebenen Informationen angezeigt. Verwenden Sie die Schaltfläche **Zurück**, wenn Sie etwas ändern möchten. Wenn Sie fertig sind, klicken Sie auf **Erstellen**, um die Siteerstellung zu starten.
- Der Benutzer, der eine Site erstellt, ist Volladministrator dieser Site. Weitere Informationen finden Sie im Artikel Delegierte Administration.

Testen einer Sitekonfiguration

Sie können einen HTML-Bericht der Testergebnisse für die Site anzeigen.

Zum Durchführen der Tests, nachdem Sie die Site erstellt haben, wählen Sie **Citrix Studio (Site *Sitename*)** oben im Navigationsbereich und klicken Sie dann im mittleren Bereich auf **Site testen**.

Erstellen von Maschinenkatalogen

Feb 29, 2016

Sammlungen von physischen oder virtuellen Maschinen werden als Einheit in einem so genannten *Maschinenkatalog* verwaltet. Alle Maschinen in einem Maschinenkatalog haben den gleichen Betriebssystemtyp: Server oder Desktop. Ein Katalog mit Serverbetriebssystemmaschinen kann entweder Windows- oder Linux-Maschinen enthalten, nicht aber beides.

Nach dem Erstellen der Site werden Sie von Studio zur Erstellung des ersten Maschinenkatalogs geführt. Nach dem Erstellen des ersten Maschinenkatalogs werden Sie von Studio zur Erstellung der ersten Bereitstellungsgruppe geführt. Später können Sie den erstellten Katalog ändern und weitere Kataloge erstellen.

Übersicht

Wenn Sie einen Maschinenkatalog für VMs erstellen, geben Sie an, wie diese bereitgestellt werden. Sie können die von Studio unterstützten Tools (z. B. Maschinenerstellungsdienste oder Provisioning Services) oder eigene Tools verwenden. Selbst wenn Sie die Maschinen bereits haben, d. h. keine Masterimages verwenden müssen, erstellen Sie mindestens einen Maschinenkatalog.

- Wenn Sie Maschinen mit Provisioning Services erstellen, lesen Sie die Dokumentation zu Provisioning Services.
- Bei Verwendung von Maschinenerstellungsdiensten (MCS) stellen Sie ein Masterimage (bzw. einen Snapshot) zum Erstellen identischer virtueller Maschinen im Katalog bereit. Vor dem Erstellen des Katalogs verwenden Sie Tools auf dem Hypervisor bzw. im Clouddienst zum Erstellen und Konfigurieren des Masterimages. Dazu gehört auch die Installation eines Virtual Delivery Agents (VDA) auf dem Image. Beim anschließenden Erstellen des Maschinenkatalogs in Studio wählen Sie das Image (bzw. dessen Snapshot) und geben die Anzahl der in dem Katalog zu erstellenden VMs und weitere Informationen an.

Beim Erstellen des ersten Maschinenkatalogs mit MCS oder PVS verwenden Sie die Hostverbindung, die Sie beim Erstellen der Site konfiguriert haben. Nach dem Erstellen des ersten Maschinenkatalogs und der ersten Bereitstellungsgruppe können Sie die Informationen über diese Verbindung ändern und zusätzliche Verbindungen erstellen.

Nach Abschließen des Assistenten zum Erstellen von Maschinenkatalogen werden automatisch Tests ausgeführt, um sicherzustellen, dass der Katalog richtig konfiguriert wurde. Wenn die Tests abgeschlossen sind, können Sie einen Testbericht anzeigen. Sie können diese Tests bei Bedarf später über **Citrix Studio** *Sitename* im Studio-Navigationsbereich ausführen.

Tipp: Wenn Sie einen Katalog direkt mit dem PowerShell-SDK anstelle von Studio erstellen, können Sie alternativ zu einem Image bzw. einem Image-Snapshot eine Hypervisorvorlage (VMTemplates) angeben.

Für Windows XP- und Windows Vista-Maschinen muss eine ältere VDA-Version verwendet werden. Die Verwendung der neuesten Produktfeatures ist hier nicht möglich. Wenn Sie diese Maschinen nicht auf eine unterstützte Windows-Betriebssystemversion aktualisieren können, empfiehlt Citrix, sie in einem separaten Maschinenkatalog zu führen.

Überblick über die Katalogerstellung mit MCS

Nachdem Sie Informationen im Assistenten zum Erstellen von Maschinenkatalogen eingegeben haben, erfolgen die nachfolgend aufgeführten Aktionen in MCS.

- Wenn Sie im Assistenten 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 Desktops hinzu, wodurch eindeutige Identitäten erstellt werden.
- MCS erstellt die im Assistenten angegebene Anzahl VMs mit jeweils zwei Datenträgern. Neben den beiden Datenträgern wird jeweils ein Master am gleichen Speicherort gespeichert. Wenn Sie mehrere Speicherorte definiert haben, werden an jedem die folgenden Datenträgertypen erstellt:
  - Vollständige Kopie des Snapshots (siehe oben); diese ist schreibgeschützt und wird von allen gerade erstellten VMs gemeinsam genutzt.
  - Eine eindeutige 16-MB-Identitätsdisk, durch die jede VM eine eindeutige Identität erhält. Jede VM erhält eine Identitätsdisk.
  - Ein eindeutiger differenzierender Datenträger zum Speichern der auf der VM erfolgten Schreibvorgänge. Dieser Datenträger ist, sofern dies vom Hostspeicher unterstützt wird, für schlanke Speicherzuweisung geeignet und kann bei Bedarf auf die maximale Größe des Masterimages, anwachsen. Jede VM erhält einen differenzierenden Datenträger. Auf diesem Datenträger werden Änderungen, die während der Sitzungen gemacht werden, gespeichert. Er ist für dedizierte Desktops permanent und für gepoolte Desktops flüchtig, d. h. er wird bei jedem Neustart gelöscht und neu erstellt.

Vorbereiten eines Masterimages auf dem Hypervisor bzw. im Clouddienst

Tipp: Benötigen Sie Informationen zum Verbindungstyp? Die finden Sie hier.

Das Masterimage enthält das Betriebssystem, nicht virtualisierte Anwendungen, den VDA und andere Software.

Gut zu wissen:

- Masterimages werden auch als Klonimage, Golden Image, Basis-VM oder Basisimage bezeichnet. Hosthersteller und Clouddienstanbieter verwenden andere Bezeichnungen.
- Wenn Sie Provisioning Services verwenden, können Sie entweder ein Masterimage oder einen physischen Computer als Masterzielgerät verwenden. In Provisioning Services wird für Images eine andere Terminologie verwendet als in MCS (Einzelheiten s. zugehörige Dokumentation).
- Stellen Sie sicher, dass Ihr Host genügend Prozessoren, Arbeitsspeicher und Speicher zur Unterbringung der Maschinen hat, die Sie erstellen möchten.
- Konfigurieren Sie den für Desktops und Anwendungen erforderlichen Speicherplatz auf der Festplatte, da dieser Wert später nicht im Maschinenkatalog geändert werden kann.
- Bei Remote-PC-Zugriff-Maschinenkatalogen werden keine Masterimages verwendet.
- Hinweise zur Microsoft KMS-Aktivierung bei Verwendung von MCS:
  - Wenn Ihre Bereitstellung 7.x-VDAs mit einem XenServer 6.1- oder 6.2-Host, einem vSphere-Host oder einem Microsoft System Center Virtual Machine Manager-Host enthält, müssen Sie Microsoft Windows oder Microsoft Office nicht manuell zurücksetzen.
  - Wenn die Bereitstellung einen 5.x-VDA mit einem XenServer 6.0.2-Host enthält, lesen Sie CTX128580.
- Installieren und konfigurieren Sie die folgende Software auf dem Masterimage:
  - Integrationstools für den Hypervisor (z. B. XenServer-Tools, Hyper-V-Integrationsdienste oder VMware-Tools). Wenn Sie diesen Schritt auslassen, funktionieren die Anwendungen und Desktops unter Umständen nicht richtig.
  - Einen VDA – Citrix empfiehlt die Installation der neuesten Version, damit die neuesten Features verfügbar sind. Wird kein VDA auf dem Masterimage installiert, schlägt die Katalogerstellung fehl.
  - Tools von Drittanbietern, zum Beispiel Antivirensoftware oder Agents zur elektronischen Softwareverteilung. Konfigurieren Sie Dienste mit den für Benutzer und Maschinentyp geeigneten Einstellungen (z. B. Featureupdates).
  - Anwendungen von Drittanbietern, die Sie nicht virtualisieren möchten. Citrix empfiehlt das Virtualisieren von Anwendungen, da dies die Kosten erheblich senkt, 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 Provisioning Services oder MCS verwenden, führen Sie auf den Masterimages nicht Sysprep aus.

1. Erstellen Sie mit dem Verwaltungstool des Hypervisors ein neues Masterimage und installieren Sie dann das Betriebssystem sowie alle Service Packs und Updates Die Anzahl der vCPUs und die Größe des Speichers sind zu diesem Zeitpunkt nicht wichtig, da Sie diese Werte ändern können, wenn Sie den Maschinenkatalog erstellen. Konfigurieren Sie jedoch den für Desktops und Anwendungen erforderlichen Speicherplatz auf der Festplatte, da dieser Wert später nicht im Katalog geändert werden kann.
2. Stellen Sie sicher, dass die Festplatte am Gerätestandort 0 verbunden ist. Dieser Standort ist in den meisten Standardmasterimagevorlagen automatisch konfiguriert; in einigen benutzerdefinierten Vorlagen ist dies jedoch nicht unbedingt der Fall.
3. Installieren und konfigurieren Sie die oben aufgeführte Software auf dem Masterimage:
4. Bei Verwendung von Provisioning Services erstellen Sie eine VHD-Datei für die vDisk von Ihrem Masterzielgerät, bevor Sie das Masterzielgerät in eine Domäne einbinden. Weitere Informationen finden Sie in der Dokumentation zu Provisioning Services.
5. Fügen Sie das Masterimage der Domäne hinzu, der Desktops und Anwendungen angehören werden, und stellen Sie sicher, dass das Masterimage auf dem Host verfügbar ist, auf dem die Maschinen erstellt werden. Das Masterimage muss keiner Domäne angefügt werden, wenn Sie MCS verwenden. Die bereitgestellten Maschinen werden Mitglied der im Assistenten zum Erstellen von Maschinenkatalogen angegebenen Domäne.
6. Citrix empfiehlt, dass Sie einen Snapshot des Masterimages erstellen und benennen, damit es künftig identifiziert werden kann. Wenn Sie ein Masterimage anstelle eines Snapshots beim Erstellen eines Maschinenkatalogs angeben, erstellt Studio automatisch einen Snapshot, der jedoch nicht umbenannt werden kann.

Vorbereiten eines Masterimages für GPU-fähige Maschinen auf XenServer

Wenn Sie für Ihre Hostinginfrastruktur XenServer verwenden, benötigen GPU-fähige Maschinen ein dediziertes Masterimage. Diese VMs erfordern Videotreiber, die GPUs unterstützen und so konfiguriert sind, dass die VMs Software verwenden können, die den 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 der GPU (entweder Passthrough oder vGPU) verwendet werden kann.
3. Installieren Sie ein unterstütztes Betriebssystem und aktivieren Sie RDP.
4. Installieren Sie XenServer-Tools und NVIDIA-Treiber.
5. Deaktivieren Sie die VNC-Verwaltungskonsole (Virtual Network Computing), um die Leistung zu optimieren, und starten Sie anschließend die VM neu.
6. Sie werden aufgefordert, RDP zu verwenden. Installieren Sie mit RDP den VDA und starten Sie dann die VM neu.
7. Optional können Sie einen Snapshot der VM erstellen und als Vorlage für andere GPU-Masterimages verwenden.
8. Installieren Sie mit RDP kundenspezifische Anwendungen, die in XenCenter konfiguriert werden und GPU-Funktionen verwenden.

Erstellen eines Maschinenkatalogs mit Studio

Bevor Sie den Assistenten zum Erstellen von Maschinenkatalogen starten, lesen Sie diesen Abschnitt, damit Sie wissen, welche Optionen Sie auswählen und welche Informationen Sie angeben müssen. Je nach den von Ihnen ausgewählten Optionen werden einige der unten beschriebenen Seiten möglicherweise nicht angezeigt oder heißen anders.

Wichtig: Wenn Sie ein Masterimage verwenden, vergewissern Sie sich vor dem Erstellen des Maschinenkatalogs, dass auf dem Image ein VDA installiert ist.

In Studio:

- Wenn Sie eine Site, jedoch noch keinen Maschinenkatalog erstellt haben, führt Studio Sie zum richtigen Startpunkt zur Erstellung eines Maschinenkatalogs.
- Wenn Sie bereits einen Maschinenkatalog erstellt haben und einen weiteren erstellen möchten, wählen Sie im Studio-Navigationsbereich **Maschinenkataloge** und dann im Aktionsbereich **Maschinenkatalog erstellen**.

Der Assistent führt Sie durch die nachfolgend beschriebenen Einstellungen. Die angezeigten Assistentenseiten können sich

je nach der von Ihnen vorgenommenen Auswahl unterscheiden.

Betriebssystem

Jeder Katalog enthält nur Maschinen eines Typs:

- **Serverbetriebssystem:** Ein Maschinenkatalog für Serverbetriebssysteme bietet Desktops und Anwendungen, die von mehreren Benutzern verwendet werden können. Auf den Maschinen können die unterstützten Versionen von Windows oder Linux ausgeführt werden, ein Katalog kann jedoch nur Windows- oder Linux-Maschinen enthalten.
- **Desktopbetriebssystem:** Ein Maschinenkatalog für Desktopbetriebssysteme bietet Desktops und Anwendungen, die unterschiedlichen Benutzern zugewiesen werden.
- **Remote-PC-Zugriff:** Ein Remote-PC-Zugriff-Maschinenkatalog bietet Benutzern Remotezugriff auf ihre physischen Büro-Desktopmaschinen. Bei Remote-PC-Zugriff wird VPN nicht für die Sicherheit benötigt.

Maschinenverwaltung

Auf der Seite **Maschinenverwaltung** wird angegeben, wie die Maschinen verwaltet und mit welchem Tool sie bereitgestellt werden.

Wählen Sie, ob für Maschinen in dem Katalog die Energieverwaltung über Studio ausgeführt werden soll.

- Maschinen mit Energieverwaltung über Studio oder über eine Cloudumgebung bereitgestellte Maschinen (z. B. VM oder Blade-PC). Diese Option ist nur verfügbar, wenn bereits eine Hypervisor- oder Clouddienstverbindung konfiguriert wurde.
- Maschinen ohne Energieverwaltung (z. B. physische Maschinen).

Wenn Sie angegeben haben, dass die Energieverwaltung der Maschinen über Studio oder die Maschinenbereitstellung über eine Cloudumgebung erfolgen soll, wählen Sie aus, welches Tool Sie für die Maschinenbereitstellung verwenden möchten.

- **Maschinenerstellungsdienste (MCS):** verwendet ein Masterimage zum Erstellen und Verwalten virtueller Maschinen. Bei Maschinenkatalogen in Cloudumgebungen wird MCS verwendet. MCS ist für physische Maschinen nicht verfügbar.
- **Provisioning Services:** verwaltet Zielgeräte als Gerätesammlung. Eine als Image eines Masterzielgeräts erstellte Provisioning Services-vDisk liefert Desktops und Anwendungen. Diese Option ist für Cloudbereitstellungen nicht verfügbar.
- **Anderes:** Tool, mit dem bereits Maschinen im Datencenter verwaltet werden. Citrix empfiehlt die Verwendung von Microsoft System Center Configuration Manager oder einer anderen Drittanbieteranwendung, um sicherzustellen, dass die Maschinen in dem Katalog konsistent sind.

Desktoptypen (Desktoperfahrung)

Über die Seite **Desktoperfahrung** wird der Typ der zu erstellenden Desktops festgelegt. Die Seite wird nur angezeigt, wenn ein Katalog für Desktopbetriebssystemmaschinen erstellt wird. Der Typ hängt davon ab, ob die jeweilige Maschine einem Benutzer zugewiesen ist und was mit den Änderungen des Benutzers passiert, wenn die Maschine neu gestartet wird.

Es gibt drei Typen:

- **Gepoolt, zufällig:** Desktops werden nach dem Zufallsprinzip zugewiesen, die Benutzer werden bei jeder Anmeldung mit einem neuen Desktop verbunden. Wenn ein Benutzer sich abmeldet, wird der Desktop für einen anderen Benutzern verfügbar. Wird der Desktop neu gestartet, werden alle gemachten Änderungen verworfen.
- **Gepoolt, statisch:** Desktops werden bleiben zugewiesen, die Benutzer werden bei jeder Anmeldung mit dem gleichen Desktop verbunden. Wenn ein Benutzer sich abmeldet, bleibt der Desktop nur für diesen Benutzer verfügbar. Wird der Desktop neu gestartet, werden alle gemachten Änderungen verworfen.

- **Dediziert:** Desktops sind dauerhaft einem Benutzer zugewiesen. Wenn ein Benutzer sich abmeldet, bleibt der Desktop nur für diesen Benutzer verfügbar. Wird der Desktop neu gestartet, werden alle gemachten Änderungen beibehalten. Änderungen können auf einem lokalen VM-Datenträger oder in einem Laufwerk auf einer eigenen persönlichen vDisk gespeichert werden.

Masterimage

Wählen Sie die Verbindung mit dem Host-Hypervisor oder Clouddienst und anschließend den zuvor erstellten Snapshot bzw. die zuvor erstellte virtuelle Maschine. Beim Erstellen des ersten Maschinenkatalogs ist nur die Verbindung verfügbar, die Sie beim Erstellen der Site konfiguriert haben.

Erinnerung:

- Wenn Sie Provisioning Services oder MCS verwenden, führen Sie auf den Masterimages nicht Sysprep aus.
- Wenn Sie ein Masterimage anstelle eines Snapshots angeben, erstellt Studio automatisch einen Snapshot, der jedoch nicht umbenannt werden kann.

Vergewissern Sie sich, dass auf dem Masterimage die aktuelle VDA-Version installiert ist, damit Sie die neuesten Produktfeatures verwenden können. Behalten Sie die Standardeinstellung für **Wählen Sie die VDA-Version** auf der Seite des Assistenten bei.

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.

Sicherheit (Cloudumgebungen)

Wählen Sie mindestens eine Sicherheitsgruppe für die virtuellen Maschinen. Diese werden nur angezeigt, wenn die Verfügbarkeitszone Sicherheitsgruppen unterstützt.

Entscheiden Sie, ob die Maschinen Hardware gemeinsam oder dedizierte Hardware verwenden sollen.

Virtuelle Maschinen, Gerätesammlung oder virtuelle Maschinen und Benutzer

Der Titel der Seite hängt von der Bereitstellungsmethode ab, die Sie auf der Seite **Maschinenverwaltung** gewählt haben.

- Wenn Sie MCS gewählt haben, lautet der Titel **Virtuelle Maschinen**.
- Wenn Sie Provisioning Services gewählt haben, lautet der Titel **Gerätesammlung**.
- Wenn Sie "Anderes" gewählt haben, lautet der Titel **VMs und Benutzer**.

Seite:

- Legen Sie fest, wie viele virtuelle Maschinen erstellt werden sollen.
- Wählen Sie die Menge Arbeitsspeicher in MB, die jede Maschine haben soll. Jede VM hat eine 32-GB-Festplatte. Dieser Wert ist im Masterimage festgelegt und kann im Katalog nicht geändert werden.
- Wenn Sie auf der Seite "Desktoperfahrung" festgelegt haben, dass die Änderungen der Benutzer an Desktops auf separaten Personal vDisks gespeichert werden sollen, geben Sie deren Größe in Gigabyte und den Laufwerksbuchstaben an.
- Wenn Ihre Bereitstellung mehrere Zonen enthält, können Sie eine Zone für den Katalog wählen.

Netzwerkkarten

Wenn Sie mehrere Netzwerkkarten verwenden möchten, weisen Sie jeder ein virtuelles Netzwerk zu. Sie können

beispielsweise einer Karte ein bestimmtes sicheres Netzwerk und einer anderen ein häufiger verwendetes Netzwerk zuweisen. Auf dieser Seite können Sie auch Netzwerkkarten hinzufügen und entfernen.

Maschinenkonten

Geben Sie die hinzuzufügenden Active Directory-Maschinenkonten oder Organisationseinheiten an, die Benutzern oder Benutzergruppen entsprechen (dies gilt nur für Remote-PC-Zugriff-Kataloge). Vergessen Sie nicht den Schrägstrich (/) im Namen von Organisationseinheiten.

Sie können eine zuvor konfigurierte Energieverwaltungsverbindung auswählen oder die Energieverwaltung nicht verwenden. Wenn Sie die Energieverwaltung verwenden möchten, jedoch noch keine geeignete Verbindung konfiguriert wurde, können Sie die Verbindung später erstellen und dann die Energieverwaltungseinstellungen des Maschinenkatalogs entsprechend bearbeiten.

Computerkonten

Jede Maschine im Maschinenkatalog benötigt ein Active Directory-Computerkonto. Geben Sie an, ob neue Konten erstellt oder vorhandene Konten verwendet werden sollen, und geben Sie den Speicherort für diese Konten an.

- Wenn Sie neue Konten erstellen, müssen Sie Zugang zu einem Domänenadministratorkonto für die Domäne haben, in der die Maschinen residieren werden.

  Legen Sie für die zu erstellenden Maschinen das Kontobenennungsschema mit Hashmarkierungen zur Kennzeichnung der Platzierung sequenzieller Zahlen bzw. Buchstaben fest. Vergessen Sie nicht den Schrägstrich (/) im Namen von Organisationseinheiten. Namen dürfen nicht mit einer Zahl beginnen. Beispiel: Das Benennungsschema "PC-Vertrieb-##" (und Aktivierung von 0-9) bewirkt eine Benennung der Computerkonten als "PC-Vertrieb-01", "PC-Vertrieb-02", "PC-Vertrieb-03" usw.

- Wenn Sie bestehende Konten verwenden, navigieren Sie zu den Konten oder klicken Sie auf "Importieren" und geben Sie eine CSV-Datei mit Kontonamen an. Die importierte Datei muss folgendes Format aufweisen:

  [ADComputerkonto]
  ADComputerkontoname.domäne

  ...

  Stellen Sie sicher, dass Sie ausreichend Konten für die hinzuzufügenden Maschinen haben. Da diese Konten von Studio verwaltet werden, gestatten Sie Studio, die Kennwörter für alle Konten zurückzusetzen, oder geben Sie das Kontokennwort (muss für alle Konten gleich sein) an.

Bei Katalogen mit physischen oder vorhandenen Maschinen wählen Sie vorhandene Konten aus oder importieren Sie diese, und weisen Sie jeder Maschine sowohl ein Active Directory-Computerkonto als auch ein Benutzerkonto zu.

Bei Maschinen, die mit Provisioning Services erstellt wurden, werden Computerkonten für Zielgeräte anders verwaltet. Weitere Informationen hierzu finden Sie in der Dokumentation zu Provisioning Services.

Name und Beschreibung

Überprüfen Sie auf der Seite **Zusammenfassung** Ihre Einstellungen. Geben Sie einen Namen und eine Beschreibung für den Katalog ein. Diese Informationen werden in Studio angezeigt.

Prüfen Sie die Informationen, die Sie angegeben haben, und klicken Sie auf **Fertig stellen**, um die Katalogerstellung zu

starten.

Verwalten von Maschinenkatalogen

Feb 29, 2016

Dieser Abschnitt enthält folgende Themen:

Einführung

Sie können Maschinen in Maschinenkatalogen hinzufügen, entfernen und umbenennen, Maschinenbeschreibungen ändern und die Active Directory-Computerkonten des Katalogs verwalten.

Zur Verwaltung von Katalogen gehören ggf. auch die Aktualisierung des Betriebssystems und der Antivirensoftware der enthaltenen Maschinen, ein Upgrade des Betriebssystems und Änderungen an der Konfiguration.

- Maschinenkataloge mit gepoolt-zufälligen Maschinen, die mit Maschinenerstellungsdienste (MCS) erstellt wurden, können Sie pflegen, indem Sie das Masterimage des Katalogs und dann die Maschinen aktualisieren. So können Sie eine große Anzahl Maschinen effizient aktualisieren. Bei mit Provisioning Services erstellten Maschinen werden Updates über die vDisk verteilt. Weitere Informationen finden Sie in der Dokumentation zu Provisioning Services.
- Bei Katalogen mit statischen (permanent zugewiesenen) oder Remote-PC-Zugriff-Maschinen verwalten Sie Updates an den Maschinen der Benutzer Studio-extern entweder einzeln oder zusammen mit Bereitstellungssoftware von Drittanbietern.

Hinzufügen von Maschinen im Maschinenkatalog

Vorbereitungen:

- Stellen Sie sicher, dass der Virtualisierungshost (Hypervisor oder Clouddienstanbieter) genügend Prozessoren, Arbeitsspeicher und Speicher zur Unterbringung der zusätzlichen Maschinen hat.
- Stellen Sie sicher, dass Sie genügend ungenutzte Active Directory-Computerkonten haben. Wenn Sie bestehende Konten verwenden, können Sie nur so viele Maschinen erstellen, wie Sie Konten haben.
- Wenn Sie Active Directory-Computerkonten für die zusätzlichen Maschinen mit Studio erstellen, müssen Sie die erforderlichen Domänenadministratorrechte haben.

Hinzufügen von Maschinen zum Maschinenkatalog

1. Wählen Sie im Studio-Navigationsbereich **Maschinenkataloge**.
2. Wählen Sie einen Maschinenkatalog und dann im Aktionsbereich **Maschinen hinzufügen**.
3. Legen Sie die Anzahl der hinzuzufügenden virtuellen Maschinen fest.

4. Gibt es nicht genügend Active Directory-Konten für die Zahl der VMs, die Sie hinzufügen möchten, wählen Sie die Domäne und den Speicherort, an dem Konten erstellt werden sollen. Legen Sie ein Kontobenennungsschema mit Hashmarkierungen zur Kennzeichnung der Platzierung sequenzieller Zahlen bzw. Buchstaben fest. Vergessen Sie nicht den Schrägstrich (/) im Namen von Organisationseinheiten. Namen dürfen nicht mit einer Zahl beginnen. Beispiel: Das Benennungsschema "PC-Vertrieb-##" (und Aktivierung von 0-9) bewirkt eine Benennung der Computerkonten als "PC-Vertrieb-01", "PC-Vertrieb-02", "PC-Vertrieb-03" usw.
5. Wenn Sie bestehende Active Directory-Konten verwenden, navigieren Sie zu den Konten oder klicken Sie auf **Importieren** und geben Sie eine CSV-Datei mit Kontonamen an. Stellen Sie sicher, dass Sie ausreichend Konten für die hinzuzufügenden Maschinen haben. Da diese Konten von Studio verwaltet werden, gestatten Sie Studio, die Kennwörter für alle Konten zurückzusetzen, oder geben Sie das Kontokennwort an. Dieses 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 Studio schließen.

Löschen von Maschinen aus einem Maschinenkatalog

Wenn Sie eine Maschine aus einem Maschinenkatalog löschen, können Benutzer nicht mehr darauf zugreifen. Vergewissern Sie sich vor dem Löschen daher, dass folgende Bedingungen erfüllt sind:

- Die Benutzerdaten wurden gesichert oder werden nicht mehr benötigt.
- Alle Benutzer sind abgemeldet. Durch das Aktivieren des Wartungsmodus wird verhindert, dass neue Verbindungen mit einer Maschine hergestellt werden.
- Die Maschinen sind ausgeschaltet.

Löschen von Maschinen aus einem Maschinenkatalog

1. Wählen Sie im Studio-Navigationsbereich **Maschinenkataloge** aus.
2. Wählen Sie einen Katalog und dann im Aktionsbereich **Maschinen anzeigen**.
3. Wählen Sie eine oder mehrere Maschinen und dann im Aktionsbereich **Löschen**.

Wählen Sie aus, ob die Maschinen wirklich gelöscht werden sollen. Falls ja, geben Sie an, ob die zugehörigen Active Directory-Konten beibehalten, deaktiviert oder gelöscht werden sollen.

Ändern einer Maschinenkatalogbeschreibung oder der Remote-PC-Zugriff-Einstellungen

1. Wählen Sie im Studio-Navigationsbereich **Maschinenkataloge**.
2. Wählen Sie einen Katalog und dann im Aktionsbereich **Maschinenkatalog bearbeiten**.
3. (Nur bei Remote-PC-Zugriff-Katalogen) Auf der Seite **Energieverwaltung** können Sie die Energieverwaltungseinstellungen ändern und eine Energieverwaltungsverbindung auswählen. Verwenden Sie die Seite **Organisationseinheiten** zum Hinzufügen und Entfernen von Active Directory-Organisationseinheiten.
4. Ändern Sie auf der Seite **Beschreibung** die Beschreibung des Maschinenkatalogs.

Umbenennen von Maschinenkatalogen

1. Wählen Sie im Studio-Navigationsbereich **Maschinenkataloge**.
2. Wählen Sie einen Katalog und dann im Aktionsbereich **Maschinenkatalog umbenennen**.
3. Geben Sie den neuen Namen ein.

Verschieben eines Maschinenkatalogs in eine andere Zone

Wenn eine Site mehrere Zonen enthält, können Sie Maschinenkataloge von Zone zu Zone verschieben.

Vorsicht: Wenn Sie einen Maschinenkatalog aus dem Hypervisor oder Clouddienst mit den zugehörigen VMs in eine andere Zone verschieben, kann sich dies negativ auf die Leistung auswirken.

1. Wählen Sie im Studio-Navigationsbereich **Maschinenkataloge**.
2. Wählen Sie einen Katalog und dann im Aktionsbereich **Verschieben**.
3. Wählen Sie die Zone aus, in die Sie den Katalog verschieben möchten.

Löschen eines Maschinenkatalogs

Vor dem Löschen eines Maschinenkatalogs müssen Sie Folgendes sicherstellen:

- Alle Benutzer sind abgemeldet und es werden keine getrennten Sitzungen ausgeführt.
- Der Wartungsmodus ist für alle Maschinen in dem Katalog aktiviert, damit keine neuen Verbindungen hergestellt werden können.
- Alle Maschinen in dem Katalog sind ausgeschaltet.
- Dem Katalog ist keine Bereitstellungsgruppe zugewiesen, d. h. keine Bereitstellungsgruppe enthält Maschinen aus dem Katalog.

Löschen eines Maschinenkatalogs

1. Wählen Sie im Studio-Navigationsbereich **Maschinenkataloge**.
2. Wählen Sie einen Katalog und dann im Aktionsbereich **Maschinenkatalog löschen**.
3. Geben Sie an, ob die Maschinen in dem Katalog gelöscht werden sollen. Falls ja, geben Sie an, ob die zugehörigen Active Directory-Computerkonten beibehalten, deaktiviert oder gelöscht werden sollen.

Verwalten von Active Directory-Computerkonten in einem Maschinenkatalog

Zum Verwalten von Active Directory-Konten in einem Maschinenkatalog haben Sie folgende Möglichkeiten:

- Freigeben nicht verwendeter Maschinenkonten durch Entfernen von Active Directory-Computerkonten aus Desktopbetriebssystem- und Serverbetriebssystemmaschinenkatalogen. Diese Konten können dann für andere Maschinen verwendet werden.
- Hinzufügen von Konten, damit beim Hinzufügen weiterer Maschinen zum Katalog Computerkonten bereit stehen. Vergessen Sie nicht den Schrägstrich (/) im Namen von Organisationseinheiten.

Verwalten von Active Directory-Konten

1. Wählen Sie im Studio-Navigationsbereich **Maschinenkataloge**.
2. Wählen Sie einen Maschinenkatalog und dann im Aktionsbereich **Active Directory-Konten verwalten**.
3. Entscheiden Sie, ob Sie Computerkonten hinzufügen oder löschen möchten. Wenn Sie Konten hinzufügen, geben Sie an, wie mit den Kennwörtern verfahren werden soll: Setzen Sie entweder alle zurück oder geben Sie ein für alle Konten geltendes Kennwort ein. Sie können die Kennwörter zurückzusetzen, wenn Sie

die aktuellen Kennwörter nicht kennen. Zum Zurücksetzen von Kennwörtern müssen Sie die entsprechende Berechtigung haben. Wenn Sie ein Kennwort eingeben, wird das Kennwort von Konten beim Importieren geändert. Wenn Sie ein Konto löschen, legen Sie fest, ob das Konto in Active Directory beibehalten, deaktiviert oder gelöscht werden soll.

Hinweis: Sie können auch angeben, ob Active Directory-Konten beibehalten, deaktiviert oder gelöscht werden sollen, wenn Sie Maschinen aus einem Katalog entfernen oder einen Katalog löschen.

Aktualisieren von Maschinenkatalogen

Citrix empfiehlt, vor dem Durchführen von Updates von Maschinen in einem Katalog Kopien oder Snapshots der Masterimages zu speichern. In der Datenbank wird von jedem Masterimage eines Maschinenkatalogs ein historischer Datensatz beibehalten. Bei Problemen mit Updates, die auf den Benutzerdesktops bereitgestellt wurden, können Sie das Masterimage auf die vorherige Version zurücksetzen und die Downtime für Benutzer minimieren. Masterimages dürfen nicht gelöscht, verschoben oder umbenannt werden, da ansonsten Kataloge nicht auf ihre Verwendung zurückgesetzt werden können.

Bei Maschinenkatalogen, die Provisioning Services verwenden, müssen Sie eine neue vDisk veröffentlichen, um Änderungen auf den Katalog anzuwenden. Informationen hierzu finden Sie in der Dokumentation zu Provisioning Services.

Nachdem eine Maschine aktualisiert wurde, wird sie automatisch neu gestartet.

Aktualisieren oder Erstellen eines Masterimages

Tipp: Benötigen Sie Informationen zum Verbindungstyp? Die finden Sie hier.

Bevor Sie einen Maschinenkatalog aktualisieren, aktualisieren Sie zunächst ein vorhandenes Masterimage oder erstellen Sie ein neues auf dem Hypervisor.

1. Erstellen Sie auf dem Hypervisor bzw. im Clouddienst einen Snapshot der aktuellen VM und geben Sie diesem einen aussagekräftigen Namen. Der Snapshot kann notfalls zur Wiederherstellung (Rollback) der Maschinen in dem Katalog verwendet werden.
2. Falls erforderlich, schalten Sie das Masterimage ein und melden Sie sich an.
3. Installieren Sie Updates bzw. nehmen Sie die erforderlichen Änderungen am Masterimage vor.
4. Wenn das Masterimage eine persönliche vDisk verwendet, aktualisieren Sie den Bestand.
5. Wenden Sie die in den folgenden Leitfäden aufgeführten Optimierungen auf Ihre Umgebung an: Windows 7 Optimization Guide und Windows 8/8.1 Virtual Desktop Optimization Guide.
6. Schalten Sie die virtuelle Maschine aus.
7. Erstellen Sie einen Snapshot der VM und geben Sie diesem einen aussagekräftigen Namen, der bei der Aktualisierung des Katalogs in Studio erkannt wird. Obwohl Studio einen Snapshot erstellen kann, empfiehlt Citrix, dass Sie einen Snapshot mit der Hypervisor-Verwaltungskonsole erstellen und dann den Snapshot in Studio auswählen. Dadurch können Sie statt eines automatisch erstellten Namens einen aussagekräftigen Namen und eine Beschreibung zuweisen. Bei GPU-Masterimages können Sie das Masterimage nur über die XenServer XenCenter-Konsole ändern.

Aktualisieren des Katalogs

Vorbereiten und Verteilen des Updates auf allen Maschinen in einem Katalog

1. Wählen Sie im Studio-Navigationsbereich **Maschinenkataloge**.
2. Wählen Sie eine Maschine und dann im Aktionsbereich **Maschinen aktualisieren**.
3. Wählen Sie auf der Seite **Masterimage** den Host und das gewünschte Masterimage.
4. Legen Sie auf der Seite **Rolloutstrategie** fest, wann die Aktualisierung der Maschinen im Maschinenkatalog erfolgen soll: beim nächsten Herunterfahren oder sofort. Details hierzu finden Sie weiter unten.
5. Überprüfen Sie die Informationen auf der Seite **Zusammenfassung** und klicken Sie dann auf **Fertig stellen**. Jede Maschine wird nach erfolgter Aktualisierung automatisch neu gestartet.

Tipp: Wenn Sie einen Katalog direkt mit dem PowerShell-SDK anstelle von Studio aktualisieren, können Sie alternativ zu einem Image bzw. einem Image-Snapshot eine Hypervisorvorlage (VMTemplates) angeben.

Rolloutstrategie

Ein Update des Images beim nächsten Herunterfahren wird angeboten, wenn Sie den Citrix Connector für System Center Configuration Manager verwenden.

Wenn Sie das Image sofort aktualisieren, konfigurieren Sie eine Zeit und Benachrichtigungen für die Verteilung.

- **Verteilungszeit:** Sie können alle Maschinen zur gleichen Zeit aktualisieren lassen oder eine Zeitdauer festlegen, während derer die Aktualisierung aller Maschinen im Katalog stattfinden soll. Ein interner Algorithmus bestimmt, wann welche Maschine während dieses Zeitraums aktualisiert und neu gestartet wird.
- **Benachrichtigung:** Wählen Sie in dieser Dropdownliste aus, ob auf den Maschinen eine Meldung angezeigt werden soll, bevor das Update beginnt. In der Standardeinstellung wird keine Meldung angezeigt. Wenn Sie festlegen, dass 15 Minuten vor dem Update eine Meldung angezeigt wird, können Sie in der rechten Dropdownliste vorgeben, dass die Meldung alle fünf Minuten nach der Erstanzeige wiederholt werden soll. Standardmäßig wird die Meldung nicht wiederholt angezeigt. Sofern Sie kein gleichzeitiges Update aller Maschinen festgelegt haben, wird die Meldung auf jeder Maschine zu der von dem internen Algorithmus berechneten Zeit vor dem Update angezeigt.

Rollback eines Updates

Nach Bereitstellung eines aktualisierten/neuen Masterimages können Sie diese mit einem Rollback rückgängig machen. Dies kann erforderlich sein, wenn Probleme bei den aktualisierten Maschinen auftreten. Bei einem Rollback werden die Maschinen in dem Katalog auf das letzte funktionierende Image zurückgesetzt. Neue Features, die das neue Image erfordern, stehen dann nicht mehr zur Verfügung. Bei einem Rollback einer Maschine ist ein Neustart erforderlich.

1. Wählen Sie im Studio-Navigationsbereich **Maschinenkataloge** aus.
2. Wählen Sie den Maschinenkatalog und dann im Aktionsbereich **Rollback für Maschinenupdate**.
3. Legen Sie fest, wann das ältere Masterimage auf die Maschinen angewendet werden soll (gemäß den Rollout-Anweisungen oben).

Das Rollback wird nur auf Maschinen angewendet, die zurückgesetzt werden müssen. Benutzer von Maschinen, die nicht mit dem neuen/aktualisierten Masterimage aktualisiert wurden (z. B. weil sie sich nicht abgemeldet hatten), erhalten keine Meldung und müssen sich nicht abmelden.

Durchführen eines Upgrades eines Maschinenkatalogs und Rückgängigmachen eines Upgrades

Aktualisieren Sie den Maschinenkatalog nach dem Upgrade der VDAs auf den Maschinen auf eine neuere Version. Citrix empfiehlt das Upgrade aller VDAs auf die aktuelle Version, damit Zugriff auf alle neuen Features besteht.

Upgradevorbereitung:

- Wenn Sie Provisioning Services verwenden, aktualisieren Sie die VDA-Version in der Provisioning Services Console.
- Starten Sie die aktualisierten Maschinen, damit sie sich bei dem Controller registrieren. Auf diese Weise kann Studio feststellen, dass die Maschinen im Maschinenkatalog aktualisiert werden müssen.

Upgrade eines Maschinenkatalogs durchführen

1. Wählen Sie im Studio-Navigationsbereich **Maschinenkataloge**.

2. Wählen Sie den Katalog aus. Auf der Registerkarte "Details" im unteren Bereich werden Versionsinformationen angezeigt.
3. Wählen Sie **Katalog aktualisieren**. Wenn Studio erkennt, dass für den Maschinenkatalog ein Upgrade erforderlich ist, wird eine Meldung angezeigt. Folgen Sie den Anweisungen. Kann eine Maschine nicht aktualisiert werden, wird eine Meldung mit einer Erläuterung der Ursache des Problems angezeigt. Citrix empfiehlt, dass Sie alle Maschinenprobleme beheben, bevor Sie den Maschinenkatalog aktualisieren, damit alle Maschinen einwandfrei funktionieren.

Wenn das Katalogupgrade abgeschlossen ist, können Sie Maschinen auf ihren vorherigen Zustand zurücksetzen, indem Sie den Maschinenkatalog und dann im Aktionsbereich **Rückgängig machen** wählen.

Hinweis: Für Windows XP- und Windows Vista-Maschinen muss eine ältere VDA-Version verwendet werden. Die Verwendung der neuesten Produktfeatures ist hier nicht möglich. Wenn Sie diese Maschinen nicht auf ein derzeit unterstütztes Windows-Betriebssystem aktualisieren können, empfiehlt Citrix, sie in einem separaten Maschinenkatalog zu führen.

Erstellen von Bereitstellungsgruppen

Feb 29, 2016

Eine Bereitstellungsgruppe ist eine Sammlung von Maschinen aus einem oder mehreren Maschinenkatalogen. Die Bereitstellungsgruppe gibt an, welche Benutzer diese Maschinen verwenden können und welche Anwendungen bzw. Desktops für diese Benutzer verfügbar sein sollen.

Das Erstellen einer Bereitstellungsgruppe ist nach dem Erstellen einer Site und eines Maschinenkatalogs der nächste Schritt beim Konfigurieren der Bereitstellung. Später können Sie die anfänglichen Einstellungen der ersten Bereitstellungsgruppe ändern und weitere Bereitstellungsgruppen erstellen. Es gibt Features und Einstellungen, die Sie nur beim Bearbeiten einer Bereitstellungsgruppe, nicht aber beim Erstellen konfigurieren können.

In Studio:

- Wenn Sie eine Site und einen Maschinenkatalog, jedoch noch keine Bereitstellungsgruppe erstellt haben, führt Studio Sie zum richtigen Startpunkt für die Erstellung einer Bereitstellungsgruppe.
- Wenn Sie bereits eine Bereitstellungsgruppe erstellt haben und eine weitere erstellen möchten, wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen** und dann im Aktionsbereich **Bereitstellungsgruppe erstellen**.

Der Assistent führt Sie durch die nachfolgend beschriebenen Einstellungen.

Maschinen

Wählen Sie einen Maschinenkatalog und die Anzahl der Maschinen, die Sie aus dem Katalog verwenden möchten.

Gut zu wissen:

- Mindestens eine Maschine in dem ausgewählten Katalog muss unbenutzt bleiben.
- Ein Maschinenkatalog kann in mehreren Bereitstellungsgruppen angegeben werden, eine Maschine kann jedoch nur in einer Bereitstellungsgruppe verwendet werden.
- Eine Bereitstellungsgruppe kann Maschinen aus mehreren Maschinenkatalogen verwenden, diese Kataloge müssen allerdings Maschinen desselben Typs enthalten (Serverbetriebssystemmaschinen oder Desktopbetriebssystemmaschinen oder Remote-PC-Zugriff-Maschinen). Sie können also in einer Bereitstellungsgruppe nicht verschiedene Maschinentypen mischen. Umfasst Ihre Bereitstellung Maschinenkataloge für Windows-Maschinen und solche für Linux-Maschinen, darf eine Bereitstellungsgruppe nur Maschinen eines Betriebssystems enthalten.
- Citrix empfiehlt, dass Sie alle Maschinen mit der neuesten VDA-Version installieren oder aktualisieren und dann das Upgrade von Maschinenkatalogen und Bereitstellungsgruppen nach Bedarf durchführen. Wenn Sie beim Erstellen einer Bereitstellungsgruppe Maschinen mit verschiedenen VDA-Versionen auswählen, ist die resultierende Bereitstellungsgruppe kompatibel mit der ältesten VDA-Version. (= *Funktionsebene* der Gruppe). Das bedeutet, dass einige Features, die neuere VDA-Versionen erfordern, in der Bereitstellungsgruppe möglicherweise nicht zur Verfügung stehen. Wenn auf einer der ausgewählten Maschinen beispielsweise ein VDA der Version 7.1 und auf den anderen die aktuelle VDA-Version installiert ist, können alle Maschinen der Gruppe nur die Features verwenden, die vom VDA der Version 7.1 unterstützt werden.
- Alle Maschinen in einem Remote-PC-Zugriff-Maschinenkatalog werden automatisch einer Bereitstellungsgruppe zugewiesen. Wenn Sie eine Remote-PC-Zugriff-Site erstellen, werden automatisch ein Maschinenkatalog unter dem Namen "Remote-PC-Zugriff-Maschinen" und eine Bereitstellungsgruppe unter dem Namen "Remote-PC-Zugriff-

Desktops" erstellt.

Bereitstellungstyp

Geben Sie an, was eine Bereitstellungsgruppe bietet: nur Desktops, nur Anwendungen oder beides. Bereitstellungsgruppen mit statischen Desktopbetriebssystemmaschinen können keine Desktops und Anwendungen zugleich enthalten.

Benutzer

Geben Sie die Benutzer und Benutzergruppen an, die die Anwendungen und/oder Desktops in der Bereitstellungsgruppe verwenden können.

Festlegung von Benutzerlisten

Active Directory-Benutzerlisten werden angegeben, wenn Sie Folgendes erstellen oder bearbeiten:

- Benutzerzugriffsliste für eine Site, die nicht über Studio konfiguriert wird. Standardmäßig umfasst die Anwendungsanspruch-Richtlinienregel alle Benutzer (Einzelheiten s. BrokerAppEntitlementPolicyRule-Cmdlets des PowerShell-SDKs.
- Bereitstellungsgruppen
- Anwendungen

Die Liste der Benutzer, die Zugriff auf eine Anwendung über StoreFront haben, wird aus der Schnittmenge der oben angegebenen Benutzerlisten erstellt. Zum Einschränken der Fähigkeit zum Starten von "Anwendung A" auf Benutzer der Finanzabteilung stehen Ihnen beispielsweise folgende Möglichkeiten offen:

- Verwenden der Standardanwendungsanspruch-Richtlinienregel, die für alle Benutzer gilt
- Konfigurieren der Benutzerliste der Bereitstellungsgruppe, sodass alle Benutzer die Anwendungen der Bereitstellungsgruppe verwenden können
- Konfigurieren der Eigenschaften von Anwendung A, sodass sie nur Benutzern der Finanzabteilung angezeigt wird

Authentifizierte und nicht authentifizierte Benutzer

Es gibt zwei Benutzertypen: authentifizierte und nicht authentifizierte Benutzer (nicht authentifizierte Benutzer werden auch als "anonyme" Benutzer bezeichnet). Konfigurieren einen oder beide Typen in einer Bereitstellungsgruppe konfigurieren.

- **Authentifiziert**: Die Benutzer und Gruppenmitglieder, die Sie namentlich festlegen, müssen für den Zugriff auf Anwendungen und Desktops in StoreFront oder Citrix Receiver Anmeldeinformationen, z. B. Smartcard oder Benutzernamen und Kennwort, angeben. (Bei Bereitstellungsgruppen mit Desktopbetriebssystemmaschinen können Sie eine Liste der Benutzer später unter Bearbeiten der Bereitstellungsgruppe importieren.)
- **Nicht authentifiziert (anonym):** Bei Bereitstellungsgruppen mit Serverbetriebssystemmaschinen können Sie Benutzern Zugriff auf Anwendungen und Desktops gewähren, ohne dass die Benutzer Anmeldeinformationen in StoreFront oder Citrix Receiver eingeben müssen. Beispiel: Beim Zugriff über einen Kiosk werden für die Anwendung Anmeldeinformationen benötigt, nicht aber für das Citrix Zugriffsportal und Citrix Tools. Eine Gruppe anonymer Benutzer wird erstellt, wenn Sie den ersten Delivery Controller installieren.

  Damit nicht authentifizierten Benutzern Zugriff erteilt werden kann, muss auf jeder Maschine in der

Bereitstellungsgruppe ein VDA für Windows-Serverbetriebssysteme (mindestens Version 7.6) installiert sein. Wenn nicht authentifizierte Benutzer aktiviert sind, müssen Sie einen StoreFront-Store ohne Authentifizierung haben.

Nicht authentifizierte Benutzerkonten werden bei Bedarf beim Start einer Sitzung erstellt und "AnonXYZ" genannt (XYZ ist ein eindeutiger 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.

Die folgende Tabelle enthält die Optionen der Seite "Benutzer":

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

Anwendungen

Es wird eine Liste der Anwendungen angezeigt. Wählen Sie eine oder mehrere Anwendungen aus.

- Wurde der ausgewählte Maschinenkatalog mit einem Masterimage mit Anwendungen erstellt, wird eine Liste der Anwendungen angezeigt, die auf einer von diesem Image erstellten Maschine erkannt wurden.
- Wenn Sie App-V-Serverinformationen konfiguriert haben und für den App-V-Server Pakete verfügbar sind, wird eine Liste der betreffenden Anwendungen angezeigt.
- Sie können Anwendungen außerdem manuell hinzufügen. Geben Sie den Pfad zur ausführbaren Datei, das Arbeitsverzeichnis, optionale Befehlszeilenargumente und Anzeigenamen für Administratoren und Benutzer an.

Gut zu wissen:

- Sie können Anwendungen für Remote-PC-Zugriff-Bereitstellungsgruppen erstellen.
- Standardmäßig werden neue Anwendungen, die Sie hinzufügen, in einem Ordner mit dem Namen **Applications** abgelegt. Sie können einen anderen Ordner angeben. Einzelheiten finden Sie im Artikel Verwalten von Anwendungen.
- Sie können die Eigenschaften von Anwendungen im Assistenten zum Erstellen von Bereitstellungsgruppe ändern oder auch später. Weitere Informationen finden Sie im Artikel Verwalten von Anwendungen.
- Wenn Sie eine Anwendung hinzufügen und es bereits eine Anwendung mit dem gleichen Namen im gleichen Ordner gibt, werden Sie aufgefordert, die neue Anwendung umzubenennen. Wenn Sie dies ablehnen, wird die Anwendung mit einem Suffix hinzugefügt, sodass ihr Name innerhalb des Ordners eindeutig ist.
- Wenn Sie zwei Anwendungen mit dem gleichen Namen für die gleichen Benutzern hinzufügen, ändern Sie die Eigenschaft

Anwendungsname (Benutzer), sonst wird den Benutzern der Name in Receiver doppelt angezeigt.

StoreFront

Wählen Sie StoreFront-URLs, die von den auf allen Maschinen in der Bereitstellungsgruppe installierten Citrix Receiver-Instanzen verwendet werden sollen (bzw. fügen Sie diese URLs hinzu). Sie können StoreFront-Serveradressen auch später festlegen, indem Sie im Studio-Navigationsbereich **Konfiguration > StoreFront** auswählen.

Verwalten von Bereitstellungsgruppen

Feb 29, 2016

Einführung

Nach dem Erstellen einer Bereitstellungsgruppe können Sie Einstellungen ändern, die Sie beim Erstellen der Gruppe gewählt haben, und weitere Einstellungen konfigurieren, die beim Erstellen von Bereitstellungsgruppen nicht zur Verfügung stehen.

Informationen zur Verwaltung von Bereitstellungsgruppen finden Sie in den folgenden Artikeln:

- Verwalten von Anwendungen
- Verwalten von Maschinen
- Verwalten von Sitzungen

Ändern der Benutzereinstellungen für eine Bereitstellungsgruppe

Der Name dieser Seite kann **Benutzereinstellungen** oder **Grundeinstellungen** lauten.

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und dann im Aktionsbereich **Bereitstellungsgruppe bearbeiten**.
3. Ändern Sie auf der Seite **Benutzereinstellungen** (bzw. **Grundeinstellungen**), die folgenden Optionen nach Bedarf und klicken Sie dann auf **OK** oder **Anwenden**.

Wenn Sie	**Beschreibung**
Beschreibung	Text in StoreFront, der Benutzern angezeigt wird
Bereitstellungsgruppe aktivieren	Zeigt an, ob die Bereitstellungsgruppe aktiviert ist.
Desktops pro Benutzer	(Nur zugewiesene Desktopbetriebssystemmaschinen) Maximale Anzahl freigegebener Desktops, die ein Benutzer gleichzeitig aktiv haben darf. Bei Bereitstellungen mit Zuweisung bei der ersten Verwendung gibt dieser Wert an, wie viele Desktops Benutzer sich selbst zuweisen können.
Zeitzone	
Secure ICA aktivieren	Schützt die Kommunikation zwischen Maschinen in der Bereitstellungsgruppe mit SecureICA, wodurch das ICA-Protokoll verschlüsselt wird (Standardverschlüsselungsgrad ist 128 Bit, dieser kann mit dem SDK geändert werden). Citrix empfiehlt die Verwendung zusätzlicher

	Verschlüsselungsmethoden, z. B. TLS-Verschlüsselung, wenn Datenübertragungen über öffentliche Netzwerke stattfinden. Bei SecureICA wird die Datenintegrität auch nicht geprüft.

Hinzufügen und Entfernen von Benutzern zu bzw. aus Bereitstellungsgruppen

Ausführliche Informationen zu Benutzern finden Sie im Abschnitt "Benutzer" des Artikels Erstellen von Bereitstellungsgruppen.

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und dann im Aktionsbereich **Bereitstellungsgruppe bearbeiten**.
3. Zum Hinzufügen von Benutzern klicken Sie auf der Seite **Benutzer** auf **Hinzufügen** und geben Sie die Benutzer an, die Sie hinzufügen möchten. Zum Entfernen von Benutzern wählen Sie mindestens einen Benutzer aus und klicken Sie auf **Entfernen**. Sie können auch den Zugriff nicht authentifizierter Benutzer über das entsprechende Kontrollkästchen aktivieren oder deaktivieren.
4. Klicken Sie auf **OK** oder **Übernehmen**.

Importieren und Exportieren von Benutzerlisten

Bei Bereitstellungsgruppen mit physischen Desktopbetriebssystemmaschinen können Sie Benutzerinformationen nach dem Erstellen der Bereitstellungsgruppe aus einer CSV-Datei importieren. Sie können Benutzerinformationen auch in eine CSV-Datei exportieren. Die CSV-Datei kann Daten aus einer vorherigen Produktversion enthalten.

Die erste Zeile der CSV-Datei muss durch Trennzeichen getrennte Spaltenüberschriften (in beliebiger Reihenfolge) enthalten, z. B. ADComputerAccount, AssignedUser, VirtualMachine und HostId. Die nachfolgenden Zeilen enthalten durch Trennzeichen getrennte Daten. Die Einträge unter ADComputerAccount können allgemeine Namen, IP-Adressen Distinguished Names oder Domänen-/Computernamenpaare sein.

Importieren oder Exportieren von Benutzerinformationen

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Bereitstellungsgruppe und dann im Aktionsbereich **Bereitstellungsgruppe bearbeiten**.
3. Klicken Sie auf der Seite **Maschinenzuteilung** auf **Liste importieren** bzw. **Liste exportieren** und navigieren Sie zum Speicherort der Datei.

Ändern des Bereitstellungstyps von Bereitstellungsgruppen

Der Bereitstellungstyp bestimmt, was eine Gruppe bereitstellen kann: Anwendungen, Desktops oder beides.

Bevor Sie eine Bereitstellungsgruppe des Typs **Nur Anwendungen** oder **Desktops und Anwendungen** in eine Bereitstellungsgruppe des Typs **Nur Desktops** ändern, löschen Sie alle Anwendungen aus der Bereitstellungsgruppe.

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen**.

2. Wählen Sie eine Bereitstellungsgruppe und dann im Aktionsbereich **Bereitstellungsgruppe bearbeiten**.
3. Wählen Sie auf der Seite **Bereitstellungstyp** den gewünschten Bereitstellungstyp.
4. Klicken Sie auf **OK** oder **Übernehmen**.

Ändern der StoreFront-Informationen

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und dann im Aktionsbereich **Bereitstellungsgruppe bearbeiten**.
3. Wählen Sie auf der Seite **StoreFront** die StoreFront-URLs aus (bzw. fügen Sie sie hinzu), die von der auf jeder Maschine in der Bereitstellungsgruppe installierten Citrix Receiver-Instanz verwendet werden sollen.
4. Klicken Sie auf **OK** oder **Übernehmen**.

Sie können die StoreFront-Serveradresse auch festlegen, indem Sie im Studio-Navigationsbereich **Konfiguration > StoreFront** auswählen.

Durchführen eines Upgrades einer Bereitstellungsgruppe und Rückgängigmachen eines Bereitstellungsgruppenupgrades

Nach dem Upgrade der VDAs auf Maschinen einer Bereitstellungsgruppe sowie den Maschinen in den von ihr verwendeten Maschinenkatalogen führen Sie ein Upgrade der Bereitstellungsgruppe durch.

Führen Sie vor dem Upgrade der Bereitstellungsgruppe folgende Schritte durch:

- Wenn Sie Provisioning Services verwenden, aktualisieren Sie die VDA-Version in der Provisioning Services Console.
- Starten Sie die Maschinen mit dem aktualisierten VDA, damit sie sich bei dem Delivery Controller registrieren können. Dadurch wird Studio darüber informiert, welche Elemente in der Bereitstellungsgruppe aktualisiert werden müssen.
- Wenn Sie ältere VDA-Versionen weiterverwenden müssen, sind neuere Produktfeatures ggf. nicht verfügbar. Weitere Informationen finden Sie in den Artikeln zu Upgrades.

Bereitstellungsgruppen aktualisieren:

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und dann im Aktionsbereich **Upgrade von Bereitstellungsgruppe durchführen**. Die Aktion **Upgrade von Bereitstellungsgruppe durchführen** wird nur angezeigt, wenn Studio aktualisierte VDAs erkennt.

Vor dem Starten des Upgrades wird in Studio gemeldet, welche Maschinen nicht aktualisiert werden können (falls es solche gibt) und warum. Sie können das Upgrade dann abbrechen, die Ursachen beheben und das Upgrade erneut starten.

Wenn das Upgrade abgeschlossen ist, können Sie Maschinen auf ihren vorherigen Zustand zurücksetzen, indem Sie die Bereitstellungsgruppe und dann im Aktionsbereich **Rückgängig machen** wählen.

Verwalten von Remote-PC-Zugriff-

Bereitstellungsgruppen

Wenn eine Maschine eines Remote-PC-Zugriff-Maschinenkatalogs keinem Benutzer zugewiesen wurde, weist Studio sie vorübergehend einer Bereitstellungsgruppe zu, die dem Maschinenkatalog zugeordnet ist. Dadurch kann sie später einem Benutzer zugewiesen werden.

Die Zuweisung der Bereitstellungsgruppe zum Maschinenkatalog ist mit einem Prioritätswert verbunden. Die Priorität bestimmt, welcher Bereitstellungsgruppe eine Maschine zugewiesen ist, die bei der Registrierung beim System oder wenn ein Benutzer eine Maschinenzuweisung benötigt: je geringer der Wert, desto höher die Priorität. Wenn ein Remote-PC-Zugriff-Maschinenkatalog mehrere Bereitstellungsgruppenzuweisungen hat, wird die mit der höchsten Priorität vom System ausgewählt. Sie können die Priorität mit dem PowerShell-SDK festlegen.

Beim Erstellen eines Remote-PC-Zugriff-Maschinenkatalogs wird dieser einer Bereitstellungsgruppe zugeordnet. Dies bedeutet, dass dem Maschinenkatalog später hinzugefügte Maschinenkonten oder Organisationseinheiten in der Bereitstellungsgruppe hinzugefügt werden können. Die Zuordnung kann deaktiviert oder aktiviert werden.

Zuordnung eines Remote-PC-Zugriff-Maschinenkatalogs zu einer Bereitstellungsgruppe hinzufügen oder entfernen:

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Remote-PC-Zugriff-Gruppe aus.
3. Wählen Sie im Abschnitt "Details" die Registerkarte **Maschinenkataloge** und dann einen Remote-PC-Zugriff-Maschinenkatalog.
4. Um eine Zuordnung hinzuzufügen oder wiederherzustellen, wählen Sie **Desktops hinzufügen**. Zum Entfernen einer Zuordnung wählen Sie **Zuordnung entfernen**.

Verwalten von Maschinen in Bereitstellungsgruppen

Feb 29, 2016

Einführung

Sie können auch Maschinen in einem Maschinenkatalog verwalten. Informationen hierzu finden Sie unter Verwalten von Maschinenkatalogen.

Herunterfahren und Neustart von Maschinen

Dieser Vorgang wird für Remote-PC-Zugriff-Maschinen nicht unterstützt.

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Gruppe und dann im Aktionsbereich **Maschinen anzeigen**.
3. Wählen Sie die Maschine und anschließend im Aktionsbereich eine der folgenden Optionen (einige Optionen sind je nach Maschinenzustand ggf. nicht verfügbar):

- **Herunterfahren erzwingen**: Das Abschalten der Maschine wird erzwungen und die Liste der Maschinen wird aktualisiert.
- **Neu starten**: Das Betriebssystem wird heruntergefahren und die Maschine dann neu gestartet. Wenn das Betriebssystem diese Aufgaben nicht ausführen kann, bleibt die Maschine im aktuellen Zustand.
- **Neustart erzwingen** Das Betriebssystem wird heruntergefahren und die Maschine dann neu gestartet.
- **Anhalten**: Die Maschine wird angehalten, ohne sie herunterzufahren, und die Liste der Maschinen aktualisiert.
- **Herunterfahren**: Das Betriebssystem wird heruntergefahren.

Wird bei Aktionen ohne Erzwingen eine Maschine nicht innerhalb von 10 Minuten heruntergefahren, wird sie ausgeschaltet. Wenn Windows versucht, während des Herunterfahrens Updates zu installieren, besteht die Gefahr, dass die Maschine ausgeschaltet wird, bevor die Updates abgeschlossen sind.

Citrix empfiehlt, dass Sie das Herunterfahren von Desktopbetriebssystemmaschinen durch Benutzer während einer Sitzung nicht zulassen. Einzelheiten finden Sie in der Microsoft-Dokumentation zu Richtlinien.

Energieverwaltung für Maschinen

Die Energieverwaltung ist nur bei virtuellen Desktopbetriebssystemmaschinen, nicht aber bei physischen Maschinen (einschließlich Remote-PC-Zugriff-Maschinen) möglich. Desktopbetriebssystemmaschinen mit GPU-Funktionen können nicht angehalten werden, sodass Energieverwaltungsvorgänge fehlschlagen. Für Serverbetriebssystemmaschinen können Sie einen Neustartzeitplan erstellen. Das Verfahren wird im vorliegenden Abschnitt beschrieben.

In Bereitstellungsgruppen mit gepoolten Maschinen können virtuelle Desktopbetriebssystemmaschinen einen der folgenden Zustände annehmen:

- Zufällig zugewiesen und in Verwendung
- Nicht zugewiesen und nicht verbunden

In Bereitstellungsgruppen mit statischen Maschinen können virtuelle Desktopbetriebssystemmaschinen einen der folgenden Zustände aufweisen:

- Dauerhaft zugeordnet und in Verwendung
- Dauerhaft zugewiesen und nicht verbunden (aber bereit für Verbindungen)
- Nicht zugewiesen und nicht verbunden

Statische Bereitstellungsgruppen enthalten im Normalbetrieb sowohl dauerhaft zugewiesene als auch nicht zugewiesene Maschinen. Anfangs sind alle Maschinen nicht zugewiesen (außer beim Erstellen der Bereitstellungsgruppe manuell zugewiesene Maschinen). Wenn Benutzer eine Verbindung herstellen, werden Maschinen dauerhaft zugewiesen. Die Energieverwaltung ist bei nicht zugewiesenen Maschinen in den Bereitstellungsgruppen vollständig, bei dauerhaft zugewiesenen Maschinen nur teilweise möglich.

Pools und Puffer: Unter einem Pool versteht man bei gepoolten Bereitstellungsgruppen und statischen Bereitstellungsgruppen mit nicht zugewiesenen Maschinen eine Gruppe nicht zugewiesener (oder temporär zugewiesener) Maschinen, die eingeschaltet bleiben und mit denen Benutzer eine Verbindung herstellen können (eine Maschine ist direkt nach der Anmeldung verfügbar). Die Poolgröße (d. h. die Zahl der Maschinen, die eingeschaltet bleiben) kann abhängig von der Tageszeit konfiguriert werden. Verwenden Sie zum Konfigurieren des Pools bei statischen Bereitstellungsgruppen das SDK.

Ein Puffer ist eine zusätzliche Gruppe nicht zugewiesener Maschinen, die eingeschaltet werden, wenn die Anzahl der Maschinen im Pool unter einen Schwellenwert (Prozentsatz der Größe der Bereitstellungsgruppe) fällt. Für große Bereitstellungsgruppen wird unter Umständen eine große Zahl Maschinen eingeschaltet, wenn der Schwellenwert unterschritten wird. Planen Sie die Größe Ihrer Bereitstellungsgruppen daher sorgfältig oder passen Sie die Standardpuffergröße mit dem SDK an.

Energiestatustimer: Sie können mit den Energiestatustimern Maschinen anhalten, wenn die Verbindung eine bestimmte Zeit lang getrennt war. Maschinen werden zum Beispiel automatisch außerhalb der Bürostunden angehalten, wenn die Verbindung mindestens 10 Minuten lang getrennt war. Zufällige Maschinen oder Maschinen mit persönlichen vDisks werden bei Abmeldung des Benutzers automatisch heruntergefahren, es sei denn, Sie konfigurieren die Bereitstellungsgruppeneigenschaft "ShutdownDesktopsAfterUse" im SDK.

Sie können Timer für Werktage und Wochenenden sowie für Spitzen- und Nebenzeiten konfigurieren.

Teilweise Energieverwaltung bei dauerhaft zugewiesenen Maschinen: Bei dauerhaft zugewiesenen Maschinen können Sie Energiestatustimer, aber keine Pools oder Puffer einrichten. Die Maschinen werden zu Beginn jeder Spitzenzeit eingeschaltet und zu Beginn eines Zeitraums mit geringer Auslastung ausgeschaltet. Es ist keine Feinsteuerung der Zahl der Maschinen möglich, die als Ausgleich für verwendete Maschinen verfügbar werden (im Gegensatz zu nicht zugewiesenen Maschinen).

Einstellen der Energieverwaltung für Desktopbetriebssystemmaschinen

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und dann im Aktionsbereich **Bereitstellungsgruppe bearbeiten**.
3. Wählen Sie auf der Seite **Energieverwaltung** im Dropdownmenü "Energieverwaltung für Maschinen" die Option **Werktage** aus. Wochentage umfassen standardmäßig die Tage von Montag bis Freitag.
4. Wählen Sie bei zufälligen Bereitstellungsgruppen unter **Maschinen einschalten** die Option **Bearbeiten** und geben Sie die Poolgröße während der Werktage an. Wählen Sie anschließend die Anzahl der einzuschaltenden Maschinen.
5. Legen Sie unter **Spitzenzeiten** die Zeiträume für Spitzen- und Nebenzeiten für jeden Tag fest.
6. Stellen Sie die Energiestatustimer für Spitzen- und Nebenzeiten an Werktagen ein: Geben Sie für **Während**

Spitzenzeiten > Wenn getrennt die Verzögerung in Minuten ein, nach der getrennte Maschinen in der Bereitstellungsgruppe angehalten werden sollen, und klicken Sie auf "Anhalten". Geben Sie für **Während Nicht-Spitzenzeiten > Wenn getrennt** die Verzögerung in Minuten ein, nach der abgemeldete Maschinen in der Bereitstellungsgruppe heruntergefahren werden, und klicken Sie auf **Herunterfahren**. Dieser Timer ist für Bereitstellungsgruppen mit zufälligen Maschinen nicht verfügbar.

7. Wählen Sie im Dropdownmenü "Energieverwaltung für Maschinen" die Option **Wochenende** aus und konfigurieren Sie die Spitzenzeiten und Energiestatustimer für Wochenenden.
8. Klicken Sie auf **OK** oder **Übernehmen**.

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

Erstellen eines Neustartzeitplans

Über einen Neustartzeitplan wird der regelmäßige Neustart aller Maschinen in einer Bereitstellungsgruppe festgelegt.

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Bereitstellungsgruppe und dann im Aktionsbereich **Bereitstellungsgruppe bearbeiten**.
3. Wenn Sie nicht möchten, dass die Maschinen in der Bereitstellungsgruppe automatisch neu gestartet werden, wählen Sie auf der Seite **Neustartzeitplan** das Optionsfeld **Nein** und fahren Sie mit dem letzten Schritt dieses Verfahrens fort. Es wird kein Neustartzeitplan bzw. keine Rolloutstrategie konfiguriert. Wenn Sie zuvor einen Zeitplan konfiguriert hatten, wird er durch diese Auswahl aufgehoben.
4. Sollen die Maschinen in der Bereitstellungsgruppe automatisch neu gestartet werden, wählen Sie das Optionsfeld **Ja**.
5. Wählen Sie für **Neustartintervall** die Option **Täglich** oder den Wochentag, an dem der Neustart durchgeführt werden soll.
6. Wählen Sie für **Neustart beginnen um** die Tageszeit, zu der der Neustart beginnen soll.
7. Wählen Sie unter **Neustartdauer** aus, ob alle Maschinen gleichzeitig gestartet werden sollen oder geben Sie die Gesamtzeitdauer zum Beginnen des Neustarts an. Ein interner Algorithmus bestimmt, wann welche Maschine während dieses Zeitraums neu gestartet wird.
8. Wählen Sie in der Dropdownliste **Benachrichtigung** aus, ob auf den betroffenen Maschinen eine Meldung angezeigt werden soll, bevor der Neustart beginnt. In der Standardeinstellung wird keine Meldung angezeigt. Wenn Sie festlegen, dass 15 Minuten vor dem Neustart eine Meldung angezeigt wird, können Sie in der Dropdownliste **Benachrichtigung erneut senden** vorgeben, dass die Meldung alle fünf Minuten nach Erstanzeige wiederholt werden soll. Standardmäßig wird die Meldung nicht wiederholt angezeigt.
9. Geben Sie im Feld **Benachrichtigung** den Text der Meldung ein (es gibt keinen Standardtext). Wenn die Meldung die Zeit in Minuten bis zum Neustart enthalten soll, verwenden Sie die Variable **%m%** (z. B. "Achtung: Der Computer wird in %m% Minuten automatisch neu gestartet.") Wenn Sie die Benachrichtigung wiederholen lassen und die Variable "%m%" verwenden, wird die Zeitangabe bei jeder Wiederholung um fünf Minuten verringert. Sofern Sie keinen gleichzeitigen Neustart aller Maschinen festgelegt haben, wird die Meldung auf jeder Maschine in der Bereitstellungsgruppe zu der von dem internen Algorithmus berechneten Zeit angezeigt.
10. Klicken Sie auf **OK** oder **Übernehmen**.

Sie können kein automatisiertes Einschalten oder Herunterfahren über Studio durchführen, sondern nur Neustarts.

Unterbinden der Benutzerverbindung mit Maschinen (Wartungsmodus)

Wenn Sie vorübergehend verhindern möchten, dass neue Verbindungen mit Maschinen hergestellt werden, können Sie den Wartungsmodus für eine oder alle Maschinen in einer Bereitstellungsgruppe aktivieren. Das ist beispielsweise vor dem Anwenden von Patches oder der Verwendung von Verwaltungstools nützlich.

- Wenn sich eine Serverbetriebssystemmaschine im Wartungsmodus befindet, können Benutzer eine Verbindung mit vorhandenen Sitzungen herstellen, aber keine neuen Sitzungen starten.
- Bei einer Desktopbetriebssystemmaschine (oder einem Computer mit Remote-PC-Zugriff) im Wartungsmodus können Benutzer keine Verbindung herstellen. Aktuelle Verbindungen bleiben bis zur Trennung oder Abmeldung erhalten.

Wartungsmodus ein- oder ausschalten:

1. Wählen Sie im Studio-Navigationsbereich "Bereitstellungsgruppen" aus.
2. Wählen Sie eine Gruppe aus.
3. Zum Aktivieren des Wartungsmodus für alle Maschinen in der Bereitstellungsgruppe wählen Sie im Aktionsbereich "Wartungsmodus einschalten". Zum Aktivieren des Wartungsmodus für einzelne Maschinen wählen Sie im Aktionsbereich "Maschinen anzeigen". Wählen Sie eine Maschine aus und wählen Sie dann im Aktionsbereich "Wartungsmodus einschalten".
4. Zum Deaktivieren des Wartungsmodus für eine oder alle Maschinen in einer Bereitstellungsgruppe befolgen Sie die o. g. Anweisungen oben unter Auswahl der Option "Wartungsmodus ausschalten" im Aktionsbereich.

Einstellungen für Windows-Remotedesktopverbindungen wirken sich auch darauf aus, ob eine Serverbetriebssystemmaschine im Wartungsmodus ist. Der Wartungsmodus ist in folgenden Fällen aktiviert:

- Der Wartungsmodus wurde wie oben beschrieben aktiviert.
- Die Remotedesktopverbindung wurde auf **Keine Verbindung mit diesem Computer zulassen** festgelegt.
- Die Remotedesktopverbindung wurde auf **Keine Verbindung mit diesem Computer zulassen** festgelegt und für den Anmeldemodus der Remotehostkonfiguration wurde **Neue Verbindungen zulassen, doch neue Anmeldungen verhindern** oder **Neue Verbindungen zulassen, doch Neuanmeldungen bis zum Neustart des Servers verweigern** gewählt.

Sie können auch den Wartungsmodus für eine Verbindung ein- und ausschalten, was sich auf die Maschine auswirkt, die die Verbindung verwendet, oder für einen Maschinenkatalog, was sich auf alle Maschinen in diesem auswirkt.

Ändern der Maschinen-Benutzer-Zuweisung

Sie können die Zuweisungen von Desktopbetriebssystemmaschinen, nicht aber die von Serverbetriebssystemmaschinen oder Maschinen, die mit Provisioning Services erstellt wurden, ändern.

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Gruppe aus.
3. Zum Ändern der Zuweisung mehrerer Maschinen wählen Sie im Aktionsbereich **Bereitstellungsgruppe bearbeiten**. Wählen Sie auf der Seite **Maschinenzuteilung** die Maschinen aus und geben Sie die neuen Benutzer an. Klicken Sie auf

OK oder **Anwenden**.

4. Zum Ändern der Zuweisung einer Maschine wählen Sie im Aktionsbereich **Maschinen anzeigen**. Wählen Sie die Maschine und dann im Aktionsbereich **Benutzer ändern**. Fügen Sie einen Benutzer hinzu oder entfernen Sie den Benutzer.

Ändern der maximalen Anzahl Maschinen pro Benutzer

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und dann im Aktionsbereich **Bereitstellungsgruppe bearbeiten**.
3. Legen Sie auf der Seite **Benutzereinstellungen** (bzw. **Grundeinstellungen**) einen Wert für "Desktops pro Benutzer" fest.
4. Klicken Sie auf **OK** oder **Übernehmen**.

Lastverwaltung

Die Lastverwaltung ist nur bei Serverbetriebssystemmaschinen möglich.

Bei der Lastverwaltung wird die Serverlast gemessen und festgelegt, welcher Server unter den aktuellen Umgebungsbedingungen auszuwählen ist. Diese Auswahl basiert auf folgenden Faktoren:

Wartungsmodusstatus des Servers: Eine Serverbetriebssystemmaschine wird nur für den Lastausgleich berücksichtigt, wenn der Wartungsmodus für sie deaktiviert ist.

Serverlastindex: bestimmt, mit welcher Wahrscheinlichkeit ein Server, der Serverbetriebssystemmaschinen bereitstellt, Verbindungen erhält. Der Index basiert auf einer Kombination von Lastauswertungskriterien: Anzahl der Sitzungen sowie Einstellungen für Leistungswerte (z. B. CPU-, Datenträger- und Speichernutzung). Die die Lastauswertungskriterien werden in den Richtlinieneinstellungen für die Lastverwaltung festgelegt.

Sie können den Lastindex in Director, über die Suche in Studio und im SDK überwachen.

In Studio ist die Serverlastindexspalte standardmäßig ausgeblendet. Zum Anzeigen der Spalte wählen Sie eine Maschine, klicken Sie mit der rechten Maustaste auf eine Spaltenüberschrift und wählen Sie "Spalte auswählen". Klicken Sie in der Kategorie "Maschine" auf Serverlastindex.

Verwenden Sie im SDK das Cmdlet **Get-BrokerMachine**. Weitere Informationen finden Sie unter CTX202150.

Ein Serverlastindex von 10.000 bedeutet, dass der Server voll ausgelastet ist. Wenn keine anderen Server verfügbar sind, erhalten die Benutzer beim Starten einer Sitzung u. U. eine Meldung, dass der Desktop oder die Anwendung zurzeit nicht verfügbar ist.

Richtlinieneinstellung "Toleranzwert für gleichzeitige Anmeldungen": maximale Anzahl gleichzeitiger Serveranmeldeanforderungen. (Diese Einstellung entspricht der Lastdrosselung in XenApp-Versionen vor 7.5.)

Wenn alle Server den Toleranzwert für gleichzeitige Anmeldungen erreichen oder überschreiten, wird die nächste Anmeldeanforderung dem Server mit der niedrigsten Anzahl ausstehender Anmeldungen zugewiesen. Wenn mehrere Server diese Kriterien erfüllen, wird der Server mit dem niedrigsten Lastindex ausgewählt.

Entfernen von Maschinen aus Bereitstellungsgruppen

Beim Entfernen einer Maschine wird diese aus der Bereitstellungsgruppe gelöscht, jedoch nicht aus dem Maschinenkatalog, den die Bereitstellungsgruppe verwendet. Die Maschine steht daher für Zuweisungen zu anderen Bereitstellungsgruppen zur Verfügung.

Maschinen müssen heruntergefahren werden, bevor sie entfernt werden können. Wenn Sie vorübergehend verhindern möchten, dass Benutzer eine Verbindung mit der Maschine herstellen, während Sie sie löschen, setzen Sie die Maschine in den Wartungsmodus, bevor Sie sie herunterfahren.

Wenn Sie eine Maschine einem anderen Benutzer zuweisen, denken Sie daran, dass Maschinen persönliche Daten enthalten können. Es empfiehlt sich ggf. ein Reimaging der Maschine.

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und wählen Sie dann im Aktionsbereich **Maschinen anzeigen**.
3. Stellen Sie sicher, dass die Maschine heruntergefahren ist.
4. Wählen Sie im Aktionsbereich **Aus Bereitstellungsgruppe entfernen**.

Einschränken des Zugriffs auf Maschinen

Alle Änderungen zum Einschränken des Zugriffs auf Maschinen in einer Bereitstellungsgruppe haben Vorrang vor zuvor durchgeführten Einstellungen, unabhängig von der verwendeten Methode. Sie haben folgende Möglichkeiten:

Einschränken des Zugriffs für Administratoren über Geltungsbereiche für die delegierte Administration. Sie können einen Geltungsbereich erstellen und zuweisen, in dem Administratoren auf alle Anwendungen zugreifen können, und einen zweiten Geltungsbereich, der nur den Zugriff auf spezifische Anwendungen zulässt. Weitere Informationen finden Sie im Artikel Delegierte Administration.

Einschränken des Zugriffs für Benutzer über SmartAccess-Richtlinienausdrücke, mit denen über NetScaler Gateway hergestellte Benutzerverbindungen gefiltert werden.

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und dann im Aktionsbereich **Bereitstellungsgruppe bearbeiten**.
3. Wählen Sie auf der Seite "Zugriffsrichtlinie" **Über NetScaler Gateway hergestellte Verbindungen**.
4. Wenn Sie nur einen Teil dieser Verbindungen auswählen möchten, wählen Sie **Verbindungen, auf die mindestens einer der folgenden Filter zutrifft**. Legen Sie dann die NetScaler Gateway-Site fest und fügen Sie SmartAccess-Richtlinienausdrücke für zulässige Benutzerzugriffsszenarios hinzu, bzw. bearbeiten oder löschen Sie diese. Weitere Informationen finden Sie in der Dokumentation zu NetScaler Gateway.
5. Klicken Sie auf **OK** oder **Übernehmen**.

Einschränken des Zugriffs für Benutzer über Ausschlussfilter für mit dem SDK festgelegte Zugriffsrichtlinien. Zugriffsrichtlinien werden auf Bereitstellungsgruppen angewendet, um Verbindungen genauer zu definieren. Sie können beispielsweise den Maschinenzugriff für eine Untergruppe von Benutzern einschränken und zulässige Benutzergeräte festlegen. Mit Ausschlussfiltern können Zugriffsrichtlinien weiter angepasst werden. Aus Sicherheitsgründen können Sie beispielsweise den Zugriff für eine Untergruppe der Benutzer oder Geräte verweigern. Ausschlussfilter sind in der Standardeinstellung deaktiviert.

Wenn Sie beispielsweise den Zugriff von einem Lernlabor im Subnetz des Unternehmensnetzwerks auf eine spezifische Bereitstellungsgruppe verhindern möchten, unabhängig davon, wer die Maschinen im Labor nutzt, verwenden Sie folgenden Befehl: Set-BrokerAccessPolicy -Name VPDesktops_Direct -ExcludedClientIPFilterEnabled $True -

Sie können das Sternchen (*) als Platzhalter für alle Tags, die mit dem gleichen Richtlinienausdruck beginnen, verwenden. Wenn Sie beispielsweise auf einer Maschine das Tag "VPDesktops_Direct" hinzufügen und auf einer anderen das Tag "VPDesktops_Test", wird der Filter durch Festlegen des Tags auf "VPDesktops_*" im Skript "Set-BrokerAccessPolicy" auf beide Maschinen angewendet.

Aktualisieren einer Maschine

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Gruppe und dann im Aktionsbereich **Maschinen anzeigen**.
3. Wählen Sie eine Maschine und dann im Aktionsbereich **Maschinen aktualisieren**.

   Zum Auswählen eines anderen Masterimages wählen Sie **Masterimage** und dann einen Snapshot.

   Zum Anwenden der Änderungen und Benachrichtigen der Benutzer der Maschine wählen Sie **Rolloutbenachrichtigung für Endbenutzer**. Legen Sie anschließend Folgendes fest: ob die Aktualisierung des Masterimages sofort oder beim nächsten Neustart erfolgen soll, die Neustartverteilung (Gesamtzeit des Beginns der Aktualisierung aller Maschinen in der Gruppe) und ob Benutzer über den Neustart benachrichtigt werden sollen sowie die entsprechende Meldung.

Verwalten von Anwendungen

Feb 29, 2016

Dieser Abschnitt enthält folgende Themen:

Hinzufügen von Anwendungen

Gut zu wissen:

- Sie können Remote-PC-Zugriff-Bereitstellungsgruppen keine Anwendungen hinzufügen.
- Standardmäßig werden neu hinzugefügte Anwendungen in einem Ordner mit dem Namen "Applications" abgelegt. Sie können einen anderen Ordner festlegen (siehe *Verwalten von Anwendungsordnern* unten).
- Wenn Sie eine Anwendung hinzufügen und es bereits eine Anwendung mit dem gleichen Namen im gleichen Ordner gibt, werden Sie aufgefordert, die neue Anwendung umzubenennen. Wenn Sie dies ablehnen, wird die Anwendung mit einem Suffix hinzugefügt, sodass ihr Name innerhalb des Ordners eindeutig ist.
- Sie können keine Anwendungen mit dem Assistenten zum Hinzufügen von Anwendungen aus Bereitstellungsgruppen entfernen, denn dies ist ein eigener Vorgang.
- Wenn Sie zwei Anwendungen mit dem gleichen Namen den gleichen Benutzern bereitstellen, ändern Sie in Studio die Eigenschaft "Anwendungsname (Benutzer)", sonst wird den Benutzern der Name in Citrix Receiver doppelt angezeigt.

Hinzufügen von Anwendungen

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Gruppe aus.
3. Klicken Sie im Aktionsbereich auf **Anwendungen hinzufügen**. Es wird eine Liste der Anwendungen angezeigt. Wählen Sie eine oder mehrere Anwendungen aus.

Wurde der ausgewählte Maschinenkatalog mit einem Masterimage mit Anwendungen erstellt, enthält die Liste auch die Anwendungen, die auf einer von diesem Image erstellten Maschine erkannt wurden.

Wenn Sie App-V-Serverinformationen konfiguriert haben und für den App-V-Server Pakete verfügbar sind, enthält die Liste die betreffenden Anwendungen.

Sie können Anwendungen außerdem mit **Anwendungen manuell hinzufügen** manuell hinzufügen. Geben Sie in dem damit geöffneten Dialogfeld den Pfad zur ausführbaren Datei, das Arbeitsverzeichnis, optionale Befehlszeilenargumente und die Anzeigenamen für Administratoren und Benutzer an.

Sie können die Eigenschaften einer Anwendung und den Ordner, in dem die Anwendung in Studio angezeigt wird, ändern. Informationen hierzu finden Sie in den Abschnitten unten.

Duplizieren, Aktivieren/Deaktivieren, Umbenennen und Löschen von Anwendungen

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.

Wenn das Umbenennen einer Anwendung dazu führen würde, dass ihr Name mit dem einer anderen Anwendung im selben Ordner identisch wäre, werden Sie aufgefordert, einen anderen Namen einzugeben.

Wenn Sie eine Anwendung löschen, wird diese aus der Bereitstellungsgruppe, jedoch nicht aus dem im Maschinenkatalog verwendeten Masterimage entfernt.

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie die Registerkarte **Anwendungen** im mittleren Bereich und dann die Anwendung aus.
3. Wählen Sie die relevante Aufgabe im Aktionsbereich.

Entfernen von Anwendungen aus einer Bereitstellungsgruppe

Eine Anwendung muss mindestens einer Bereitstellungsgruppe zugewiesen sein. Wenn Sie versuchen, eine Anwendung aus einer Bereitstellungsgruppe zu entfernen und dies würde bedeuten, dass die Anwendung keiner Bereitstellungsgruppe mehr zugewiesen wäre, erhalten Sie stattdessen die Option zum Löschen der Anwendung. Wenn Sie sich gegen das Löschen der Anwendung entscheiden, können Sie sie einer anderen Bereitstellungsgruppe zuweisen und dann aus der ursprünglichen Bereitstellungsgruppe entfernen.

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Bereitstellungsgruppe aus. Wählen Sie im mittleren Bereich unten die Registerkarte **Anwendungen** und dann die Anwendung, die Sie entfernen möchten.
3. Wählen Sie im Aktionsbereich **Anwendung entfernen**.

Ändern der Anwendungseigenschaften

Ändern der Eigenschaften einer Anwendung

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie die Registerkarte **Anwendungen** im mittleren Bereich und dann die Anwendung aus.
3. Wählen Sie im Aktionsbereich **Eigenschaften**.
4. Wählen Sie die Seite mit der Eigenschaft, die Sie ändern möchten. Nach Durchführung der Änderung klicken Sie auf **OK** oder **Anwenden**.

Eigenschaft	Seite

Kategorie/Ordner in Citrix Receiver	Bereitstellungsgruppe
Befehlszeilenargumente	Speicherort
Bereitstellungsgruppenzuordnung	Gruppen
Beschreibung	Identifizierung
Dateinamenerweiterungen	Dateitypzuordnung
Dateitypzuordnungen	Dateitypzuordnung
Symbol	Bereitstellungsgruppe
Schlüsselwörter für StoreFront	Identifizierung
Limits (siehe unten)	Bereitstellungsgruppe
Name	Identifizierung
Pfad zur ausführbaren Datei	Speicherort
Verknüpfung auf dem Desktop des Benutzers	Bereitstellungsgruppe
Sichtbarkeit	Sichtbarkeit beschränken
Arbeitsverzeichnis	Speicherort

Anwendungsänderungen werden evtl. für aktuelle Anwendungsbenutzer erst wirksam, wenn diese ihre Sitzung abmelden.

Konfigurieren von Anwendungslimits

Durch Konfigurieren von Anwendungslimits können Sie die Anwendungsnutzung verwalten. Sie können z. B. die Zahl der Benutzer, die gleichzeitig auf eine Anwendung zugreifen, beschränken. Analog dazu können Sie über Anwendungslimits die Zahl gleichzeitiger Instanzen ressourcenintensiver Anwendungen limitieren, um die Serverleistung zu gewährleisten und eine Dienstverschlechterung zu vermeiden.

Wichtig: Diese Funktion limitiert die Anzahl der vom Controller vermittelten Anwendungsstarts (z. B. von Citrix Receiver und StoreFront) und nicht die Anzahl ausgeführter Anwendungen, die auf andere Weise gestartet werden konnten. Anwendungslimits helfen daher bei der Verwaltung der gleichzeitigen Nutzung, gestatten jedoch nicht in allen Szenarios eine Erzwingung. Anwendungslimits können beispielsweise nicht angewendet werden, wenn der Controller eine geleaste Verbindung hat.

Standardmäßig besteht kein Limit für die Anzahl gleichzeitig ausgeführter Anwendungsinstanzen. Sie können eines oder auch beide der zwei möglichen Anwendungslimits konfigurieren:

- Maximale Anzahl gleichzeitiger Instanzen einer Anwendung für alle Benutzer in der Bereitstellungsgruppe
- Eine Anwendungsinstanz pro Benutzer in der Bereitstellungsgruppe

Wenn ein Limit konfiguriert ist und ein Benutzer versucht, eine Anwendungsinstanz zu starten, durch die das Limit überschritten würde, wird eine Fehlermeldung generiert.

Beispiele für Anwendungslimits:

- **Maximale Anzahl gleichzeitiger Instanzen:** Sie konfigurieren für eine Bereitstellungsgruppe die maximal zulässige Anzahl gleichzeitiger Instanzen der Anwendung "Alpha" mit 15. Anschließend werden in der Bereitstellungsgruppe 15 Instanzen dieser Anwendung gleichzeitig ausgeführt. Versucht nun ein Benutzer in der Bereitstellungsgruppe, Alpha zu starten, wird eine Fehlermeldung generiert und Alpha wird nicht gestartet, da hierdurch das konfigurierte Limit von 15 überschritten würde.
- **Limit von einer Instanz pro Benutzer:** In einer anderen Bereitstellungsgruppe haben Sie für die Anwendung "Beta" das Limit von einer Instanz pro Benutzer festgelegt. Benutzer Hermann startet die Anwendung Beta. Eine Weile später versucht er eine weitere Instanz von Beta zu starten. Eine Fehlermeldung wird generiert und Beta wird nicht gestartet, da dadurch das Limit überschritten würde.
- **Maximale Anzahl gleichzeitiger Instanzen plus Limit von einer Instanz pro Benutzer:** In einer anderen Bereitstellungsgruppe legen Sie die maximal zulässige Anzahl gleichzeitiger Instanzen der Anwendung "Delta" auf 10 fest und aktivieren außerdem das Limit von einer Instanz pro Benutzer. Werden anschließend alle 10 Instanzen von Delta ausgeführt, wird bei jedem weiteren Versuch, die Anwendung in der Bereitstellungsgruppe zu starten, eine Fehlermeldung angezeigt und Delta nicht gestartet. Versucht ein Benutzer, der bereits eine Delta-Instanz gestartet hat, eine zweite Instanz zu starten, wird eine Fehlermeldung angezeigt und die zweite Instanz wird nicht gestartet.

Werden Anwendungsinstanzen auch über andere Methoden als das Controllerbrokering gestartet (z. B. wenn ein Controller eine geleaste Verbindung hat) und die festgelegten Limits werden überschritten, können Benutzer erst dann wieder Instanzen starten, wenn zuvor entsprechend viele Instanzen geschlossen wurden und kein Limit mehr überschritten wird. Die Instanzen, die das Limit überschreiten, werden nicht zwangsweise geschlossen, sondern können weiterlaufen, bis die Benutzer sie schließen.

Wenn Sie das Sitzungsroaming deaktivieren, deaktivieren auch das Limit einer Anwendungsinstanz pro Benutzer. Wenn Sie das Limit einer Anwendungsinstanz pro Benutzer aktivieren, konfigurieren Sie keinen der beiden Werte, durch die neue Sitzungen auf neuen Geräten zugelassen werden. Weitere Informationen zum Roaming finden Sie im Artikel Sitzungen.

Konfigurieren von Anwendungslimits

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen** und dann eine Anwendung.
2. Wählen Sie die Registerkarte **Anwendungen** im mittleren Bereich und dann die Anwendung aus.
3. Wählen Sie im Aktionsbereich **Eigenschaften**.
4. Wählen Sie auf der Seite **Bereitstellung** eine der folgenden Optionen aus: Wenn Sie fertig sind, klicken Sie auf **OK** oder **Anwenden**.

- Uneingeschränkte Verwendung der Anwendung zulassen: Es gibt kein Limit für die Anzahl der gleichzeitig ausgeführten Instanzen. Dies ist die Standardeinstellung.
- Limit festlegen: Es sind zwei Limits, die Sie einzeln oder beide festlegen können.
  - Anzahl der gleichzeitig ausgeführten Instanzen beschränken auf:
  - Auf eine Instanz pro Benutzer beschränken

Verwalten von Anwendungsordnern

Standardmäßig werden neue Anwendungen, die Sie Bereitstellungsgruppen hinzufügen, 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.

Gut zu wissen:

- Sie können den Ordner "Applications" nicht umbenennen oder löschen. Sie können aber alle Anwendungen in diesem Ordner in andere von Ihnen erstellte Ordner verschieben.
- Ein Ordnername darf 1-64 Zeichen enthalten. Leerstellen sind zugelassen.
- Ordner können bis zu fünffach verschachtelt werden.
- Ordner müssen keine Anwendungen enthalten, leere Ordner sind zugelassen.
- Ordner werden in Studio alphabetisch aufgelistet, es sei denn, Sie verschieben sie oder geben beim Erstellen einen anderen Speicherort an.
- Sie können mehr als einen Ordner mit dem gleichen Namen haben, sofern jeder einen anderen übergeordneten Ordner hat. Sie können mehr als eine Anwendung mit dem gleichen Namen haben, sofern jede in einem anderen Ordner ist.
- Zum Entfernen, Umbenennen und Löschen eines Ordners, der Anwendungen enthält, benötigen Sie für alle enthaltenen Anwendungen die Berechtigung zum Anzeigen von Anwendungen in Ordnern und die Berechtigung zum Bearbeiten der Anwendungseigenschaften.
- Die meisten der folgenden Verfahren umfassen Aktionen aus dem Bereich "Aktionen" in Studio. Alternativ können Sie Kontextmenüs oder Drag & Drop verwenden. Wenn Sie beispielsweise einen Ordner am falschen Speicherort erstellen oder ihn dorthin verschieben, können Sie ihn per Drag & Drop an den korrekten Speicherort ziehen.

Verwalten von Anwendungsordnern

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen** und dann im mittleren Bereich die Registerkarte **Anwendungen**.
2. Zum Anzeigen aller Ordner (unter Ausschluss verschachtelter Ordner) klicken Sie oberhalb der Ordnerliste auf **Alle anzeigen**.
3. Zum Erstellen eines (unverschachtelten) Ordners auf der höchsten Ebene wählen Sie den Anwendungsordner aus. Zum Erstellen des Ordners als Unterordner eines vorhandenen Ordners wählen Sie diesen Ordner aus. Wählen Sie dann im Aktionsbereich **Ordner erstellen**. Geben Sie einen Namen ein.
4. Zum Verschieben eines Ordners wählen Sie den Ordner und dann im Aktionsbereich **Ordner verschieben**. Sie können immer nur einen Ordner verschieben, es sei denn, der Ordner enthält Unterordner. **Tipp:** Die einfachste Möglichkeit zum Verschieben von Ordnern ist das Drag & Drop.
5. Zum Umbenennen eines Ordners wählen Sie den Ordner und dann im Aktionsbereich **Ordner umbenennen**. Geben Sie einen Namen ein.
6. Zum Löschen eines Ordners wählen Sie den Ordner und dann im Aktionsbereich **Ordner löschen**. Beim Löschen eines Ordners, der Anwendungen und andere Ordner enthält, werden diese Objekte auch gelöscht. Beim Löschen einer

Anwendung wird die Anwendungszuweisung aus der Bereitstellungsgruppe aber nicht aus der Maschine entfernt.

7. Zum Verschieben von Anwendungen in einen Ordner wählen Sie eine oder mehrere Anwendungen. Wählen Sie dann im Aktionsbereich **Anwendung verschieben**. Wählen Sie den Ordner aus. Zum Verschieben von Anwendungen in einen anderen Ordner über den Assistenten zum Erstellen von Bereitstellungsgruppen wählen Sie auf der Seite **Anwendungen** des Assistenten **Ändern** und dann einen Ordner, bzw. erstellen Sie einen neuen Ordner.

Verwalten von Sitzungen über Bereitstellungsgruppen

Feb 29, 2016

Lesen Sie neben den Erläuterungen unten den Artikel Sitzungsverwaltung zu Sitzungszuverlässigkeit, Sitzungsroaming, automatischer Wiederverbindung von Clients, ICA- Keep-Alive und Workspace Control.

Abmelden oder Trennen einer Sitzung oder Senden einer Nachricht an Benutzer

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Gruppe und dann im Aktionsbereich **Maschinen anzeigen**.
3. Zum Abmelden einer Sitzung wählen Sie die Sitzung oder den Desktop und dann im Aktionsbereich **Abmelden**. Die Sitzung wird geschlossen und die Maschine steht nun anderen Benutzern zur Verfügung, sofern sie nicht einem bestimmten Benutzer zugewiesen ist.
4. Zum Trennen einer Sitzung wählen Sie die Sitzung oder den Desktop und dann im Aktionsbereich **Trennen**. Anwendungen werden weiter ausgeführt und die Maschine bleibt dem Benutzer zugewiesen. Der Benutzer kann eine Verbindung mit derselben Maschine wiederherstellen.
5. Zum Senden einer Nachricht an die Benutzer wählen Sie die Sitzung, die Maschine oder den Benutzer und dann im Aktionsbereich **Nachricht senden**. Geben Sie die Nachricht ein.

Sie können die Energiestatustimer für Desktopbetriebssystemmaschinen so konfigurieren, dass nicht genutzte Sitzungen automatisch verarbeitet werden. Weitere Informationen finden Sie im Abschnitt *Energieverwaltung für Maschinen* des Artikels Verwalten von Maschinen in einer Bereitstellungsgruppe.

Konfigurieren des Vorabstarts und des Fortbestehens von Sitzungen

Diese Features werden nur auf Serverbetriebssystemmaschinen unterstützt.

Vorabstart und Fortbestehen von Sitzungen ermöglichen einen schnellen Zugriff durch Benutzer auf Anwendungen, indem Sitzungen gestartet werden, bevor sie angefordert werden, und aktiv bleiben, nachdem ein Benutzer alle Anwendungen geschlossen hat.

In der Standardeinstellung werden diese Features nicht verwendet, d. h. eine Sitzung startet, wenn ein Benutzer eine Anwendung startet, und bleibt so lange aktiv, bis die letzte Anwendung der Sitzung geschlossen wird.

Überlegungen:

- Die Bereitstellungsgruppe muss Anwendungen unterstützen und auf den Maschinen muss ein VDA für Windows-Serverbetriebssysteme in mindestens Version 7.6 ausgeführt werden.
- Diese Features werden nur bei Verwendung von Citrix Receiver für Windows unterstützt, sie erfordern außerdem zusätzliche Citrix Receiver-Konfigurationsschritte. Anweisungen hierzu finden Sie in der Produktdokumentation zu Ihrer Citrix Receiver für Windows-Version. Suchen Sie dort nach "Sitzungsvorabstart".

- Citrix Receiver für HTML5 wird nicht unterstützt.
- Wird ein Computer in den Modus "Anhalten" oder in den Ruhezustand versetzt, funktioniert der Sitzungsvorabstart unabhängig von den Vorabstarteinstellungen nicht. Die Benutzer können den Computer bzw. die Sitzung sperren, wenn sie sich jedoch von Citrix Receiver abmelden, wird die Sitzung beendet und ein Vorabstart ist nicht mehr möglich.
- Wird der Sitzungsvorabstart verwendet, können die Energieverwaltungsfunktionen "Anhalten" und "Ruhezustand" auf physischen Clientcomputern nicht verwendet werden. Clientmaschinenbenutzer können ihre Sitzungen sperren, sollten sich aber nicht abmelden.
- Vorab gestartete und fortbestehende Sitzungen verbrauchen eine Lizenz, jedoch nur wenn sie verbunden sind. Nicht genutzte vorab gestartete und fortbestehende Sitzungen werden standardmäßig nach 15 Minuten getrennt. Dieser Wert kann über das PowerShell-Cmdlet "New/Set-BrokerSessionPreLaunch" konfiguriert werden.
- Eine sorgfältige Planung und Überwachung der Aktivitätsmuster von Benutzern ist wichtig, damit diese Features so eingerichtet werden können, dass sie einander ergänzen. In einer optimalen Konfiguration besteht ein Gleichgewicht zwischen dem Vorteil einer schnelleren Anwendungsverfügbarkeit für Benutzer und den durch den Verbrauch von Lizenzen und die fortdauernde Zuteilung von Ressourcen entstehenden Kosten.
- Sie können den Vorabstart von Sitzungen auch für eine spezifische Uhrzeit in Citrix Receiver konfigurieren.

Dauer des Aktivbleibens nicht genutzter vorab gestarteter und fortbestehender Sitzungen

Wie lange eine nicht genutzte Sitzung aktiv bleibt, wenn der Benutzer keine Anwendung startet, kann über ein Timeout oder über Serverlast-Schwellenwerte angegeben werden. Sie können alle Parameter konfigurieren und die Sitzung wird jeweils durch das zuerst auftretende Ereignis beendet.

- **Timeout:** Ein konfiguriertes Timeout gibt die Anzahl der Minuten, Stunden oder Tage an, die eine nicht genutzte vorab gestartete oder fortbestehende Sitzung aktiv bleibt. Wenn Sie ein zu kurzes Timeout konfigurieren, werden vorab gestartete Sitzungen beendet, bevor der Benutzer in den Genuss des schnelleren Anwendungszugriffs kommt. Ist das Timeout zu lang, werden eingehende Benutzerverbindungen möglicherweise abgewiesen, da der Server nicht genügend Ressourcen hat.

  Sie können dieses Timeout über das SDK (Cmdlet "New/Set-BrokerSessionPreLaunch"), nicht aber über Studio deaktivieren. Wenn Sie das Timeout deaktivieren, wird es für die betreffende Bereitstellungsgruppe in Studio und im Assistenten zum Bearbeiten von Bereitstellungsgruppen nicht angezeigt.

- **Schwellenwerte:** Das automatische Beenden vorab gestarteter und fortbestehender Sitzungen auf der Basis der Serverlast gewährleistet, dass Sitzungen so lange wie möglich geöffnet bleiben (vorausgesetzt, es sind Serverressourcen verfügbar). Nicht genutzte vorab gestartete und fortbestehende Sitzungen verursachen keine Abweisung von Verbindungen, da sie automatisch beendet werden, wenn Ressourcen für neue Benutzersitzungen benötigt werden.

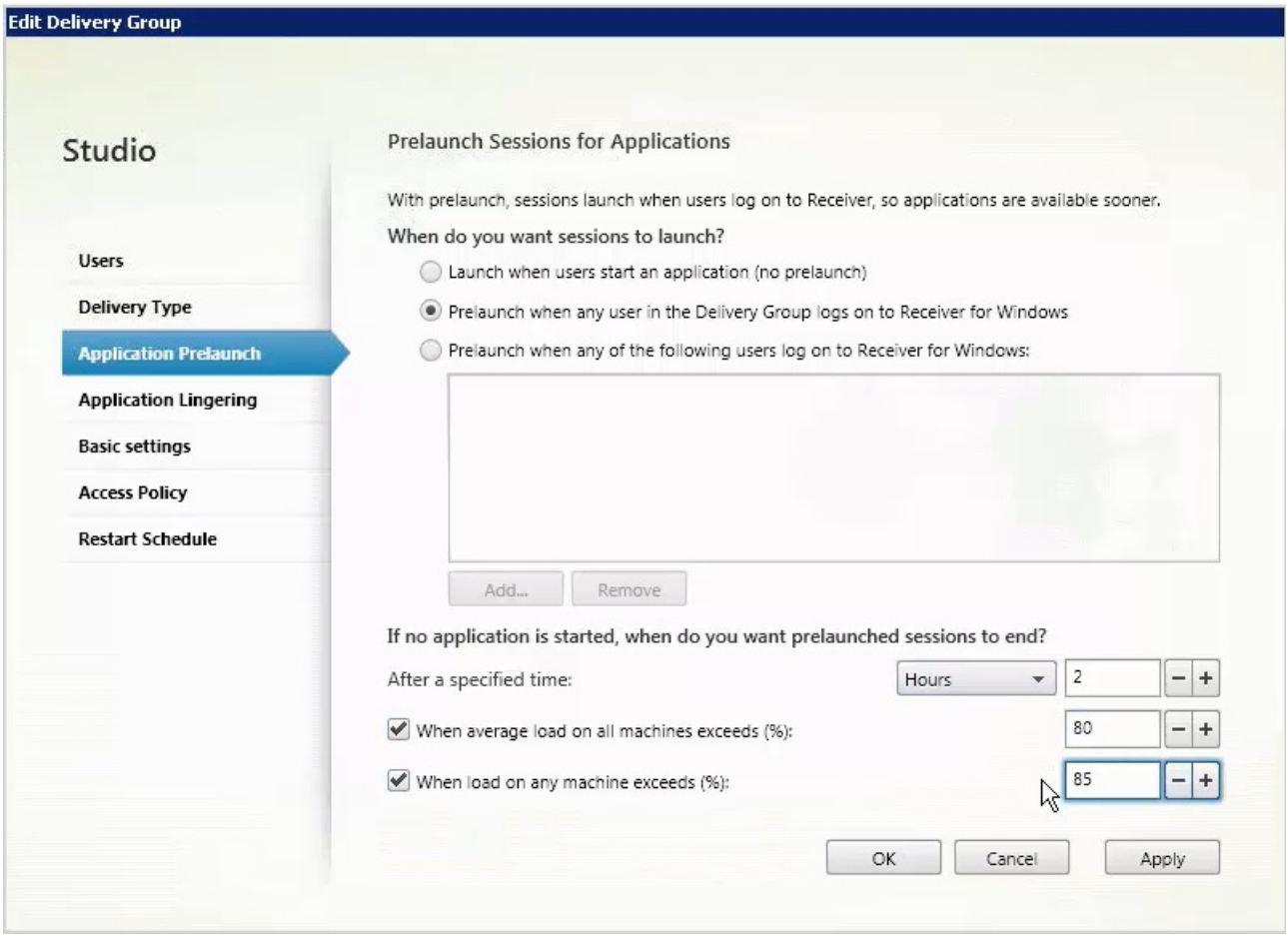
  Sie können zwei Schwellenwerte konfigurieren: die durchschnittliche Last aller Server der Bereitstellungsgruppe und die höchste Last eines Servers in der Bereitstellungsgruppe (beides in Prozent). Wird ein Schwellenwert überschritten, werden jeweils die Sitzungen beendet, die sich am längsten im Zustand "vorab gestartet" bzw. "fortbestehend" befinden. Das Beenden erfolgt einzeln im Minutentakt bis die Last unter den Schwellenwert fällt. (Solange der Schwellenwert überschritten ist, werden keine neuen Sitzungen vorab gestartet.)

Server mit VDAs, die nicht beim Controller registriert sind, und Server im Wartungsmodus gelten als voll ausgelastet. Bei einem ungeplanten Ausfall werden vorab gestartete und fortbestehende Sitzungen automatisch beendet, um Kapazität freizugeben.

Aktivieren des Vorabstarts von Sitzungen

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen**.

2. Wählen Sie eine Bereitstellungsgruppe und dann im Aktionsbereich **Bereitstellungsgruppe bearbeiten**.
3. Aktivieren Sie den Vorabstart von Sitzungen, indem Sie auf der Seite **Anwendungsvorabstart** auswählen, wann Sitzungen gestartet werden sollen:
   - Wenn Benutzer eine Anwendung starten. Dies ist die Standardeinstellung. Der Vorabstart von Sitzungen ist deaktiviert.
   - Wenn ein Benutzer der Bereitstellungsgruppe sich bei Citrix Receiver für Windows anmeldet.
   - Wenn ein beliebiger Benutzer einer Liste mit Benutzern und Bereitstellungsgruppen sich bei Citrix Receiver für Windows anmeldet. Bei Auswahl dieser Option müssen Sie auch die Benutzer oder Benutzergruppen festlegen.

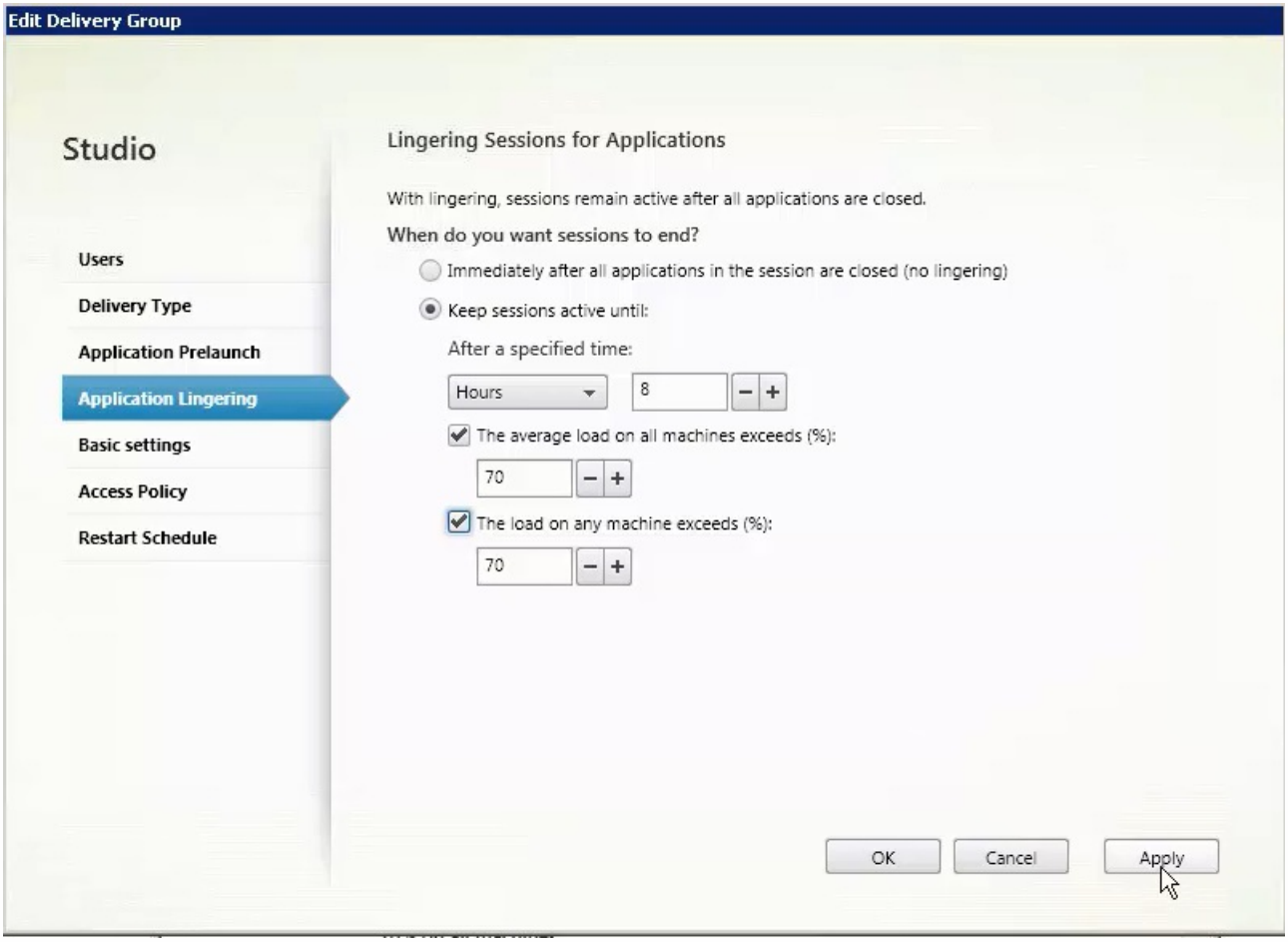


4. Eine vorab gestartete Sitzung wird durch eine normale Sitzung ersetzt, wenn der Benutzer eine Anwendung startet. Wenn der Benutzer keine Anwendung startet (d. h. die vorab gestartete Sitzung wird nicht verwendet), wird durch die folgenden Einstellungen bestimmt, wie lange die Sitzung aktiv bleibt.
   - Ablauf eines vorgegebenen Zeitintervalls. Das Zeitintervall können Sie ändern (1-99 Tage, 1-2376 Stunden oder 1-142.560 Minuten).
   - Wenn die durchschnittliche Last auf allen Maschinen in der Bereitstellungsgruppe einen bestimmten Prozentsatz (1-99 %) übersteigt.
   - Wenn die Last auf einer Maschine in der Bereitstellungsgruppe einen bestimmten Prozentsatz (1-99 %) übersteigt.

   Eine vorab gestartete Sitzung bleibt also bis zum Eintreten eines der folgenden Ereignisse aktiv: ein Benutzer startet eine Anwendung, das vorgegebene Zeitintervall läuft ab oder der angegebene Lastschwellenwert wird überschritten.

Aktivieren des Sitzungsfortbestehens

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen**.
2. Wählen Sie eine Bereitstellungsgruppe und dann im Aktionsbereich **Bereitstellungsgruppe bearbeiten**.
3. Aktivieren Sie auf der Seite **Anwendungsfortbestehen** das Sitzungsfortbestehen durch Aktivieren des Optionsfelds **Sitzungen bleiben aktiv bis**.



4. Mehrere Einstellungen wirken sich darauf aus, wie lange eine Sitzung aktiv bleibt, wenn der Benutzer keine weitere Anwendung startet.
   - Ablauf eines vorgegebenen Zeitintervalls. Das Zeitintervall können Sie ändern (1-99 Tage, 1-2376 Stunden oder 1-142.560 Minuten).
   - Wenn die durchschnittliche Last auf allen Maschinen in der Bereitstellungsgruppe einen bestimmten Prozentsatz (1-99 %) übersteigt.
   - Wenn die Last auf einer Maschine in der Bereitstellungsgruppe einen bestimmten Prozentsatz (1-99 %) übersteigt.

   Eine fortbestehende Sitzung bleibt also bis zum Eintreten eines der folgenden Ereignisse aktiv: ein Benutzer startet eine Anwendung, das vorgegebene Zeitintervall läuft ab oder der angegebene Lastschwellenwert wird überschritten.

Remote-PC-Zugriff

Feb 29, 2016

Mit Remote-PC-Zugriff kann ein Endbenutzer sich remote von jedem Standort aus an einem physischen Windows-PC im Büro anmelden. Der Virtual Delivery Agent (VDA) wird auf dem Büro-PC installiert. Er registriert sich bei dem Delivery Controller und verwaltet die HDX-Verbindung zwischen dem PC und den Clientgeräten des Endbenutzers. Remote-PC-Zugriff unterstützt ein Self-Service Modell. Nach der Einrichtung der Positivliste der Maschinen, die für Benutzer zugänglich sind, können die entsprechenden Benutzer ihre Büro-PCs einer Site ohne Eingriff des Administrators hinzufügen. Citrix Receiver wird auf ihrem Clientgerät ausgeführt und ermöglicht Zugriff auf alle Anwendungen und Daten auf dem Büro-PC von der Remote-PC-Zugriff-Desktopsitzung aus.

Ein Benutzer kann mehrere Desktops haben, einschließlich mehrere physische PCs oder eine Kombination von physischen PCs und virtuellen Desktops.

Hinweis: Energiesparmodus und Ruhezustand werden für Remote-PC-Zugriff nicht unterstützt. Remote-PC-Zugriff gilt nur für XenDesktop-Lizenzen. Sitzungen verbrauchen Lizenzen genauso wie andere XenDesktop-Sitzungen.

Überlegungen zu Active Directory

Bevor Sie die Bereitstellungssite für Remote-PC-Zugriff konfigurieren, richten Sie die Organisationseinheiten und Sicherheitsgruppen ein und erstellen Sie dann Benutzerkonten. Verwenden Sie diese Konten, um die Benutzer für die Bereitstellungsgruppen anzugeben, die für Remote-PC-Zugriff verwendet werden.

Wenn Sie Active Directory modifizieren, nachdem eine Maschine dem Maschinenkatalog hinzugefügt wurde, wird diese Zuweisung von Remote-PC-Zugriff nicht erneut ausgewertet. Sie können, falls erforderlich, Maschinen manuell einem anderen Katalog zuweisen.

Wenn Sie Organisationseinheiten verschieben oder löschen, sind die für Remote-PC-Zugriff verwendeten möglicherweise nicht mehr aktuell. VDAs sind u. U. (wenn überhaupt) nicht mehr dem am besten geeigneten Maschinenkatalog bzw. der am besten geeigneten Bereitstellungsgruppe zugewiesen.

Überlegungen zu Maschinenkatalogen und Bereitstellungsgruppen

Eine Maschine kann nur jeweils einem Maschinenkatalog und einer Bereitstellungsgruppe zugewiesen sein.

Sie können Maschinen in einen oder mehrere Remote PC-Zugriff-Maschinenkataloge einfügen.

Wenn Sie Maschinenkonten für den Maschinenkatalog auswählen, wählen Sie die niedrigste zutreffende Organisationseinheit, um einen möglichen Konflikt mit Maschinen eines anderen Maschinenkatalogs zu vermeiden. Beispiel: Im Fall von Bank/Bankbeamte/Kassierer, wählen Sie Kassierer.

Sie können alle Maschinen eines Remote-PC-Zugriff-Maschinenkatalogs über eine oder mehrere Bereitstellungsgruppen zuweisen. Wenn eine Benutzergruppe beispielsweise bestimmte Richtlinieneinstellungen und eine andere Gruppe andere Einstellungen benötigt, können Sie die Benutzer unterschiedlichen Bereitstellungsgruppen zuweisen und so die HDX-

Richtlinien nach Bereitstellungsgruppe filtern.

Wenn die Benutzerbetreuung in Ihrer IT-Infrastruktur auf dem geografischen Standort, der Abteilung oder einer anderen Kategorie beruht, können Sie Maschinen und Benutzer entsprechend gruppieren und so die delegierte Administration ermöglichen. Stellen Sie sicher, dass jeder Administrator über Berechtigungen für die relevanten Maschinenkataloge und die entsprechenden Bereitstellungsgruppen hat.

Erstellen Sie für Benutzer mit Büro-PCs mit Windows XP einen separaten Maschinenkatalog und eine separate Bereitstellungsgruppe für diese Systeme. Aktivieren Sie bei der Auswahl von Maschinenkonten für diesen Katalog in Studio das Kontrollkästchen für Maschinen, die unter Windows XP ausgeführt werden.

Überlegungen zur Bereitstellung

Sie können eine Remote-PC-Zugriff-Bereitstellung erstellen und dann später konventionelle Virtual Desktop Infrastructure-Desktops (VDI) oder Anwendungen hinzufügen. Sie können auch Remote-PC-Zugriff-Desktops einer vorhandenen VDI-Bereitstellung hinzufügen.

Erwägen Sie eine Aktivierung der Microsoft-Remoteunterstützung bei der VDA-Installation auf Büro-PCs. Diese Option ermöglicht es den Helpdeskteams, die Director verwenden, Benutzersitzungen mit der Microsoft-Remoteunterstützung anzuzeigen und zu steuern.

Legen Sie fest, wie Sie den VDA auf jedem Büro-PC bereitstellen möchten. Citrix empfiehlt, eine elektronische Softwareverteilung zu verwenden, z. B. Active Directory-Skripts und Microsoft System Center Configuration Manager. Das Installationsmedium enthält Active Directory-Beispielskripts.

Lesen Sie für Remote-PC-Zugriff-Bereitstellungen den Artikel Sicherheitsüberlegungen.

Die Funktionalität für sicheren Start wird zurzeit nicht unterstützt. Deaktivieren Sie sicheren Start, wenn Sie planen, den Workstation-VDA bereitzustellen.

Jeder Büro-PC muss in der Domäne per Netzwerkkabel verbunden sein.

Windows 7 Aero wird für Büro-PCs unterstützt, ist aber nicht erforderlich.

Tastatur und Maus müssen direkt am PC oder Laptop angeschlossen werden, nicht am Bildschirm oder an anderen Komponenten, die ausgeschaltet werden können. Wenn Sie Eingabegeräte an solche Komponenten (z. B. Bildschirme) anschließen müssen, sollten diese nicht ausgeschaltet werden.

Wenn Sie Smartcards verwenden, lesen Sie den Artikel Smartcards.

Remote-PC-Zugriff kann auf den meisten Laptop-Computern verwendet werden. Für einen besseren Zugriff und die optimale Verbindung konfigurieren Sie die Energiesparoptionen bei Laptops wie die eines Desktop-PCs. Beispiel:

- Deaktivieren Sie den Ruhezustand.
- Deaktivieren Sie den Standbymodus.
- Legen Sie die Aktion beim Schließen des Deckels auf "Keine Aktion" fest.
- Legen Sie die Aktion bei Betätigen der Ein-/Ausschalttaste auf "Herunterfahren" fest.
- Deaktivieren Sie die Energiesparfunktionen der Grafikkarte.
- Deaktivieren Sie die Energiesparfunktionen der Netzwerkkarte.
- Deaktivieren Sie Akku-Energiespartechnologien.

Folgendes wird für Remote-PC-Zugriff-Geräte nicht unterstützt:

- An-/Ausdocken des Laptops.
- KVM-Switches oder andere Komponenten, die eine Sitzung trennen.
- Hybrid-PCs, einschließlich All-in-One- und NVIDIA Optimus-Laptops und -PCs.

Folgende XenDesktop-Features werden für Remote-PC-Zugriff-Bereitstellungen nicht unterstützt:

- Erstellen von Masterimages und virtuellen Maschinen
- Bereitstellen gehosteter Anwendungen
- Personal vDisks
- Clientordnerumleitung

Installieren Sie Citrix Receiver auf jedem Clientgerät mit Remotezugriff auf den Büro-PC.

Mehrere Benutzer mit Remotezugriff auf denselben Büro-PC sehen in Citrix Receiver dasselbe Symbol. Wenn ein Benutzer eine Remoteanmeldung am PC vornimmt, wird diese Ressource anderen Benutzern als nicht verfügbar angezeigt.

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.

> **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. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.
>
> HKLM\SOFTWARE\Citrix\PortICA\RemotePC "SasNotification"=dword:00000001
>
> Zur weiteren Anpassung des Verhaltens dieses Features:
> HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC
>
> RpcaMode (dword):
>
> > 1 = Remotebenutzer gewinnt immer, wenn er nicht innerhalb des angegebenen Timeouts auf die Meldung reagiert.
> >
> > 2 = Lokaler Benutzer gewinnt immer. Wenn diese Einstellung nicht festgelegt wird, gewinnt standardmäßig der Remotebenutzer.
>
> RpcaTimeout (dword):
>
> > Timeout in Sekunden für den Benutzer, bis entschieden wird, welche Art von Modus erzwungen werden soll. Wenn diese Einstellung nicht festgelegt wird, gilt der Standardwert von 30 Sekunden. Als Mindestwert sollte hier 30 Sekunden festgelegt werden. Der Benutzer muss den Computer neu starten, damit die Änderungen in Kraft treten.
> >
> > Wenn der lokale Benutzer den Zugriff auf die Konsole erzwingen möchte, kann er 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 der Computer von einem Remotebenutzer verwendet wird, wird der Remotebenutzer gefragt, ob er die Verbindung des lokalen Benutzers zulässt oder verweigert. Bei der Zulassung der Verbindung wird die Sitzung des Remotebenutzers getrennt.

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, z. B. bei witterungsbedingten Problemen.

Das Wake-On-LAN-Feature von Remote-PC-Zugriff wird auf Folgendem unterstützt:

- PCs, die Intel Active Management Technology (AMT) unterstützen.
- PCs, auf denen Wake-On-LAN im BIOS aktiviert ist.

Sie müssen Microsoft System Center Configuration Manager (ConfigMgr) 2012 konfigurieren, um das Wake-On-LAN-Feature zu verwenden. ConfigMgr bietet Zugriff auf AMT-Energiebefehle für den Computer und Unterstützung für den Aktivierungsproxy sowie Magic Packets. Wenn Sie anschließend mit Studio eine Bereitstellung für den Remote-PC-Zugriff erstellen (bzw. wenn Sie eine andere Energieverwaltungsverbindung für den Remote-PC-Zugriff hinzufügen), aktivieren Sie die Energieverwaltung und geben Sie ConfigMgr-Zugriffsinformationen an.

Beachten Sie außerdem Folgendes:

- Die Verwendung der AMT-Energieverwaltung wird aus Gründen der Sicherheit und Sitzungszuverlässigkeit zwar bevorzugt, es werden jedoch auch zwei Methoden ohne AMT unterstützt: ConfigMgr-Aktivierungsproxy und Magic Packets.
- Nur AMT-fähige Maschinen: Das Wake-On-LAN-Feature unterstützt auch die Aktionen "Herunterfahren erzwingen" und "Neustart erzwingen" von Studio und Director. Außerdem ist in StoreFront und Receiver eine Neustartaktion verfügbar.

Weitere Informationen finden Sie unter Microsoft System Center Configuration Manager und Remote-PC-Zugriff-Wake-On-LAN.

Informationen zu dem experimentellen SDK, mit dem Sie oder der Drittanbieter einer Wake-On-LAN-Lösung ohne System Center 2012 R2 einen Connector erstellen können, finden Sie unter CTX202272.

Konfigurationsreihenfolge und Überlegungen

Vor Erstellen der Remote-PC-Zugriff-Site

Wenn Sie das Energieverwaltungsfeature von Remote-PC-Zugriff ("Remote-PC-Zugriff-Wake-On-LAN") verwenden möchten, führen Sie die Konfigurationsaufgaben auf den PCs und in Microsoft System Center Configuration Manager (ConfigMgr) vor dem Erstellen der Remote-PC-Zugriff-Bereitstellung in Studio durch. Siehe Configuration Manager und Wake-On-LAN-Feature für den Remote-PC-Zugriff.

Im Assistenten für die Siteerstellung

- Wählen Sie als Sitetyp "Remote-PC-Zugriff-Site".
- Auf der Seite "Energieverwaltung" können Sie die Energieverwaltung für die Maschinen im Standardmaschinenkatalog für Remote-PC-Zugriff aktivieren oder deaktivieren. Wenn Sie die Energieverwaltung aktivieren, geben Sie ConfigMgr-Verbindungsinformationen an.
- Geben Sie auf den Seiten "Benutzer" und "Maschinenkonten" Benutzer und Maschinenkonten an.

Bei der Erstellung einer Remote-PC-Zugriff-Site werden ein Standardmaschinenkatalog unter dem Namen "Remote-PC-Zugriff-Maschinen" und eine Standardbereitstellungsgruppe unter dem Namen "Remote-PC-Zugriff-Desktops" erstellt.

Wenn Sie einen weiteren Maschinenkatalog für die Verwendung mit Remote-PC-Zugriff erstellen, gilt Folgendes:

- Wählen Sie auf der Seite "Betriebssystem" die Option "Remote-PC-Zugriff" und eine Energieverwaltungsverbindung. Das Verwenden der Energieverwaltung ist nicht obligatorisch. Wenn keine Energieverwaltungsverbindungen konfiguriert sind, können Sie nach dem Abschließen des Assistenten für die Erstellung eines Maschinenkatalogs eine erstellen (Verbindungstyp=Microsoft Configuration Manager-Wake-On-LAN) und dann den Maschinenkatalog unter Angabe der neuen Verbindung bearbeiten.
- Auf der Seite "Maschinenkonten" können Sie Maschinenkonten oder Organisationseinheiten auswählen oder hinzufügen.

Installieren Sie den VDA auf den Büro-PCs, die für lokalen und Remotezugriff verwendet werden. Normalerweise wird der VDA automatisch mit dem Verwaltungssoftwarepaket bereitgestellt. Bei Test- oder kleinen Bereitstellungen können Sie jedoch den VDA manuell auf jedem Büro-PC installieren.

Wenn der VDA installiert ist, wird der nächste Domänenbenutzer, der sich auf dem Büro-PC bei einer Konsolensitzung anmeldet (lokal oder über RDP), automatisch dem Remote-PC-Zugriff-Desktop zugewiesen. Wenn in der Konsolensitzung weitere Domänenbenutzer angemeldet werden, werden sie der Desktopbenutzerliste unter Berücksichtigung der eingerichteten Beschränkungen ebenfalls hinzugefügt.

Zum Verwenden von RDP-Verbindungen außerhalb Ihrer XenApp- bzw. XenDesktop-Umgebung müssen Sie Benutzer oder Gruppen zur Gruppe der Benutzer mit direktem Zugriff hinzufügen.

Weisen Sie die Benutzer an, auf jedem Clientgerät, das sie für den Remotezugriff auf den Büro-PC verwenden, Citrix Receiver herunterzuladen und zu installieren. Citrix Receiver ist unter http://www.citrix.com oder in den Anwendungsverteilungssystemen für unterstützte Mobilgeräte verfügbar.

Konfigurieren erweiterter Verbindungseinstellungen

Sie können eine Energieverwaltungsverbindung zum Konfigurieren der erweiterten Einstellungen bearbeiten. Sie können Folgendes aktivieren:

- ConfigMgr-Aktivierungsproxy
- Wake-On-LAN-Pakete (Magic Packets). Wenn Sie Wake-On-LAN-Pakete aktivieren, können Sie eine Wake-On-LAN-Übertragungsmethode auswählen: subnetzgesteuertes Broadcast oder Unicast.

Der PC verwendet AMT-Energiebefehle (sofern unterstützt) und alle aktivierten erweiterten Einstellungen. Wenn der PC keine AMT-Befehle verwendet, werden die erweiterten Einstellungen verwendet.

Problembehandlung

Der Delivery Controller schreibt die folgenden Diagnoseinformationen über Remote-PC-Zugriff in das Windows-Anwendungsereignisprotokoll. 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

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).

App-V

Feb 29, 2016

Mit Microsoft Application Virtualization (App-V) können Sie Anwendungen als Dienste bereitstellen, aktualisieren und unterstützen. Benutzer können auf Anwendungen zugreifen, ohne sie auf ihren Geräten installieren zu müssen. App-V und Microsoft User State Virtualization (USV) ermöglichen den Zugriff auf Anwendungen und Daten unabhängig vom Standort oder von der Internetverbindung.

Die folgende Tabelle enthält eine Liste der unterstützen Versionen. (Der App-V-Client 4.6.2 wird nicht mehr unterstützt.)

App-V	**XenDesktop-/XenApp-Version**	
	Delivery Controller	**VDA**
5.0 oder 5.0 SP1	XenDesktop 7 bis aktuelle Version XenApp 7.5 bis aktuelle Version	7.0 bis aktuelle Version
5.0 SP2	XenDesktop 7 bis aktuelle Version XenApp 7.5 bis aktuelle Version	7.1 bis aktuelle Version
5.0 SP3 und 5.1	XenDesktop 7,6 bis aktuelle Version XenApp 7.6 bis aktuelle Version	7.6.300 bis aktuelle Version

Der Offlinezugriff auf Anwendungen wird vom unterstützten App-V-Client nicht unterstützt. Die Unterstützung der App-V-Integration umfasst die Verwendung von SMB-Freigaben für Anwendungen. Das HTTP-Protokoll wird nicht unterstützt.

Anwendungen sind nahtlos verfügbar, ohne dass Vorkonfigurationen oder Änderungen an den Einstellungen des Betriebssystems vorgenommen werden müssen. App-V enthält die folgenden Komponenten:

- Verwaltungsserver: Bietet eine zentrale Konsole zum Verwalten der App-V-Infrastruktur und zum Bereitstellen von virtuellen Anwendungen für den App-V-Desktop Client und den Remotedekstopdienste-Client. Der App-V-Verwaltungsserver führt das vom Administrator benötigte Authentifizieren, Anfordern und Bereitstellen von Sicherheit, Messungen, Überwachung und Sammeln von Daten durch. Der Server verwendet Active Directory und unterstützende Tools zum Verwalten von Benutzern und Anwendungen.
- Veröffentlichungsserver: Stellt App-V-Clients Anwendungen für bestimmte Benutzer bereit und hostet das virtuelle Anwendungspaket für das Streaming. Die Pakete werden vom Verwaltungsserver abgerufen.
- Client: Ruft virtuelle Anwendungen ab, veröffentlicht die Anwendungen auf dem Client und erstellt und verwaltet automatisch virtuelle Umgebungen zur Laufzeit auf Windows-Geräten. Der App-V-Client wird auf dem Virtual Desktop Agent installiert und speichert benutzerspezifische virtuelle Anwendungseinstellungen, wie Registrierungs- und Dateiänderungen, in den Benutzerprofilen.

Sie können App-V-Anwendungen von Serverbetriebssystem- und Desktopbetriebssystem-Bereitstellungsgruppen starten:

- Über Citrix Receiver
- Vom Startmenü
- Über den App-V-Client und Citrix Receiver
- Gleichzeitig von mehreren Benutzern auf mehreren Geräten
- Über Citrix StoreFront

Geänderte App-V-Anwendungseigenschaften werden implementiert, wenn die Anwendung gestartet wird. Beispiel: Bei Anwendungen mit einem geänderten Anzeigenamen oder einem angepassten Symbol wird die Modifikation angezeigt, wenn Benutzer die Anwendung starten.

Es besteht keine Änderung in der Leistung von App-V-Anwendungen, wenn eine Desktop- und Anwendungsbereitstellungsgruppe in eine Nur-Anwendungsbereitstellungsgruppe geändert wird.

Es wird nur eine serverbasierte App-V-Bereitstellung unterstützt, in der ein Administrator mit einem App-V-Verwaltungsserver und -Veröffentlichungsserver App-V-Anwendungen verwaltet.

Konfigurieren von App-V

Bereitstellen von App-V-Anwendungen

1. Stellen Sie App-V bereit (Anweisungen siehe http://technet.microsoft.com/en-us/virtualization/hh710199).
2. Veröffentlichen Sie die App-V-Anwendungen auf dem App-V-Verwaltungsserver. Konfigurieren von Einstellungen, u. a. Berechtigungen und Dateitypzuordnung Diese Einstellungen sind bereits vorhanden, wenn Sie App-V bereits bereitgestellt haben.
3. Sie können auch die Einstellungen des App-V-Veröffentlichungsservers ändern. Weitere Informationen finden Sie weiter unten.
4. Installieren Sie den App-V-Client auf VDAs.
5. Während der Siteerstellung in Studio geben Sie die URLs des App-V-Veröffentlichungs- und App-V-Managementservers mit Portnummern an. Diese Server werden automatisch von den Bereitstellungsgruppen verwendet.
6. Installieren Sie den App-V-Client auf dem Masterimage für Maschinenkataloge. Konfigurieren Sie den Client mit Einstellungen, u. a. ShareContentStoreMode und EnablePackageScripts. (Sie müssen den App-V-Veröffentlichungsserver nicht im Masterimage konfigurieren, da er beim Anwendungsstart konfiguriert wird.)
7. Wählen Sie die App-V-Anwendungen beim Erstellen der Bereitstellungsgruppe aus.

Die Anwendungen sind jetzt verfügbar.

Sie können nach dem Erstellen einer Site die Informationen zum App-V-Server angeben oder ändern. Wählen Sie im Studio-Navigationsbereich Konfiguration > App-V-Veröffentlichung und dann Einträge im Aktionsbereich aus. Sie können App-V-Veröffentlichung mit URLs von Portnummern für die App-V-Verwaltungs- und -Veröffentlichungsserver hinzufügen. Sie können diese Adressen auch bearbeiten oder entfernen. Wenn Sie App-V-Anwendungen aktualisieren, wird angezeigt, ob ein Problem bei der Verbindung mit einem Server aufgetreten ist, und Einträge für nicht mehr verfügbare Anwendungen werden entfernt.

App-V-Veröffentlichungsservereinstellungen

Zum Ändern der Veröffentlichungsservereinstellungen empfiehlt Citrix die Verwendung der SDK-Cmdlets auf dem Controller.

- Geben Sie Get-CtxAppvServerSetting -AppVPublishingServer ein, um die Einstellungen des Veröffentlichungsservers anzuzeigen.
- Um sicherzustellen, dass App-V-Anwendungen richtig gestartet werden, geben Sie Set-CtxAppvServerSetting –UserRefreshonLogon 0 ein.

Mit dem folgenden Cmdlet werden die Einstellungen des App-V-Veröffentlichungsservers auf dem Controller geändert. Nicht alle Parameter sind obligatorisch.

Set-CtxAppvServerSetting –AppVPublishingServer -UserRefreshOnLogon -UserRefrehEnabled -UserRefreshInterval -UserRefreshIntervalUnit -GlobalRefreshOnLogon -GlobalRefresfEnabled -Gl
Hinweis: Wenn Sie zuvor GPO-Richtlinieneinstellungen für die Verwaltung der Veröffentlichungsservereinstellungen verwendet haben, werden die App-V-Integrationseinstellungen, einschließlich der

vorherigen Cmdlet-Einstellungen, von den GPO-Einstellungen überschrieben. Dies kann dazu führen, dass der Start der App-V-Anwendung fehlschlägt. Citrix empfiehlt, dass Sie alle GPO-Richtlinieneinstellungen entfernen und die gleichen Einstellungen mit dem SDK konfigurieren.

Problembehandlung

- Wenn Sie die Adresse des App-V-Verwaltungsservers und des Veröffentlichungsservers in Studio festlegen und beim Testen der Verbindung ein Fehler auftritt, prüfen Sie Folgendes:
  1. App-V-Server ist eingeschaltet: Senden Sie entweder einen Ping-Befehl oder prüfen Sie in IIS-Manager, ob für jeden Server als Zustand "Gestartet" und "Wird ausgeführt" angezeigt wird.
  2. PowerShell Remoting ist auf dem App-V-Server aktiviert. Ist dies nicht der Fall, folgen Sie den Anweisungen unter http://technet.microsoft.com/en-us/magazine/ff700227.aspx.
  3. Der App-V-Server wurde Active Directory hinzugefügt.
     Sind Studio-Maschine und App-V-Server in verschiedenen Active Directory-Domänen, zwischen denen keine Vertrauensbeziehung besteht, führen Sie über die PowerShell-Konsole auf der Studio-Maschine winrm s winrm/Config/client '@{TrustedHosts="<App-V-Server FQDN>"}' aus. Wird "TrustedHosts" über das Gruppenrichtlinienobjekt verwaltet, wird eine Fehlermeldung angezeigt, die besagt, dass die Konfigurationseinstellung "TrustedHosts" nicht geändert werden kann, da sie von Richtlinien gesteuert wird, und dass die Richtlinie auf "Nicht konfiguriert" festgelegt werden müsste, damit die Konfigurationseinstellung geändert werden kann. Wenn diese Meldung angezeigt wird, fügen Sie einen Eintrag für den App-V-Servernamen in der TrustedHosts-Richtlinie im Gruppenrichtlinienobjekt hinzu (Administrative Vorlagen > Windows-Komponenten > Windows-Remoteverwaltung (WinRM) > WinRM-Client).
  4. Der Studio-Administrator ist gleichzeitig App-V-Serveradministrator.
  5. Auf dem App-V-Server ist die Dateifreigabe aktiviert. Geben Sie hierfür in Windows-Explorer oder über den Befehl "Ausführen" Folgendes ein: \\<App-V-Server FQDN>
  6. Der App-V-Server hat dieselben Dateifreigabeberechtigungen wie der App-V-Administrator. Fügen Sie hierzu auf dem App-V-Server einen Eintrag für \\<App-V-Server FQDN> in "Gespeicherte Benutzernamen und Kennwörter" hinzu und geben Sie die Anmeldeinformationen des Benutzers ein, der Administratorberechtigungen auf dem App-V-Server hat. Weitere Informationen finden Sie unter http://support.microsoft.com/kb/306541.
- Wenn die Anwendungserkennung fehlschlägt, überprüfen Sie Folgendes:
  1. Der Studio-Administrator ist ein Administrator auf dem App-V-Verwaltungsserver.
  2. Der App-V-Verwaltungsserver wird ausgeführt. Prüfen Sie dies, indem Sie den IIS-Manager öffnen. Der Server sollte sich im Zustand "Gestartet" und "Ausgeführt" befinden.
  3. PowerShell Remoting ist auf den App-V-Servern aktiviert. Wenn es nicht aktiviert ist, folgen Sie den Anweisungen unter http://technet.microsoft.com/en-us/magazine/ff700227.aspx.
  4. Pakete haben entsprechende Sicherheitsberechtigungen, sodass der Studio-Administrator Zugriff hat.
- Wenn die App-V-Anwendungen nicht starten, überprüfen Sie Folgendes:
  1. Der Veröffentlichungsserver wird ausgeführt. Prüfen Sie dies, indem Sie den IIS-Manager öffnen. Der Server sollte sich im Zustand "Gestartet" und "Ausgeführt" befinden.
  2. App-V-Pakete haben entsprechende Sicherheitsberechtigungen, sodass Benutzer Zugriff haben.
  3. Auf dem VDA:
     - Stellen Sie sicher, dass Temp auf den richtigen Speicherort verweist und dass genügend Speicherplatz im Verzeichnis Temp verfügbar ist.
     - Stellen Sie sicher, dass der App-V-Client installiert ist, und zwar mindestens Version 5.0.
     - Stellen Sie sicher, dass Sie Administratorberechtigungen haben und Get-AppvClientConfiguration ausführen. Stellen Sie sicher, dass EnablePackageScripts auf "1" gesetzt ist. Wenn es nicht auf "1" gesetzt ist, führen Sie Set-AppvClientConfiguration -EnablePackageScripts $true aus.
       Citrix empfiehlt, dass Sie diesen Schritt beim Erstellen eines Masterimages ausführen, sodass alle VDAs, die vom Masterimage erstellt werden, die richtige Konfiguration haben.
     - Navigieren Sie im Registrierungs-Editor (regedit) zu HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\AppV. Stellen Sie sicher, dass der Schlüssel "AppVServers" den folgenden Wert hat: AppVManagementServer+metadata;PublishingServer (zum Beispiel: http://xmas-demo-appv.blrstrm.com+0+0+0+1+1+1+0+1;http://xmas-demo-appv.blrstrm.com:8082).
     - Stellen Sie sicher, dass CtxAppVCOMAdmin über Administratorrechte verfügt. Bei der Installation von VDA wird normalerweise CtxAppVCOMAdmin erstellt und der lokalen Administratorgruppe auf der VDA-Maschine hinzugefügt. Abhängig von der Active Directory-Richtlinie verliert der Benutzer u. U. die administrative Zuordnung.
       Führen Sie compmgmt.msc aus und navigieren Sie zu den Benutzern "Lokale Benutzer und Gruppen". Wenn CtxAppVCOMAdmin kein Administrator ist, bearbeiten Sie die Gruppenrichtlinie oder wenden Sie sich an den Administrator, damit das Benutzerkonto die administrative Zuordnung behält.
  4. Auf dem Masterimage, auf dem der App-V-Client installiert ist, muss "PowerShell ExecutionPolicy" auf RemoteSigned eingestellt sein, da das von Microsoft bereitgestellte App-V-Clientmodul nicht signiert ist und PowerShell mit "ExecutionPolicy" nicht signierte Skripts und Cmdlets ausführen kann. Stellen Sie "ExecutionPolicy" mit einer der folgenden Methoden ein:
     - Melden Sie sich als Administrator an und geben Sie das folgende PowerShell-Cmdlet ein: Set-ExecutionPolicy RemoteSigned.
     - Navigieren Sie in den Gruppenrichtlinieneinstellungen zu "Computerkonfiguration > Richtlinien > Administrative Vorlagen > Windows-Komponenten > Windows PowerShell> Skriptausführung aktivieren".
  5. Überprüfen Sie die Veröffentlichungsserver:
     - Führen Sie Get-AppvPublishingServer * aus, damit die Liste der Veröffentlichungsserver angezeigt wird.
     - Überprüfen Sie, ob UserRefreshonLogon auf "False" festgelegt ist. Sonst schlägt der Start der ersten App-V-Anwendung normalerweise fehl.
     - Führen Sie mit Administratorprivilegien Set-AppvPublishingServer aus und stellen Sie "UserRefreshonLogon" auf "False" ein.

  Wenn Sie mit diesen Schritten die Probleme nicht beheben können, aktivieren und prüfen Sie die Protokolle.

Aktivieren von Protokollen

Aktivieren von Studio-Protokollen

1. Erstellen Sie den Ordner C:\CtxAppvLogs.
2. Gehen Sie zu C:\Programme\Citrix\StudioAppVIntegration\SnapIn\Citrix.Appv.Admin.V1 und öffnen Sie CtxAppvCommon.dll.config als Administrator in einem Texteditor, z. B. Editor. Heben Sie die Auskommentierung der folgenden Zeile auf:

Aktivieren von VDA-Protokollen

1. Erstellen Sie den Ordner C:\CtxAppvLogs.
2. Gehen Sie zu C:\Programme\Citrix\Virtual Desktop Agent und öffnen Sie CtxAppvCommon.dll.config als Administrator in einem Texteditor, z. B. Editor. Heben Sie die Auskommentierung der folgenden Zeile auf:
3. Heben Sie die Auskommentierung der folgenden Zeile auf und stellen Sie den Wert auf "1" ein, wie im folgenden Beispiel:

   Alle mit der Konfiguration zusammenhängenden Protokolle befinden sich unter C:\CtxAppvLogs. Die Anwendungsstartprotokolle finden Sie unter:
   - XenDesktop 7.1 und höher und XenApp 7.5 und höher: %LOCALAPPDATA%\Citrix\CtxAppvLogs.
   - XenDesktop 7.0: %LocalAppData%\temp\CtxAppVLogs\

   LOCALAPPDATA wird in den lokalen Ordner des angemeldeten Benutzers aufgelöst. Prüfen Sie den lokalen Ordner des Benutzers, für den der Anwendungsstart fehlschlägt.
4. Starten Sie als Administrator den Brokerdienst oder die VDA-Maschine neu, damit die Protokollierung gestartet wird.

Lokaler App-Zugriff und URL-Umleitung

Feb 29, 2016

Dieser Abschnitt enthält folgende Themen:

Einführung

Durch lokalen App-Zugriff werden lokal installierte Windows-Anwendungen problemlos in eine gehostete Desktopumgebung integriert, ohne dass ein Wechsel zwischen Computern nötig ist. Lokaler App-Zugriff ermöglicht Folgendes:

- Direkter Zugriff von virtuellen Desktops auf Anwendungen, die lokal auf einem Laptop, PC oder einem anderen Gerät installiert sind
- Bereitstellung einer flexiblen Anwendungsbereitstellungslösung Wenn Benutzer lokale Anwendungen haben, die Sie nicht virtualisieren können oder die IT nicht verwaltet, verhalten sich diese Anwendungen weiterhin so, als ob sie auf einem virtuellen Desktop installiert wären.
- Eliminieren Sie Doppelhoplatenz bei separat vom virtuellen Desktop gehosteten Anwendungen, indem Sie eine Verknüpfung mit der veröffentlichten Anwendung auf das Windows-Gerät des Benutzers platzieren.
- Unter anderem können die folgenden Anwendungen verwendet werden:
  - Videokonferenzsoftware, z. B. GoToMeeting.
  - Spezial- oder Nischenanwendungen, die noch nicht virtualisiert sind.
  - Anwendungen und Peripheriegeräte, die andernfalls große Datenmengen von einem Benutzergerät zum Server und zurück zum Benutzergerät senden würden, wie DVD-Brenner und TV-Tuner.

In XenApp und XenDesktop verwenden gehostete Desktopsitzungen die URL-Umleitung zum Starten von lokalen App-Zugriff-Anwendungen. Durch URL-Umleitung wird die Anwendung unter mehr als einer URL-Adresse bereitgestellt. Durch Auswählen eingebetteter Links in einem Browser in einer Desktopsitzung wird ein lokaler Browser gestartet (basierend auf der URL-Sperrliste des Browsers). Wenn Sie auf eine URL klicken, die nicht auf der Sperrliste steht, wird die URL erneut in der Sitzung geöffnet.

Die URL-Umleitung funktioniert nur in Desktopsitzungen und nicht in Anwendungssitzungen. Für Anwendungssitzungen können Sie nur Host-zu-Client-Inhaltsumleitung verwenden, wobei es sich um eine Art von Server-Dateitypzuordnung handelt. Diese FTA leitet bestimmte Protokolle an den Client um, z. B. HTTP, HTTPS, RTSP oder MMS. Wenn Sie beispielsweise nur eingebettete Links mit HTTP öffnen, werden die Links direkt in der Clientanwendung geöffnet. Für diese Art der Umleitung wird keine URL-Sperrliste oder URL-Positivliste unterstützt.

Wenn der lokale App-Zugriff aktiviert ist, werden URLs, die Benutzern als Links von lokal ausgeführten Anwendungen oder von Benutzern gehosteten Anwendungen bzw. als Verknüpfungen auf dem Desktop angezeigt werden, auf eine der folgenden Arten umgeleitet:

- Umleitung vom Computer des Benutzers zum gehosteten Desktop
- Umleitung vom XenApp- bzw. XenDesktop-Server auf den Computer des Benutzers
- Wiedergabe in der Umgebung, in der sie gestartet werden (keine Umleitung)

Zur Angabe des Pfads für die Inhaltsumleitung von bestimmten Websites konfigurieren Sie die URL-Positivliste und die URL-Sperrliste auf dem Virtual Delivery Agent. Diese Listen enthalten mehrteilige Registrierungsschlüssel, die die Richtlinieneinstellungen für die URL-Umleitung festlegen; weitere Informationen hierzu finden Sie unter "Einstellungen der Richtlinie 'Lokaler App-Zugriff'".

Mit den folgenden Ausnahmen können URLs auf dem VDA wiedergegeben werden:

- Regions-/Gebietsschemainformationen: Websites, die Gebietsschemainformationen benötigen, wie msn.com oder news.google.com (je nach Region wird eine bestimmte Seite geöffnet). Wenn VDA beispielsweise von einem Datenzentrum in Großbritannien bereitgestellt wird und der Client eine Verbindung aus Indien herstellt, würde der Benutzer erwarten, dass die Website in.msn.com erscheint, es wird jedoch uk.msn.com angezeigt.
- Multimedia-Inhalt: Websites mit Rich-Media-Inhalten, die auf dem Clientgerät wiedergegeben werden, ermöglichen eine gewohnte Benutzererfahrung und das Einsparen von Bandbreite während die Funktionalität auch in Netzwerken mit hoher Latenz gewährleistet ist. Die Flash-Umleitung wird durch die Umleitung von Sites mit anderen Medientypen wie Silverlight ergänzt. Somit ist die Umgebung sehr sicher. Die vom Administrator genehmigten URLs werden auf dem Client ausgeführt, während die restlichen URLs an VDA weitergeleitet werden.

Neben der URL-Umleitung können Sie auch FTA-Umleitung (File Type Association = Dateitypzuordnung) verwenden. FTA startet lokale Anwendungen, wenn Dateien in einer Sitzung geöffnet werden sollen. Wenn die lokale Anwendung gestartet wird, muss sie Zugriff auf die Datei haben, um sie zu öffnen. Daher können Sie mit lokalen Anwendungen nur Dateien öffnen, die sich auf Netzwerkfreigaben oder auf Clientlaufwerken (mit Clientlaufwerkzuordnung) befinden. Wenn beispielsweise der PDF-Reader eine lokale Anwendung ist und eine PDF-Datei geöffnet werden soll, wird zum Öffnen der Datei der lokale PDF-Reader verwendet. Da die lokale Anwendung direkt auf die Datei zugreifen kann, erfolgt keine Netzwerkübertragung über ICA zum Öffnen der Datei.

Anforderungen, Faktoren und Einschränkungen

Lokaler App-Zugriff wird auf den gültigen Betriebssystemen für VDAs für Windows-Serverbetriebssysteme und VDAs für Windows-Desktopbetriebssysteme unterstützt und erfordert mindestens Citrix Receiver für Windows Version 4.1. Die folgenden Browser werden unterstützt:

- Internet Explorer 8, 9, 10 und 11
- Firefox 3.5 bis 21.0
- Chrome 10

Beachten Sie die folgenden Punkte und Einschränkungen, wenn Sie lokalen App-Zugriff und URL-Umleitung verwenden.

- Lokaler App-Zugriff ist für virtuelle Desktops im Vollbildmodus unter Einbeziehung aller Monitore gedacht:
  - Die Benutzererfahrung kann beeinträchtigt werden, wenn lokaler App-Zugriff auf einem virtuellen Desktop verwendet wird, der im Fenstermodus ausgeführt wird oder der nicht auf allen Monitoren ausgeführt wird.
  - Bei der Verwendung mehrerer Monitore ist der maximierte Monitor der Standarddesktop für alle Anwendungen, die in der Sitzung gestartet werden, selbst wenn nachfolgende Anwendungen normalerweise auf einem anderen Monitor starten würden.
  - Das Feature unterstützt einen VDA; es ist keine Integration mit mehreren gleichzeitigen VDAs möglich.
- Einige Anwendungen können sich unerwartet verhalten und Benutzer beeinträchtigen:
  - Benutzer können die Laufwerkbuchstaben verwechseln, z. B. das lokale C:-Laufwerk mit dem virtuellen C:-Desktoplaufwerk.
  - Auf virtuellen Desktops verfügbare Drucker sind nicht für die lokalen Anwendungen verfügbar.

- Anwendungen, die erweiterte Berechtigungen erfordern, können nicht als clientgehostete Anwendungen gestartet werden.
- Keine spezielle Behandlung von Anwendungen mit einer Instanz (z. B. Windows Media Player).
- Lokale Anwendungen werden mit dem Windows-Design des lokalen Computers angezeigt.
- Vollbildanwendungen werden nicht unterstützt. Dies schließt Anwendungen ein, die im Vollbildmodus geöffnet werden, z. B. PowerPoint-Bildschirmpräsentationen oder Fotoanzeigen, die den gesamten Desktop ausfüllen.
- Lokaler App-Zugriff kopiert die Eigenschaften der lokalen Anwendung (z. B. die Verknüpfungen auf dem Clientdesktop und im Startmenü) auf dem VDA. Es werden jedoch keine anderen Eigenschaften, wie Tastenkombinationen und schreibgeschützte Attribute, kopiert.
- Anwendungen, die die Reihenfolge der überlappenden Fenster anpassen, können unvorhersehbare Ergebnisse verursachen. Beispielsweise könnten einige Fenster ausgeblendet werden.
- Verknüpfungen, einschließlich Arbeitsplatz, Papierkorb, Systemsteuerung, Netzlaufwerkverknüpfungen und Ordnerverknüpfungen werden nicht unterstützt.
- Die folgenden Dateitypen und Dateien werden nicht unterstützt: benutzerdefinierte Dateitypen, Dateien ohne zugeordnete Programme, ZIP-Dateien und ausgeblendete Dateien.
- Taskleistengruppierung wird nicht für gemischte 32-Bit und 64-Bit clientgehostete Anwendungen und VDA-Anwendungen unterstützt, z. B. die Gruppierung von 32-Bit-Versionen lokaler Anwendungen mit 64-Bit-VDA-Anwendungen.
- Anwendungen können nicht über COM gestartet werden. Beispiel: Wenn Sie auf ein eingebettetes Office-Dokument in einer Office-Anwendung klicken, wird der Prozessstart nicht erkannt und die Integration der lokalen Anwendung schlägt fehl.

- Die URL-Umleitung unterstützt nur explizite URLs, d. h. solche, die in der Adressleiste des Browsers angezeigt werden oder mit der browserinternen Suchfunktion gefunden wurden (je nach Browser).
- Die URL-Umleitung funktioniert nur in Desktopsitzungen und nicht in Anwendungssitzungen.
- Benutzer haben keine Berechtigung, im lokalen Desktopordner in einer VDA-Sitzung neue Dateien zu erstellen.
- Mehrere Instanzen einer lokal ausgeführten Anwendung verhalten sich entsprechend den Taskleisteneinstellungen für den virtuellen Desktop. Verknüpfungen zu lokal ausgeführten Anwendungen werden jedoch nicht mit ausgeführten Instanzen dieser Anwendungen gruppiert. Sie werden auch nicht mit ausgeführten Instanzen von gehosteten Anwendungen oder mit an gehosteten Anwendungen angehefteten Verknüpfungen gruppiert. Benutzer können nur Fenster von lokal ausgeführten Anwendungen von der Taskleiste aus schließen. Zwar können Benutzer die Fenster von lokalen Anwendungen in der Desktop-Taskleiste und im Startmenü anheften, jedoch starten die Anwendungen bei Verwendung dieser Verknüpfungen möglicherweise nicht konsistent.

Interaktion mit Windows

Bei der Interaktion zwischen lokaler App-Zugriff und Windows tritt u. a. das folgende Verhalten auf.

- Verknüpfungen in Windows 8 und Windows Server 2012
  - Windows Store-Apps, die auf dem Client installiert sind, werden nicht als Teil der Verknüpfungen von lokalem App-Zugriff aufgelistet.
  - Bild- und Videodateien werden normalerweise standardmäßig mit Windows Store-Apps geöffnet. Lokaler App-Zugriff listet die Windows Store-Apps jedoch auf und öffnet Verknüpfungen mit Desktopanwendungen.
- Local Programs
  - In Windows 7 ist der Ordner im Startmenü verfügbar.
  - In Windows 8 ist der Ordner "Local Programs" nur verfügbar, wenn der Benutzer **Alle Apps** als Kategorie auf der Startseite auswählt. Nicht alle Unterordner werden in Local Programs angezeigt.

- Windows 8-Grafikfunktionen für Anwendungen
  - Desktopanwendungen sind auf den Desktopbereich beschränkt und werden von der Startseite bzw. Anwendungen im Windows 8-Stil vollständig abgedeckt.
  - Mit lokalem App-Zugriff verwendete Anwendungen verhalten sich jedoch bei der Verwendung von mehreren Monitoren nicht wie Desktopanwendungen. Bei der Verwendung mehrerer Monitore werden die Startseite und der Desktop auf unterschiedlichen Monitoren angezeigt.
- Windows 8 und lokaler App-Zugriff mit URL-Umleitung
  - Da bei Windows 8 Internet Explorer keine Add-Ons aktiviert sind, müssen Sie den Desktop-Internet Explorer zum Aktivieren von URL-Umleitung verwenden.
  - In Windows Server 2012 werden Add-Ons von Internet Explorer standardmäßig deaktiviert. Um URL-Umleitung zu implementieren, deaktivieren Sie die verstärkte Sicherheitskonfiguration für Internet Explorer. Setzen Sie die Internet Explorer-Optionen zurück und starten Sie das Programm neu, um sicherzustellen, dass Add-Ons für Standardbenutzer aktiviert sind.

Konfigurieren von lokalem App-Zugriff und URL-Umleitung

Verwenden von lokalem App-Zugriff und URL-Umleitung für Citrix Receiver:

- Installieren Sie Citrix Receiver auf dem lokalen Clientcomputer. Sie können beide Features während der Installation von Citrix Receiver aktivieren. Alternativ können Sie die Vorlage für den lokalen App-Zugriff mit dem Gruppenrichtlinien-Editor aktivieren.
- Legen Sie die Richtlinieneinstellung für **Lokalen App-Zugriff zulassen** auf **Aktiviert** fest. Sie können zudem URL-Positivlisten- und Sperrlisten-Richtlinieneinstellungen für die URL-Umleitung konfigurieren. Weitere Informationen finden Sie unter Einstellungen der Richtlinie "Lokaler App-Zugriff".

Aktivieren des lokalen App-Zugriffs und der URL-Umleitung bei der Installation von Citrix Receiver

Aktivieren des lokalen App-Zugriffs und der URL-Umleitung für alle lokalen Anwendungen:

1. Legen Sie die Richtlinieneinstellung für **Lokalen App-Zugriff zulassen** auf **Aktiviert** fest. Mit dieser Einstellung überlässt der VDA dem Client die Entscheidung darüber, ob vom Administrator veröffentlichte Anwendungen und Verknüpfungen für den lokalen App-Zugriff in der Sitzung aktiviert sind. (Wenn die Einstellung deaktiviert ist, sind sowohl vom Administrator veröffentlichte Anwendungen als auch Verknüpfungen für den lokalen App-Zugriff für den VDA deaktiviert.) Diese Richtlinie gilt für den gesamten Computer als auch für die URL-Umleitungsrichtlinie.
2. Aktivieren Sie den lokalen App-Zugriff und die URL-Umleitung für alle Benutzer eines Computers, wenn Sie Citrix Receiver installieren. Bei dieser Aktion werden die für URL-Umleitung erforderlichen Browser-Add-Ons registriert. Führen Sie an der Eingabeaufforderung den jeweiligen Befehl zum Installieren von Receiver mit der folgenden Option aus:

   CitrixReceiver.exe /ALLOW_CLIENTHOSTEDAPPSURL=1

   CitrixReceiverWeb.exe /ALLOW_CLIENTHOSTEDAPPSURL=1

Aktivieren der Vorlage für den lokalen App-Zugriff mit dem Gruppenrichtlinien-Editor

1. Führen Sie **gpedit.msc** aus.
2. Wählen Sie den Knoten **Computerkonfiguration**. Klicken Sie mit der rechten Maustaste auf **Administrative Vorlagen**

und wählen Sie **Vorlagen hinzufügen/entfernen > Hinzufügen** aus.
3. Fügen Sie die Vorlage icaclient.adm im Citrix Receiver-Konfigurationsordner (normalerweise unter C:\Programme (x86)\Citrix\Online Plugin\Configuration) hinzu. (Nach dem Hinzufügen der Vorlage icaclient.adm zur Computerkonfiguration steht diese auch in der Benutzerkonfiguration zur Verfügung.)
4. Erweitern Sie **Administrative Vorlagen > Klassische administrative Vorlage (ADM) > Citrix Komponenten > Citrix Receiver > Benutzerauthentifizierung**.
5. Wählen Sie **Einstellungen für lokalen App-Zugriff**.
6. Wählen Sie **Aktiviert** und anschließend **URL-Umleitung zulassen**. Registrieren Sie für die URL-Umleitung Browser-Add-Ons über die Befehlszeile wie unten erläutert.

Ermöglichen von Zugriff ausschließlich auf veröffentlichte Anwendungen

Ermöglichen von Zugriff ausschließlich auf veröffentlichte Anwendungen:

1. Führen Sie auf dem Server, auf dem der Delivery Controller installiert ist, **regedit.exe** aus.
   1. Navigieren Sie zu HKLM\Software\Wow6432Node\Citrix\DesktopStudio.
   2. Fügen Sie den REG_DWORD-Eintrag ClientHostedAppsEnabled mit dem Wert 1 hinzu. (Durch den Wert 0 wird der lokale App-Zugriff deaktiviert.)
2. Starten Sie den Delivery Controller-Server neu und starten Sie dann Studio neu.
3. Veröffentlichen Sie lokale App-Zugriff-Anwendungen.
   1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen** und dann die Registerkarte "Anwendungen".
   2. Wählen Sie im Aktionsbereich **Anwendung mit lokalem Zugriff erstellen**.
   3. Wählen Sie die Desktopbereitstellungsgruppe.
   4. Geben Sie den vollständigen Pfad der ausführbaren Datei der Anwendung auf dem lokalen Computer des Benutzers ein.
   5. Geben Sie an, ob die Verknüpfung mit der lokalen Anwendung auf dem virtuellen Desktop im Startmenü, auf dem Desktop oder beiden angezeigt wird.
   6. Akzeptieren Sie die Standardwerte auf der Seite "Name" und überprüfen Sie die Einstellungen.
4. Aktivieren Sie den lokalen App-Zugriff und die URL-Umleitung für alle Benutzer eines Computers, wenn Sie Citrix Receiver installieren. Bei dieser Aktion werden die für URL-Umleitung erforderlichen Browser-Add-Ons registriert. Führen Sie an der Eingabeaufforderung den Befehl zum Installieren von Citrix Receiver mit der folgenden Option aus:
   CitrixReceiver.exe /ALLOW_CLIENTHOSTEDAPPSURL=1
   CitrixReceiverWeb.exe /ALLOW_CLIENTHOSTEDAPPSURL=1
5. Legen Sie die Richtlinieneinstellung für **Lokalen App-Zugriff zulassen** auf **Aktiviert** fest. Mit dieser Einstellung überlässt der VDA dem Client die Entscheidung darüber, ob vom Administrator veröffentlichte Anwendungen und Verknüpfungen für den lokalen App-Zugriff in der Sitzung aktiviert sind. (Wenn die Einstellung deaktiviert ist, sind sowohl vom Administrator veröffentlichte Anwendungen als auch Verknüpfungen für den lokalen App-Zugriff für den VDA deaktiviert.)

Registrieren von Browser-Add-Ons

Hinweis: Die für URL-Umleitung erforderlichen Browser-Add-Ons werden automatisch registriert, wenn Sie Citrix Receiver 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*>
- Registrierung von Add-Ons auf einem Clientgerät aufheben: <*client-installation-folder*>\redirector.exe /unreg<*browser*>
- Registrieren von Add-Ons auf einem VDA: <*VDAinstallation-folder*>\VDARedirector.exe /reg<*browser*>

- Registrierung von Add-Ons auf einem VDA aufheben: <*VDAinstallation-folder*>\VDARedirector.exe /unreg<*browser*>

<*browser*> kann "IE", "FF", "Chrome" oder "All" sein.

Beispiel: Mit dem folgenden Befehl werden Internet Explorer-Add-Ons auf einem Gerät mit Citrix Receiver registriert.

```
C:\Programme\Citrix\ICA Client\redirector.exe/regIE
```

Mit dem folgenden Befehl werden alle Add-Ons auf einem VDA für Windows-Serverbetriebssysteme registriert.

```
C:\Programme (x86)\Citrix\System32\VDARedirector.exe /regAll
```

URL-Abfang in Browsern

- Standardmäßig wird die eingegebene URL von Internet Explorer umgeleitet. Wenn die URL nicht in der Sperrliste enthalten ist, aber vom Browser oder der Website an eine andere URL-Adresse umgeleitet wird, wird die endgültige URL nicht umgeleitet, selbst wenn sie auf der Sperrliste steht.

  Zum richtigen Funktionieren der URL-Umleitung müssen Sie bei entsprechender Aufforderung durch den Browser das Add-On aktivieren. Wenn die mit Internetoptionen verbundenen Add-Ons bzw. die angeforderten Add-Ons deaktiviert sind, funktioniert die URL-Umleitung nicht richtig.

- Firefox-Add-Ons leiten URLs immer um.

  Wenn ein Add-On installiert wurde, bietet Firefox auf einer neuen Registerkarte die Möglichkeit, die Add-On-Installation zuzulassen oder zu verhindern. Sie müssen das Add-On zulassen, 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

1. Führen Sie auf dem gehosteten Desktop **gpedit.msc** aus.
2. Navigieren Sie zu HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Client Hosted Apps\Policies\Session State. Bei einem 64-Bit-System, navigieren Sie zu der Registrierungsstruktur HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Citrix\Client Hosted Apps\Policies\Session State.
3. Fügen Sie den REG_DWORD-Eintrag "Terminate" mit einem der folgenden Werte hinzu:
   - 1: Lokale Anwendungen werden weiterhin ausgeführt, wenn sich ein Benutzer abmeldet oder die Verbindung zum virtuellen Desktop trennt. Bei der Wiederverbindung werden lokale Anwendungen wieder integriert, wenn sie in der lokalen Umgebung verfügbar sind.
   - 3: Lokale Anwendungen werden geschlossen, wenn sich ein Benutzer abmeldet oder die Verbindung zum virtuellen Desktop trennt.

Server-VDI

Feb 29, 2016

Verwenden Sie das Server-VDI-Feature (Virtual Desktop Infrastructure), um einen Desktop von einem Serverbetriebssystem einem einzelnen Benutzer bereitzustellen.

- Enterprise-Administratoren können Serverbetriebssysteme als VDI-Desktops bereitstellen. Dies ist für Benutzer, z. B. Techniker und Designer, nützlich.
- Dienstanbieter können Desktops von der Cloud anbieten. Diese Desktops entsprechen dem Microsoft Services Provider License Agreement (SPLA).

Mit der Citrix Richtlinieneinstellung "Enhanced Desktop Experience" können Sie das Serverbetriebssystem wie ein Windows 7-Betriebssystem aussehen lassen.

Die folgenden Features können nicht mit der Server-VDI verwendet werden:

- Personal vDisks
- HDX 3D Pro
- Gehostete Anwendungen
- Lokaler App-Zugriff
- Direkte (nicht vermittelte) Desktopverbindungen
- Remote-PC-Zugriff

Server-VDI wird auf den gleichen Serverbetriebssystemen wie der VDA für Windows Serverbetriebssysteme unterstützt.

1. Bereiten Sie den Windows-Server auf die Installation vor: Stellen Sie sicher, dass die Rollendienste "Remotedesktopdienste" nicht installiert sind, und dass Benutzer auf eine Sitzung eingeschränkt sind:
   - Stellen Sie mit dem Windows-Server-Manager sicher, dass die Rollendienste für Remotedesktopdienste nicht installiert sind. Wenn sie installiert sind, entfernen Sie die Dienste.
   - Stellen Sie sicher, dass die Eigenschaft "Nur eine Sitzung pro Benutzer zulassen" aktiviert ist.
     - Unter Windows Server 2008 R2 greifen Sie auf diese Eigenschaft über Verwaltung > Remotedesktopdienste > Remotedesktop-Sitzungshostkonfiguration zu. Im Abschnitt "Einstellungen bearbeiten > Allgemein" muss die Einstellung Nur eine Sitzung pro Benutzer zulassen auf Ja festgelegt sein.
     - Unter Windows Server 2012 bearbeiten Sie die Registrierung und stellen Sie die Terminalservereinstellung ein. Legen Sie für den Registrierungsschlüssel HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer den Eintrag DWORD fSingleSessionPerUser auf 1 fest.
2. Installieren Sie für Windows Server 2008 R2 Microsoft .NET Framework 3.5 SP1 auf dem Server, bevor Sie den VDA installieren.
3. Installieren Sie einen VDA über die Befehlszeilenschnittstelle mit den Optionen "/quiet" und "/servervdi" auf einem unterstützten Server oder einem Servermasterimage. (In der Standardeinstellung blockiert das Installationsprogramm den VDA für Windows-Desktopbetriebssysteme auf einem Serverbetriebssystem. Mit der Befehlszeile überschreiben Sie dieses Verhalten.)
   XenDesktopVdaSetup.exe /quiet /servervdi

   Sie können den oder die Delivery Controller bei der VDA-Installation über die Befehlszeile mit der Option **/controller** festlegen.

   Öffnen Sie mit der Option **/enable_hdx_ports** Ports in der Firewall, wenn die Firewall nicht manuell konfiguriert wird.

   Fügen Sie die Option **/masterimage** hinzu, wenn Sie den VDA auf einem Image installieren, und verwenden Sie MCS zum

Erstellen von Server-VMs von diesem Image.

Schließen Sie keine Optionen für Features ein, die nicht mit Server-VDI unterstützt werden, u. a. /baseimage, /enable_hdx_3d_pro oder /xa_server_location.

4. Erstellen Sie einen Maschinenkatalog für Server-VDI.
   1. Klicken Sie auf der Seite Betriebssystem auf **Desktopbetriebssystem**.
   2. Geben Sie auf der Seite Zusammenfassung einen Maschinenkatalognamen und eine Beschreibung für Administratoren an, die ausdrücklich Server-VDI angeben. Dies ist die einzige Angabe in Studio, dass der Katalog Server-VDI unterstützt.

   Wenn Sie eine Suche in Studio durchführen, wird der erstellte Server-VDI-Katalog auf der Registerkarte "Desktopbetriebssystemmaschinen" angezeigt, obwohl der VDA auf einem Server installiert wurde.

5. Erstellen Sie eine Bereitstellungsgruppe und weisen Sie den Server-VDI-Katalog zu, den Sie im letzten Schritt erstellt haben.

Wenn Sie während der Installation des VDA keinen Delivery Controller festgelegt haben, geben sie ihn später über eine Citrix Richtlinieneinstellung, Active Directory oder durch Bearbeiten der Registrierungswerte des VDA-Computers an.

Personal vDisk

Feb 29, 2016

Das Personal vDisk-Feature bietet die Einzelimageverwaltung für gepoolte und gestreamte Desktops, während Benutzer Anwendungen installieren und ihre Desktopeinstellungen anpassen können. Im Gegensatz zu traditionellen Virtual Desktop Infrastructure (VDI)-Bereitstellungen mit gepoolten Desktops, bei denen Benutzer Anpassungen und eigene Anwendungen verlieren, wenn der Administrator das Masterimage ändert, werden in Bereitstellungen mit persönlichen vDisks diese Änderungen beibehalten. Dies bedeutet, dass Administratoren die Masterimages auf einfache Weise zentral verwalten können, während Benutzer gleichzeitig von einer individuell angepassten Desktoperfahrung profitieren.

Persönliche vDisks erreichen diese Trennung, indem Sie alle auf der VM des Benutzers vorgenommenen Änderungen an einen separaten Datenträger, die persönliche vDisk, weiterleiten, die mit der VM des Benutzers verknüpft ist. Der Inhalt der persönlichen vDisk wird zur Laufzeit mit dem Inhalt des Masterimages zusammengeführt, um eine einheitliche Erfahrung zu gewährleisten. Auf diese Weise können Benutzer immer noch auf die Anwendungen zugreifen, die der Administrator auf dem Masterimage zur Verfügung gestellt hat.

Persönliche vDisks bestehen aus zwei Teilen, die unterschiedliche Laufwerksbuchstaben verwenden und ungefähr gleich groß sind:

- Benutzerprofil: Dieser Teil enthält Benutzerdaten, Dokumente und das Benutzerprofil. Standardmäßig wird hierfür Laufwerk P: verwendet, Sie können aber einen anderen Laufwerksbuchstaben wählen, wenn Sie einen Maschinenkatalog mit Maschinen erstellen, die persönliche vDisks verwenden. Das verwendete Laufwerk hängt auch von der Einstellung für EnableUserProfileRedirection ab.
- Virtual Hard Disk-Datei (.vhd): Dieser Teil enthält alle anderen Objekte, z. B. Anwendungen, die unter C:\Programme installiert sind. Dieser Teil wird nicht in Windows Explorer angezeigt und benötigt seit Version 5.6.7 keinen Laufwerksbuchstaben.

Mit persönlichen vDisks können Anwendungen auf Abteilungsebene bereitgestellt werden und sie unterstützen auch Anwendungen, die von Benutzern heruntergeladen und installiert wurden, einschließlich solcher, für die Treiber (außer Phase-1-Treiber), Datenbanken und Maschinenverwaltungssoftware erforderlich ist. Wenn die Änderung eines Benutzers mit der Änderung eines Administrators kollidiert, können diese Änderungen mit einer persönlichen vDisk leicht und automatisch abgestimmt werden.

Außerdem können lokal verwaltete Anwendungen (z. B. solche, die von lokalen IT-Abteilungen bereitgestellt werden) auch in der Umgebung des Benutzers bereitgestellt werden. Der Benutzer bemerkt keine Unterschiede bei der Verwendung; mit persönlichen vDisks wird sichergestellt, dass alle Änderungen und alle installierten Anwendungen auf der vDisk gespeichert werden. In Fällen, bei denen eine Anwendung auf einer persönlichen vDisk genau mit einer Anwendung auf einem Masterimage übereinstimmt, wird die Version auf der persönlichen vDisk aus Platzspargründen verworfen, ohne dass der Benutzer den Zugriff auf die Anwendung verliert.

Persönliche vDisks werden physisch auf dem Hypervisor gespeichert, sie müssen sich aber nicht am gleichen Speicherort befinden wie andere auf dem virtuellen Desktop bereitgestellte Datenträger. Dadurch können sich die Kosten für persönlichen vDisk-Speicher verringern.

Wenn Sie während der Site-Erstellung eine Verbindung erstellen, legen Sie Speicherorte für die Datenträger fest, die von den virtuellen Maschinen verwendet werden. Sie können die persönlichen vDisks von den Datenträgern für das Betriebssystem trennen. Jede VM muss Zugriff auf den Speicherort der beiden Datenträger haben. Wenn Sie für beide lokalen Speicher verwenden, muss der Hypervisor in der Lage sein, auf beide zuzugreifen. Um dies zu gewährleisten, bietet Studio nur

kompatible Speicherorte an. Später können Sie auch über "Konfiguration > Hosting" in Studio persönliche vDisks und Speicher dafür vorhandenen Hosts (aber nicht Maschinenkatalogen) hinzufügen.

Erstellen Sie regelmäßig ein Backup der persönlichen vDisks mit der bevorzugten Methode. vDisks sind standardmäßige Volumes in der Speicherebene eines Hypervisors. Sie können genauso wie andere Volumes gesichert werden.

Neue Features in Personal vDisk 7.6.1

Dieses Release enthält folgende Verbesserungen:

- Diese Version von Personal vDisk enthält Leistungsverbesserungen, durch die die zum Anwenden eines Imageupdates auf einen Personal vDisk-Katalog benötigte Zeit verkürzt wird.

Die folgenden Probleme wurden in diesem Release behoben:

- Bei dem Versuch, eine Basis-VM mit einem direkten Upgrade von Microsoft Office 2010 auf Microsoft Office 2013 zu aktualisieren, wurde dem Benutzer ein Konfigurationsfenster gefolgt von der folgenden Fehlermeldung angezeigt: "Error 25004. The product key you entered cannot be used on this machine." Zuvor wurde in diesem Fall empfohlen, Office 2010 auf der Basis-VM zu deinstallieren und danach Office 2013 zu installieren. Jetzt ist es nicht mehr nötig, Office 2010 beim Durchführen eines direkten Upgrades auf der Basis-VM zu deinstallieren (#391225).
- Wenn während eines Imageupdates eine höhere Version von Microsoft .Net auf der persönlichen vDisk des Benutzers gefunden wurde, wurde diese vom Basisimage mit einer niedrigeren Version überschrieben. Dies führte für Benutzer zu Problemen beim Ausführen bestimmter, auf ihrer persönlichen vDisk installierter Anwendungen, die eine höhere Version, z. B. Visual Studio, benötigten (#439009).
- Ein mit Provisioning Services bereitgestellter Datenträger, auf dem Personal vDisk installiert und aktiviert ist, kann nicht zum Erstellen eines nicht-Personal vDisk-Maschinenkatalogs verwendet werden. Diese Einschränkung wurde entfernt (#485189).

Info zu Personal vDisk 7.6

Neue Features in Version 7.6:

- Verbesserte Fehlerbehandlung und Berichterstellung für Personal vDisk. Wenn Sie in Studio PvD-aktivierte Maschinen in einem Katalog anzeigen, können Sie auf der Registerkarte "PvD" den Überwachungsstatus während Imageupdates sowie die geschätzte Abschlusszeit und den Fortschritt verfolgen. Außerdem wurden die Zustandsanzeigen verbessert.
- Ein Überwachungstool für PvD-Imageupdates ist für frühere Versionen auf dem ISO-Medium verfügbar (ISO\Support\Tools\Scripts\PvdTool). Überwachungsfunktionen wurden auch in früheren Releases unterstützt, jedoch sind die Berichterstellungsfunktionen nicht so robust wie im aktuellen Release.
- Im Provisioning Services-Testmodus können Sie Maschinen mit einem aktualisierten Image in einem Testkatalog starten. Nachdem Sie die Stabilität überprüft haben, können Sie die Testversion der persönlichen vDisk auf "Production" hochstufen.
- Mit einer neuen Funktion können Sie das Delta (die Differenz) zwischen zwei Beständen während einer Bestandsaktualisierung berechnen statt sie für jeden PvD-Desktop einzeln berechnen zu müssen. Es sind neue Befehle zum Exportieren und Importieren eines vorherigen Bestands für MCS-Kataloge verfügbar. (Provisioning Services-Master-vDisks haben bereits den vorherigen Bestand.)

Bekannte Probleme aus Version 7.1.3, die in Version 7.6 behoben wurden:

- Unterbrechen des Upgrades einer Personal vDisk-Installation kann dazu führen, dass eine vorhandene Personal vDisk-Installation beschädigt wird. [#424878]
- Ein virtueller Desktop reagiert möglicherweise nicht mehr, wenn die persönliche vDisk über einen langen Zeitraum ausgeführt wird und es zu einem Speicherverlust im nicht-ausgelagerten Speicher kommt. [#473170]

Neue bekannten Probleme in Version 7.6:

- Das Vorhandensein von Antivirenprodukten kann sich darauf auswirken, wie lange das Durchführen einer Bestandsaktualisierung oder eines Updates dauert. Die Leistung kann verbessert werden, wenn Sie CtxPvD.exe und CtxPvDSvc.exe der PROCESS-Ausschlussliste des Antivirenprodukts hinzufügen. Diese Dateien befinden sich im Ordner C:\Programme\Citrix\personal vdisk\bin. [#326735]
- Feste Links zwischen Dateien, die vom Masterimage geerbt wurden, bleiben in persönlichen vDisk-Katalogen nicht erhalten. [#368678]
- Nach dem Upgrade von Office 2010 auf 2013 auf dem Personal vDisk-Masterimage kann Office nicht auf virtuellen Maschinen gestartet werden, da der KMS-Lizenzierungsproduktschlüssel von Office beim Upgrade entfernt wurde. Als Workaround können Sie Office 2010 deinstallieren und Office 2013 auf dem Masterimage neu installieren. [#391225]
- Personal vDisk-Kataloge unterstützen keine VMware Paravirtual SCSI (PVSCSI)-Controller. Verwenden Sie den Standardcontroller, um dieses Problem zu vermeiden. [#394039]
- Für virtuelle Desktops, die mit Personal vDisk Version 5.6.0 erstellt wurden und auf 7 aktualisiert werden, finden Benutzer, die sich an der Master-VM anmelden, nicht alle Dateien in der gepoolten VM. Dieses Problem tritt auf, da ein neues Benutzerprofil erstellt wird, wenn sich Benutzer an der gepoolten VM anmelden. Für dieses Problem gibt es keinen Workaround. [#392459]
- Personal vDisks, die unter Windows 7 ausgeführt werden, können das Feature "Sichern und Wiederherstellen" nicht verwenden, wenn der Windows-Systemschutz aktiviert ist. Wenn der Systemschutz deaktiviert ist, wird ein Backup des Benutzerprofils aber nicht der Datei userdata.v2.vhd erstellt. Citrix empfiehlt, den Systemschutz zu deaktivieren und ein Backup des Benutzerprofils mit dem Feature "Sichern und Wiederherstellen" zu erstellen. [#360582]
- Beim Erstellen einer VHD-Datei auf der Basis-VM mit dem Datenträgerverwaltungstool können Sie die virtuelle Festplatte (VHD) möglicherweise nicht bereitstellen. Um dieses Problem zu umgehen, kopieren Sie die VHD auf das PvD-Volume. [#355576]
- Office 2010-Verknüpfungen bleiben auf virtuellen Desktops erhalten, nachdem diese Software entfernt wurde. Um dieses Problem zu umgehen, löschen Sie die Verknüpfungen. [#402889]
- Wenn Sie Microsoft Hyper-V verwenden, können Sie mit Maschinen mit persönlichen vDisks keinen Katalog erstellen, wenn die Maschinen lokal gespeichert sind und die vDisks auf freigegebenen Clustervolumes (CSVs) gespeichert sind. Die Katalogerstellung schlägt fehl und ein Fehler wird angezeigt. Um dieses Problem zu umgehen, verwenden Sie einen anderen Speicherort für die vDisks. [#423969]
- Wenn Sie sich das erste Mal bei einem virtuellen Desktop anmelden, der von einem Provisioning Services-Katalog erstellt wurde, werden Sie aufgefordert, den Desktop neu zu starten, wenn die persönliche vDisk zurückgesetzt wurde (mit dem Befehl "ctxpvd.exe -s reset"). Um dieses Problem zu lösen, starten Sie den Desktop neu, wenn Sie dazu aufgefordert werden. Es handelt sich hier um eine einmalige Zurücksetzung, die bei erneuter Anmeldung nicht erforderlich ist. [#340186]
- Wenn Sie .NET 4.5 auf einer persönlichen vDisk installieren und .NET 4.0 bei einem späteren Update des Images installiert oder bearbeitet wird, schlagen Anwendungen, die von .NET 4.5 abhängig sind, fehl. Um dieses Problem zu umgehen, stellen Sie .NET 4.5 vom Basisimage aus als Imageupdate bereit.
- Weitere Informationen finden Sie unter
  — Bekannte Probleme
  in der Dokumentation zu XenApp und XenDesktop 7.6.

Info zu Personal vDisk 7.1.3

Bekannte Probleme aus Version 7.1.1, die in Version 7.1.3 behoben wurden:

- Direkte Upgrades von Personal vDisk 5.6.0 auf Personal vDisk 7.x können zu Fehlern bei Personal vDisk führen. [#432992]
- Benutzer können möglicherweise nur zeitweilig Verbindungen zu virtuellen Desktops mit persönlichen vDisks herstellen. [#437203]

- Wenn das Update eines Personal vDisk-Images während der Aktualisierung von Personal vDisk 5.6.5 oder höher auf Personal vDisk 7.0 oder höher unterbrochen wird, können spätere Updates fehlschlagen. [#436145]

Info zu Personal vDisk 7.1.1

Bekannte Probleme aus Version 7.1, die in Version 7.1.1 behoben wurden:

- Nach der Aktualisierung auf Symantec Endpoint Protection 12.1.3 über ein Imageupdate meldet symhelp.exe beschädigte Antivirus-Definitionen. [#423429]
- Personal vDisk kann den Neustart gepoolter Desktops verursachen, wenn der Dienststeuerungs-Manager (services.exe) abstürzt. [#0365351]

Neue bekannten Probleme in Version 7.1.1: Keine

Info zu Personal vDisk 7.1

Neue Features in Version 7.1:

- Sie können Personal vDisk nun auch auf Desktops unter Windows 8.1 verwenden und die Ereignisprotokollierung wurde verbessert.
- Copy-on-Write (CoW) wird in diesem Release nicht mehr unterstützt. Beim Upgrade von Personal vDisk Version 7.0 auf 7.1 gehen alle von CoW verwalteten Datenänderungen verloren. CoW war ein experimentelles Feature in XenDesktop 7 und es war standardmäßig deaktiviert. Wenn Sie es nicht aktiviert haben, sind Sie nicht betroffenen.

Bekannte Probleme aus Version 7.0.1, die in Version 7.1 behoben wurden:

- Wenn der Wert des Personal vDisk-Registrierungsschlüssels EnableProfileRedirection auf 1 oder ON eingestellt ist, und Sie den Wert beim Aktualisieren des Images in 0 oder OFF ändern, wird der ganze Personal vDisk-Speicherplatz u. U. den vom Benutzer installierten Anwendungen zugeordnet, sodass kein Platz für Benutzerprofile vorhanden ist, die auf der vDisk bleiben. Wenn die Profilumleitung für einen Katalog deaktiviert ist und Sie die Profilumleitung während eines Imageupdates aktivieren, können sich Benutzer u. U. nicht bei ihren virtuellen Desktops anmelden. [#381921]
- Der Desktopdienst protokolliert nicht den richtigen Fehler in der Ereignisanzeige, wenn das Update des Personal vDisk-Bestands fehlschlägt. [#383331]
- Beim Upgrade auf Personal vDisk 7.x bleiben geänderte Regeln nicht erhalten. Dieses Problem wurde für das Upgrade von Version 7.0 auf Version 7.1 behoben. Beim Upgrade von Version 5.6.5 auf Version 7.1 müssen Sie die Regeldatei zuerst speichern und die Regeln nach dem Upgrade erneut anwenden. [#388664]
- Personal vDisks, die unter Windows 8 ausgeführt werden, können keine Anwendungen vom Windows Store installieren. Eine Fehlermeldung gibt an, dass der Kauf nicht abgeschlossen werden konnte. Wenn Sie den Windows Update-Dienst aktivieren, wird das Problem nun behoben. Von Benutzern installierte Anwendungen müssen jedoch nach dem Neustart des Systems neu installiert werden. [#361513]
- Einige symbolische Verknüpfungen fehlen auf gepoolten Windows 7-Desktops mit persönlichen vDisks. Daher werden Symbole, die von Anwendungen unter C:\Benutzer\Alle Benutzer gespeichert werden, nicht im Startmenü angezeigt. [#418710]
- Der Start einer persönlichen vDisk schlägt fehl, wenn ein USN-Journalüberlauf aufgrund zahlreicher Systemänderungen nach einer Bestandsaktualisierung auftritt. [#369846]
- Der Start einer persönlichen vDisk schlägt fehl und der Statuscode 0x20 sowie Fehlercode 0x20000028 werden angezeigt. [#393627]
- Symantec Endpoint Protection 12.1.3 zeigt die Fehlermeldung "Proactive Threat Protection is malfunctioning" an und der Liveupdatestatus dieser Komponente ist nicht verfügbar. [#390204]

Neue bekannte Probleme in Version 7.1: Weitere Informationen finden Sie unter

— Bekannte Probleme

in der Dokumentation zu XenDesktop 7.1.

Info über Personal vDisk 7.0.1

Neu in Version 7.0.1: Personal vDisk ist jetzt robuster bei Änderungen der Umgebung. Virtuelle Desktops mit persönlichen vDisks werden jetzt beim Delivery Controller registriert, selbst wenn das Imageupdate fehlschlägt, und das Herunterfahren von unsicheren Systemen setzt die vDisks in einen permanent deaktivierten Zustand. Darüber hinaus können Sie nun während einer Bereitstellung Dateien und Ordner mithilfe von Regeldateien von vDisks ausschließen.

Bekannte Probleme aus Version 5.6.13, die in Version 7.0.1 behoben wurden:

- Änderungen an der Mitgliedschaft einer Gruppe, die von einem Benutzer an einem gepoolten virtuellen Desktop vorgenommen wurden, gehen u. U. nach einem Imageupdate verloren. [#286227]
- Imageupdates schlagen u. U. mit einer Fehlermeldung, dass der Speicherplatz auf dem Datenträger niedrig ist, fehl, selbst wenn die persönliche vDisk genug Speicherplatz hat. [#325125]
- Die Installation einiger Anwendungen schlägt auf virtuellen Desktops mit einer persönlichen vDisk fehl, und eine Meldung weist auf einen erforderlichen Neustart hin. Grund ist eine ausstehende Umbenennung. [#351520]
- Symbolische Links, die im Masterimage erstellt wurden, funktionieren nicht auf virtuellen Desktops mit persönlichen vDisks. [#352585]
- In Umgebungen mit der Citrix Profilverwaltung und Personal vDisk funktionieren Anwendungen, die Benutzerprofile auf einem Systemvolume überprüfen u. U. nicht richtig, wenn die Profilumleitung aktiviert ist. [#353661]
- Die Bestandsaktualisierung schlägt auf Masterimages fehl, wenn der Bestand größer als 2 GB ist. [#359768]
- Imageupdates schlagen mit einem Fehlercode 112 fehl und persönliche vDisks sind beschädigt, selbst wenn die vDisks ausreichend Speicherplatz für das Update haben. [#363003]
- Das Skript für das Ändern der Größe schlägt für Kataloge fehl, die mehr als 250 Desktops haben. [#363365]
- Benutzerseitige Änderungen einer Umgebungsvariablen gehen bei einer Aktualisierung des Images verloren. [#372295]
- Lokale Benutzer, die auf einem virtuellen Desktop mit einer persönlichen vDisk erstellt wurden, gehen bei einer Aktualisierung des Images verloren. [#377964]
- Der Start einer persönlichen vDisk schlägt u. U. fehl, wenn ein USN-Journalüberlauf aufgrund zahlreicher Systemänderungen nach einer Bestandsaktualisierung auftritt. Erhöhen Sie die USN-Journalgröße im Masterimage auf mindestens 32 MB und aktualisieren Sie das Image, um dieses Problem zu vermeiden. [#369846]
- Ein Problem wurde mit Personal vDisk festgestellt, das ein richtiges Funktionieren der Registrierungsstrukturaktionen des AppSense-Umgebungs-Managers verhindert, wenn AppSense im Ersetzenmodus verwendet wird. Citrix und AppSense arbeiten an der Behebung des Problems, das mit dem Verhalten der RegRestoreKey-API zusammenhängt, wenn Personal vDisk installiert ist. [#0353936]

Release-unabhängige bekannte Probleme

- Wenn eine Anwendung auf einer persönlichen vDisk (PvD) mit einer auf dem Masterimage installierten anderen Anwendung derselben Version verbunden ist, funktioniert die Anwendung auf der PvD nach einem Imageupdate möglicherweise nicht mehr. Dieses Problem tritt auf, wenn die Anwendung vom Masterimage deinstalliert oder auf eine neuere Version aktualisiert wird, da durch diese Aktion die Dateien entfernt werden, die die Anwendung auf der PvD vom Masterimage benötigt. Um dies zu verhindern, lassen Sie die Anwendung mit den Dateien, die von der Anwendung auf der PvD benötigt werden, auf dem Masterimage.
  Beispiel: Das Masterimage enthält Office 2007 und ein Benutzer installiert Visio 2007 auf der PvD. Die Office-Anwendungen und Visio funktionieren einwandfrei. Später ersetzt der Administrator Office 2007 durch Office 2010 auf dem Masterimage und aktualisiert anschließend alle betroffenen Maschinen mit dem aktualisierten Image. Visio 2007 funktioniert nicht mehr. Um dies zu verhindern, lassen Sie Office 2007 auf dem Masterimage. [#320915]

- Wenn Personal vDisk verwendet wird, verwenden Sie bei der Bereitstellung von McAfee Virus Scan Enterprise (VSE) die

Version 8.8 Patch 4 oder höher auf einem Masterimage. [#303472]

- Wenn eine Verknüpfung für eine Datei auf dem Masterimage nicht mehr funktioniert, weil das Verknüpfungsziel in PvD umbenannt wurde, erstellen Sie die Verknüpfung neu. [#367602]
- Verwenden Sie keine absoluten bzw. festen Links auf einem Masterimage. [#368678]
- Das mit Windows 7 verfügbare Feature "Sichern und Wiederherstellen" wird auf der persönlichen vDisk nicht unterstützt. [#360582]
- Nach der Anwendung eines aktualisierten Masterimages ist kein Zugriff auf die Konsole für lokale Benutzer und Gruppen möglich oder sie zeigt inkonsistente Daten an. Um das Problem zu lösen, setzen Sie die Benutzerkonten auf der VM zurück. Dazu muss die Sicherheitsstruktur zurückgesetzt werden. Dieses Problem wurde im Release 7.1.2 behoben und löst auch das Problem für VMs in späteren Releases, aber nicht für VMs, die mit einer früheren Version erstellt und dann aktualisiert wurden. [#488044]
- Bei der Verwendung einer gepoolten VM in einer ESX Hypervisor-Umgebung wird Benutzern eine Neustartaufforderung angezeigt, wenn der ausgewählte SCSI-Controllertyp ein "VMware Paravirtual" ist. Um dieses Problem zu umgehen, verwenden Sie den Controllertyp "LSI SCSI". [#394039]
- Nach dem Zurücksetzen von PvD auf einem mit Provisioning Services erstellten Desktop wird Benutzern nach der Anmeldung an der VM u. U. eine Neustartaufforderung angezeigt. Um dieses Problem zu umgehen, starten Sie den Desktop neu. [#340186]
- Benutzer von Windows 8.1-Desktops können sich u. U. nicht an ihren PvDs anmelden. Einem Administrator wird möglicherweise die Meldung "PvD was disabled due to unsafe shutdown" angezeigt und das PvDActivation-Protokoll enthält u. U. die Meldung "Failed to load reg hive [\Device\IvmVhdDisk00000001\CitrixPvD\Settings\RingCube.dat]". Dieses Problem tritt auf, wenn die VM nicht sicher heruntergefahren wird. Sie umgehen das Problem, indem Sie die persönliche vDisk zurücksetzen. [#474071]

Installation und Upgrade

Feb 29, 2016

Personal vDisk 7.x wird seit XenDesktop 5.6 bis zur aktuellen Version unterstützt. Für jede XenDesktop-Version werden in der Dokumentation unter "Systemanforderungen" die unterstützten Betriebssysteme für Virtual Delivery Agents (VDAs) sowie die unterstützten Versionen von Hosts (Virtualisierungsressourcen) und Provisioning Services aufgelistet. Weitere Informationen zu Provisioning Services-Aufgaben finden Sie in der Dokumentation zu Provisioning Services.

Installieren und Aktivieren von PvD

PvD wird automatisch installiert, wenn Sie einen VDA für Desktopbetriebssysteme auf einer Maschine installieren oder aktualisieren. Wenn Sie die PvD-Software nach der Installation des VDAs aktualisieren, verwenden Sie die hier verfügbare PvD-MSI (Citrix Anmeldeinformationen erforderlich).

Aktivieren von PvD:

- PvD wird automatisch aktiviert, wenn Sie mit den Maschinenerstellungsdiensten (MCS) einen Maschinenkatalog erstellen, dessen Desktopbetriebssystemmaschinen eine persönliche vDisk verwenden.
- Wenn Sie Provisioning Services (PVS) verwenden, wird PvD automatisch aktiviert, wenn Sie während der Erstellung des Masterimages den Bestand aufnehmen oder wenn bei einem automatischen Update der Bestand aktualisiert wird.

Während der VDA-Installation haben Sie die Möglichkeit, PvD zu aktivieren, indem Sie das Kontrollkästchen "Personal vDisk" auf der grafischen Benutzeroberfläche auswählen oder über die Befehlszeilenschnittstelle die Option "/baseimage" angeben. Auch wenn Sie diese Aktion bei der Installation des VDAs (Standard) nicht ausführen, können Sie mit dem gleichen Image PvD-Desktops und Desktops ohne PvD erstellen, da PvD während der Katalogerstellung aktiviert wird.

Hinzufügen von persönlichen vDisks

Sie fügen Hosts persönliche vDisks hinzu, wenn Sie eine Site konfigurieren. Sie können denselben Speicher auf dem Host für VMs und persönliche vDisks verwenden oder Sie können einen anderen Speicher für persönliche vDisks auswählen.

Später können Sie auch persönliche vDisks und ihren Speicher vorhandenen Hosts (Verbindungen), jedoch nicht Maschinenkatalogen, hinzufügen.

1. Wählen Sie im Studio-Navigationsbereich Konfiguration > Hosting.
2. Wählen Sie im Aktionsbereich Persönlichen vDisk-Speicher hinzufügen und geben Sie einen Speicherort an.

Aktualisieren von PvD

Die einfachste Methode, Personal vDisk von einer früheren 7.x-Version zu aktualisieren, ist das Aktualisieren der VDAs für Desktopbetriebssysteme mit der aktuellen XenDesktop-Version. Nehmen Sie anschließend den PvD-Bestand auf.

Sie können auch nur PvD mit der hier verfügbaren PvD-MSI aktualisieren.

Deinstallieren von PvD

Sie können die PvD-Software mit einer der folgenden beiden Methoden deinstallieren:

- Deinstallieren Sie den VDA. Dabei wird die PvD-Software ebenfalls entfernt.
- Wenn Sie PvD mit der PvD-MSI aktualisiert haben, können Sie es über die Liste der Programme deinstallieren.

Wenn Sie PvD deinstallieren und dieselbe oder eine neuere Version neu installieren, erstellen Sie eine Sicherungskopie des Registrierungsschlüssels HKLM\Software\Citrix\personal vDisk\config, der Konfigurationseinstellungen für die Umgebung

enthält, die sich geändert haben können. Nach der Installation von PvD können Sie die Registrierungswerte, die sich geändert haben, durch einen Vergleich mit der Sicherungskopie zurücksetzen.

Konfigurieren und Verwalten

Feb 29, 2016

In diesem Abschnitt werden Themen erläutert, die beim Konfigurieren und Verwalten einer Personal vDisk (PvD)-Umgebung zu berücksichtigen sind. Darüber hinaus werden Best Practices und Aufgabenbeschreibungen behandelt.

Beachten Sie Folgendes beim Arbeiten in der Windows-Registrierung:
Achtung: Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.

Überlegungen zur Größe einer persönlichen vDisk

Die folgenden Faktoren beeinflussen die Größe des PvD-Haupvolumes:

- **Größe der Anwendungen, die Benutzer auf ihren PvDs installieren**
  Bei Neustarts bestimmt PvD den im Anwendungsbereich verbleibenden freien Speicherplatz (UserData.v2.vhd). Wenn dieser Wert unter 10 % fällt, wird der Anwendungsbereich erweitert, indem ungenutzter Speicherplatz des Profilbereichs (standardmäßig der freie Speicherplatz auf dem Laufwerk P:) genutzt wird. Der zum Anwendungsbereich hinzugefügte Speicherplatz beträgt ungefähr 50 % des zusammengefassten freien Speicherplatzes von Anwendungs- und Profilbereich.

  Beispiel: Wenn der Anwendungsbereich auf einer 10 GB PvD, der standardmäßig eine Größe von 5 GB hat, den Wert 4,7 GB erreicht und der Profilbereich über 3 GB freien Speicherplatz verfügt, wird der zusätzliche Speicherplatz wie folgt berechnet:

  erweiterter Speicherplatz = (5,0 - 4,7) : 2 + 3,0 : 2 = 1,65 GB

  Der Wert für den zusätzlichen Speicherplatz kann nur ungefähr angegeben werden, da Abstriche für das Speichern von Protokollen und für Mehraufwand gemacht werden müssen. Die Berechnung und mögliche Größenänderung wird bei jedem Neustart ausgeführt.

- **Größe der Benutzerprofile (wenn keine separate Profilverwaltungslösung verwendet wird)**
  Zusätzlich zu dem für Anwendungen erforderlichen Speicherplatz muss auf persönlichen vDisks auch genügend Speicherplatz für das Speichern von Benutzerprofilen vorhanden sein. Schließen Sie alle nicht umgeleiteten speziellen Ordner (z. B. Dokumente und Musik) in Ihre Speicherplatzberechnungen ein. Vorhandene Profilgrößen sind in der Systemsteuerung (sysdm.cpl) verfügbar.

  Einige Profilumleitungslösungen speichern Stubdateien (Sentineldateien) anstelle echter Profildaten. Zu Beginn kann es aussehen, als würden die Profillösungen keine Daten speichern. Sie nutzen jedoch einen Dateiverzeichniseintrag pro Stubdatei im Dateisystem, was ungefähr 4 KB pro Datei ausmacht. Wenn Sie eine solche Lösung verwenden, schätzen Sie die Größe anhand der echten Profildaten und nicht basierend auf den Stubdateien.

  Unternehmensanwendungen zur Dateifreigabe, wie ShareFile und Dropbox, synchronisieren oder laden Daten möglicherweise auf die Profildatenbereiche der persönlichen vDisks von Benutzern herunter. Wenn Sie derartige Anwendungen verwenden, veranschlagen Sie genug Speicherplatz für diese Daten.

- **Mehraufwand durch die virtuelle Festplattenvorlage, die den PvD-Bestand enthält**
  Die virtuelle Festplattenvorlage enthält die PvD-Bestandsdaten (Sentineldateien, die zum Inhalt des Masterimages

gehören). Der PvD-Anwendungsbereich wird von dieser virtuellen Festplatte erstellt. Da jede Sentineldatei bzw. jeder Sentinelordner einen Dateiverzeichniseintrag im Dateisystem enthält, nimmt der Inhalt der virtuellen Festplattenvorlage PvD-Anwendungsspeicherplatz in Anspruch, bevor der Endbenutzer überhaupt eine Anwendung installiert hat. Sie können die Größe der virtuellen Festplattenvorlage bestimmten, indem Sie zum Masterimage navigieren, nachdem der Bestand aufgenommen wurde. Sie können zur ungefähren Berechnung auch die folgende Formel verwenden:

Größe der virtuellen Festplattenvorlage = (Anzahl der Dateien des Basisimage) x 4 KB

Sie ermitteln die Anzahl der Dateien und Ordner, indem Sie mit der rechten Maustaste auf das Laufwerk C: des Images der Basis-VM klicken und Eigenschaften auswählen. Beispiel: Ein Image mit 250.000 Dateien ergibt eine virtuelle Festplattenvorlage von ungefähr 1.024.000.000 Bytes (nicht ganz 1 GB). Dieser Speicherplatz ist nicht für Anwendungsinstallationen im PvD-Anwendungsbereich verfügbar.

- **Mehraufwand für PvD-Imageupdatevorgänge**
  Während PvD-Imageupdatevorgänge ausgeführt werden, muss im Stammverzeichnis der PvD (standardmäßig P:) genug Speicherplatz vorhanden sein, um die Änderungen der zwei Imageversionen mit den Änderungen, die der Benutzer an der PvD vorgenommen hat, zusammenzuführen. Normalerweise reserviert die PvD einige Hundert MB für diesen Zweck. Durch Extradaten, die im Laufwerk P: gespeichert wurden, ist jedoch möglicherweise nicht genug Speicherplatz zum Durchführen des Imageupdates vorhanden. Mit dem PvD-Poolstatistikscript (auf dem XenDesktop-Installationsmedium im Ordner "Support/Tools/Scripts") oder mit dem Überwachungstool für PvD-Imageupdates (im Ordner "Support/Tools/PvdTool") können Sie die PvD-Datenträger in einem Katalog identifizieren, für die ein Update geplant ist und die fast voll sind.

  Das Vorhandensein von Antivirenprodukten kann sich darauf auswirken, wie lange das Durchführen einer Bestandsaktualisierung oder eines Updates dauert. Die Leistung kann verbessert werden, wenn Sie CtxPvD.exe und CtxPvDSvc.exe der Ausschlussliste des Antivirenprodukts hinzufügen. Diese Dateien befinden sich im Ordner C:\Programme\Citrix\personal vdisk\bin. Durch das Ausschließen dieser ausführbaren Dateien vom Antivirenscan kann die Bestandsaktualisierungs- und Imageupdateleistung um das Zehnfache beschleunigt werden.

- **Mehraufwand für unerwartete Zunahme (unerwartete Anwendungsinstallationen usw.)**
  Kalkulieren Sie zusätzlichen Speicherplatz ein (entweder eine feste Menge oder einen Prozentsatz der vDisk-Größe), um auf unerwartete Anwendungsinstallationen von Benutzern während der Bereitstellung vorbereitet zu sein.

Konfigurieren von Größe und Zuordnung der persönlichen vDisk

Sie können den Algorithmus für die automatische Größenänderung, der die Größe der virtuellen Festplatte relativ zum Laufwerk P: festlegt, manuell anpassen, indem Sie die Ausgangsgröße der virtuellen Festplatte festlegen. Dies ist nützlich, wenn Sie beispielsweise wissen, dass Benutzer zahlreiche Anwendungen installieren werden, die nicht alle auf die virtuelle Festplatte passen werden, selbst wenn die Größe mit dem Algorithmus angepasst wurde. In dieser Situation können Sie die Ausgangsgröße des Anwendungsspeicherplatzes erhöhen, damit die vom Benutzer installierten Anwendungen genug Platz haben.

Passen Sie die Ausgangsgröße der virtuellen Festplatte am besten auf einem Masterimage an. Sie können die Größe der virtuellen Festplatte auch auf einem virtuellen Desktop anpassen, wenn ein Benutzer nicht genügend Speicherplatz für die Installation einer Anwendung hat. Sie müssen diesen Vorgang jedoch auf allen betroffenen virtuellen Desktops wiederholen, da Sie die Ausgangsgröße der virtuellen Festplatte nicht in einem bereits erstellten Katalog ändern können.

Stellen Sie sicher, dass die virtuelle Festplatte groß genug für das Speichern von Definitionsdateien von Antivirensoftware ist, da diese Dateien normalerweise sehr umfangreich sind.

Legen Sie die folgenden Registrierungsschlüssel in HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\personal vDisk\Config fest. (Ändern Sie keine anderen Einstellungen in diesem Registrierungsschlüssel.) Alle Einstellungen müssen auf dem Masterimage angegeben werden (außer für MinimumVHDSizeInMB, was auf einer individuellen Maschine geändert werden kann). Auf dem Masterimage angegebene Einstellungen werden bei der nächsten Aktualisierung des Images angewendet.

- **MinimumVHDSizeMB**
  Gibt die Mindestgröße (in Megabyte) des Anwendungsteils (C:) der persönlichen vDisk an. Die neue Größe muss größer als die vorhandene Größe und kleiner als die Größe des Datenträgers abzüglich PvDReservedSpaceMB sein.

  Durch das Erhöhen dieses Werts wird freier Speicherplatz vom Profilteil der vDisk dem Laufwerk C: zugeteilt. Diese Einstellung wird ignoriert, wenn ein geringerer Wert als die aktuelle Größe des Laufwerks C: verwendet wird oder wenn EnableDynamicResizeOfAppContainer auf 0 eingestellt ist.

  Standard = 2048

- **EnableDynamicResizeOfAppContainer**
  Aktiviert oder deaktiviert den Algorithmus zur dynamischen Größenänderung.
  - Bei der Einstellung auf 1 wird der Anwendungsspeicherplatz auf C: automatisch geändert, wenn der freie Speicherplatz auf C: unter 10 % fällt. Zulässige Werte sind 1 und 0. Ein Neustart muss durchgeführt werden, damit die Änderungen wirksam werden.
  - Bei der Einstellung auf 0 wird die Größe der virtuellen Festplatte basierend auf der Methode ermittelt, die in XenDesktop-Versionen vor 7.x verwendet wurde.

  Standard = 1

- **EnableUserProfileRedirection**
  Aktiviert oder deaktiviert die Umleitung des Benutzerprofils auf die vDisk.
  - Bei der Einstellung auf 1 leitet PvD das Benutzerprofil auf die vDisk um (standardmäßig auf P:). Profile werden entsprechend einem Windows-Standardprofil im Allgemeinen nach P:\Users umgeleitet. Durch die Umleitung werden die Profile beibehalten, falls der PvD-Desktop zurückgesetzt werden muss.
  - Bei der Einstellung auf 0 ist der gesamte Speicherplatz auf der vDisk, abzüglich PvDReservedSpaceMB, dem Laufwerk C: (dem Anwendungsteil der vDisk) zugewiesen, und das vDisk-Laufwerk (P:) ist im Windows Explorer ausgeblendet. Citrix empfiehlt das Deaktivieren der Umleitung durch die Einstellung auf 0, wenn Sie Citrix Profilverwaltung oder eine andere Roamingprofillösung verwenden.
    Durch diese Einstellung bleiben die Profile in C:\Users erhalten statt auf die vDisk umgeleitet zu werden, und sie ermöglicht der Roamingprofillösung das Verwalten der Profile.

    Dieser Wert stellt sicher, dass der ganze Speicherplatz auf P: Anwendungen zugewiesen ist.

    Bei einer Einstellung dieses Werts auf 0 wird davon ausgegangen, dass eine Profilverwaltungslösung eingesetzt wird. Das Deaktivieren der Profilumleitung ohne eine Roamingprofillösung einzusetzen wird nicht empfohlen, da die Profile sonst bei nachfolgenden PvD-Zurücksetzungsvorgängen gelöscht werden.

  Ändern Sie diese Einstellung nicht, wenn das Image aktualisiert wird, da sie zwar nicht den Speicherort vorhandener Profile ändert, jedoch den gesamten Speicherplatz auf der PvD dem Laufwerk C: zuweist und die PvD ausblendet.

  Konfigurieren Sie diesen Wert vor dem Bereitstellen eines Katalogs. Nach dem Bereitstellen eines Katalogs können Sie diesen Wert nicht mehr ändern.

  Wichtig: Ab XenDesktop 7.1 werden Änderungen an diesem Wert nicht angewendet, wenn Sie ein Imageupdate ausführen. Legen Sie den Wert des Schlüssels fest, wenn Sie die Kataloge erstellen, von denen die Profile erstellt werden. Sie können das Umleitungsverhalten später nicht mehr ändern.

Standard = 1

- **PercentOfPvDForApps**
  Legt die Teilung zwischen dem Anwendungsteil (C:) und dem Profilteil der vDisk fest. Dieser Wert wird beim Erstellen neuer VMs verwendet sowie während Imageupdates, wenn EnableDynamicResizeOfAppContainer auf 0 eingestellt ist.

  Das Ändern der Einstellung PercentOfPvDForApps macht nur einen Unterschied, wenn die Einstellung EnableDynamicResizeOfAppContainer auf 0 festgelegt ist. Standardmäßig ist EnableDynamicResizeOfAppContainer auf 1 (aktiviert) festgelegt, d. h. dass der AppContainer (Laufwerk C:) nur erweitert wird, wenn er fast voll ist (d. h. dynamisch), und zwar wenn weniger als 10 % freier Speicherplatz vorhanden ist.

  Durch das Erhöhen von PercentOfPvDForApps wird nur der Gesamtspeicherplatz für die Apps erhöht. Der Speicherplatz wird jedoch nicht sofort verfügbar gemacht. Sie müssen zudem die Zuordnungsteilung im Masterimage konfigurieren, die dann beim nächsten Imageupdate angewendet wird.

  Wenn Sie bereits einen Katalog mit Maschinen mit der Einstellung 1 für EnableDynamicResizeOfAppContainer generiert haben, ändern Sie die Einstellung im Masterimage für das nächste Update auf 0 und konfigurieren Sie die entsprechende Zuordnungsteilung. Die angeforderte Teilungsgröße wird eingehalten, solange sie größer als die aktuell zugeteilte Größe des Laufwerks C ist.

  Wenn Sie komplette Kontrolle über die Speicherplatzteilung haben möchten, legen Sie den Wert auf 0 fest. Damit haben Sie die komplette Kontrolle über die Größe des Laufwerks C und die Erweiterung des Laufwerks ist nicht davon abhängig, dass ein Benutzer eine bestimmte Menge Speicherplatz unter dem Schwellenwert in Anspruch nimmt.

  Standard = 50 % (beiden Teilen wird der gleiche Speicherplatz zugeteilt)

- **PvDReservedSpaceMB**
  Legt die Größe des reservierten Speicherplatzes (in MB) auf der vDisk für das Speichern von Personal vDisk-Protokollen und anderen Daten fest.

  Wenn in Ihrer Bereitstellung XenApp 6.5 (oder eine frühere Version) und Anwendungsstreaming verwendet wird, erhöhen Sie diesen Wert um die Größe des RadeCache.

  Standard = 512

- **PvDResetUserGroup**
  Gilt nur für XenDesktop 5.6: Ermöglicht der angegebenen Gruppe von Benutzern, eine persönliche vDisk zurücksetzen. Höhere XenDesktop-Releases verwenden dafür die delegierte Administration.

Weitere Einstellungen:

- **Windows Update Service**: Stellen Sie sicher, dass im Masterimage für Windows Updates die Einstellung Never Check for Update und für den Windows Update Service die Einstellung Disabled ausgewählt ist. Falls der Windows Update Service auf der PvD ausgeführt werden muss, wird durch die Einstellung Never Check for Update verhindert, dass die Updates auf den zugeordneten Maschinen installiert werden.
  Dieser Dienst wird von Windows 8 Store benötigt, um Modern UI-Apps installieren zu können.
- **Windows Updates**: Diese schließen Updates für Internet Explorer ein und müssen auf das Masterimage angewendet werden.
- **Updates requiring restarts**: Bei auf das Masterimage angewendeten Windows Updates sind, abhängig von den im Update enthaltenen Patches, möglicherweise mehrere Neustarts erforderlich, damit die Installation vollständig ausgeführt wird. Stellen Sie vor der PvD-Bestandsaktualisierung sicher, dass Sie das Masterimage richtig neu starten,

damit die Installation von ausgeführten Windows Updates vollständig abgeschlossen wird.
- **Application updates**: Aktualisieren Sie Anwendungen, die auf dem Masterimage installiert sind, um Speicherplatz auf den vDisks von Benutzern zu sparen. Auf diese Weise vermeiden Sie den doppelten Aufwand, der durch das Durchführen von Updates auf den vDisks einzelner Benutzer entstehen würde.

Überlegungen zu Anwendungen auf dem Masterimage

Es kann zu Konflikten zwischen Software und der von PvD erstellten Benutzerumgebung kommen. Zum Vermeiden von Konflikten müssen Sie die Software auf dem Masterimage (nicht auf den individuellen Maschinen) installieren. Auch wenn es keine Konflikte zwischen der Software und der Ausführung von PvD gibt, empfiehlt Citrix, sie auf dem Masterimage zu installieren.

Folgende Anwendungen müssen auf dem Masterimage installiert werden:
- Agents und Clients (z. B. System Center Configuration Manager-Agent, App-V-Client, Citrix Receiver)
- Anwendungen, die vorrangige Starttreiber installieren oder ändern
- Anwendungen, die Drucker- oder Scannersoftware bzw. -treiber installieren
- Anwendungen, die den Windows-Netzwerkstapel ändern
- VM-Tools wie VMware Tools und XenServer Tools

Folgende Anwendungen sollten auf dem Masterimage installiert werden:
- Anwendungen, die einer großen Anzahl an Benutzern zur Verfügung gestellt werden. Deaktivieren Sie für die folgenden Fälle vor der Bereitstellung die Anwendungsupdates:
  - Unternehmensanwendungen, die Volumenlizenzierung verwenden, z. B. Microsoft Office und Microsoft SQL Server
  - Gängige Anwendungen wie Adobe Reader, Firefox und Chrome
- Große Anwendungen, z. B. SQL Server, Visual Studio und Anwendungsframeworks wie .NET

Die folgenden Empfehlungen und Einschränkungen gelten für Anwendungen, die Benutzer auf Maschinen mit persönlichen vDisks installiert haben. Einige dieser Empfehlungen können nicht durchgesetzt werden, wenn Benutzer Administratorrechte haben:
- Benutzer sollten Anwendungen nicht vom Masterimage deinstallieren und dann auf ihrer persönlichen vDisk neu installieren.
- Vorsicht beim Aktualisieren oder Deinstallieren von Anwendungen auf dem Masterimage. Nachdem Sie die Version einer Anwendung auf dem Image installiert haben, installiert ein Benutzer möglicherweise eine Add-On-Anwendung (z. B. ein Plug-In), das diese Version erfordert. Im Fall einer solchen Abhängigkeit kann es nach dem Aktualisieren oder Deinstallieren der Anwendung auf dem Image beim Add-On zu einer Fehlfunktion kommen. Beispiel: Microsoft Office 2010 ist auf einem Masterimage installiert und ein Benutzer installiert Visio 2010 auf der persönlichen vDisk. Bei einem Upgrade von Office auf dem Masterimage kann die lokal installierte Visio-Anwendung unbrauchbar werden.
- Software mit Lizenzen, die von Hardware abhängig sind (entweder durch ein Dongle oder signaturbasierte Hardware), wird nicht unterstützt.

Überlegungen zu Provisioning Services

Wenn Sie Provisioning Services mit PvD verwenden:
- Das SOAP-Dienstkonto muss zum Administratorknoten von Studio hinzugefügt werden und es muss über die Rolle "Maschinenadministrator" oder eine höhere Rolle verfügen. Dadurch wird sichergestellt, dass die PvD-Desktops in den Status "Preparing" versetzt werden, wenn die Provisioning Services (PVS) vDisk auf "Production" hochgestuft wird.
- Das Versionsverwaltungsfeature von Provisioning Services muss zum Aktualisieren der persönlichen vDisk verwendet werden. Wenn die Version auf "Production" hochgestuft wird, versetzt der SOAP-Dienst die PvD-Desktops in den Status "Preparing".

- Die Größe der persönlichen vDisk sollte immer größer als der Provisioning Services-Schreibcachedatenträger sein, da Provisioning Services sonst fälschlicherweise die persönliche vDisk als Schreibcache nehmen könnte.
- Nach dem Erstellen einer Bereitstellungsgruppe können Sie die persönliche vDisk mit dem Überwachungstool für PvD-Imageupdates oder den Größenänderungs- und poolstats-Skripts (personal-vdisk-poolstats.ps1) überwachen.

Veranschlagen Sie genug Schreibcache. Bei normalem Betrieb werden die meisten Benutzerschreibvorgänge (Änderungen) von PvD erfasst und an die persönliche vDisk umgeleitet. Daher könnten Sie theoretisch die Größe des Provisioning Services-Schreibcache verringern. Wenn PvD jedoch nicht aktiv ist, z. B. während Imageupdatevorgängen, kann ein kleines Provisioning Services-Schreibcache schnell voll sein und den Absturz von Maschinen verursachen.

Citrix empfiehlt, dass Sie die Größe des Provisioning Services-Schreibcache entsprechend den Empfehlungen für Provisioning Services veranschlagen und dann Speicherplatz hinzufügen, der dem Doppelten der virtuellen Festplattenvorlage auf dem Masterimage entspricht (für Zusammenführungen). Es ist unwahrscheinlich, dass ein Zusammenführungsvorgang so viel Speicherplatz beansprucht, aber es ist möglich.

Wenn Sie mit Provisioning Services einen Katalog mit PvD-aktivierten Maschinen bereitstellen:
- Folgen Sie den Anweisungen in der Provisioning Services-Dokumentation.
- Sie können die Drosselungseinstellungen für Energieaktionen ändern, indem Sie die Verbindung in Studio bearbeiten.
- Zum Aktualisieren der Provisioning Services-vDisk installieren bzw. aktualisieren Sie Anwendungen und Software und starten Sie die vDisk neu. Aktualisieren Sie dann den PvD-Bestand und fahren Sie die VM herunter. Stufen Sie anschließend die neue Version auf "Production" hoch. Die PvD-Desktops im Katalog sollten automatisch in den Zustand "Preparing" versetzt werden. Wenn dies nicht der Fall ist, prüfen Sie, ob das SOAP-Dienstkonto Maschinenadministrator- oder höhere Privilegien auf dem Controller hat.

Mit dem Testmodusfeature von Provisioning Services können Sie einen Testkatalog mit Maschinen erstellen, die ein aktualisiertes Masterimage verwenden. Wenn die Tests die Funktionsfähigkeit des Katalogs bestätigen, stufen Sie ihn auf "Production" hoch.

Überlegungen zu den Maschinenerstellungsdiensten

Wenn Sie mit den Maschinenerstellungsdiensten (MCS) einen Katalog mit PvD-aktivierten Maschinen bereitstellen:
- Folgen Sie den Anweisungen in der XenDesktop-Dokumentation.
- Aktualisieren Sie nach dem Erstellen des Masterimages den PvD-Bestand und schalten Sie dann die VM aus (PvD funktioniert nicht ordnungsgemäß, wenn Sie die VM nicht ausschalten). Erstellen Sie einen Snapshot vom Masterimage.
- Geben Sie im Assistenten zum Erstellen von Maschinenkatalogen die Größe und den Laufwerksbuchstaben der persönlichen vDisk an.
- Nach dem Erstellen einer Bereitstellungsgruppe können Sie die persönliche vDisk mit dem Überwachungstool für PvD-Imageupdates oder den Größenänderungs- und poolstats-Skripts (personal-vdisk-poolstats.ps1) überwachen.
- Sie können die Drosselungseinstellungen für Energieaktionen ändern, indem Sie die Verbindung in Studio bearbeiten.
- Wenn Sie das Masterimage aktualisieren, nehmen Sie nach dem Aktualisieren der Anwendungen und der anderen Software auf dem Image den PvD-Bestand auf und schalten Sie anschließend die VM aus. Erstellen Sie einen Snapshot vom Masterimage.
- Überprüfen Sie mit dem Überwachungstool für PvD-Imageupdates oder mit dem Skript "personal-vdisk-poolstats.ps1", ob genügend Speicherplatz auf jeder PvD-aktivierten VM vorhanden ist, die das aktualisierte Masterimage verwendet.
- Nach dem Aktualisieren des Maschinenkatalogs werden die PvD-Desktops in den Zustand "Preparing" versetzt, während sie die Änderungen am neuen Masterimage verarbeiten. Die Desktops werden entsprechend der während des Maschinenupdates festgelegten Rolloutstrategie aktualisiert.
- Während die PvD im Zustand "Preparing" ist, überwachen Sie sie mit dem Überwachungstool für PvD-Imageupdates oder mit dem Skript "personal-vdisk-poolstats.ps1".

Ausschließen von Dateien und Ordner von vDisks

Mit Regeldateien schließen Sie Dateien und Ordner von vDisks aus. Dies ist möglich, während die persönlichen vDisks bereitgestellt werden. Die Regeldateien werden custom_*_rules.template.txt genannt und befinden sich im Ordner \config. Anmerkungen in den einzelnen Dateien erhalten zusätzliche Informationen.

Durchführen einer Bestandsaktualisierung beim Aktualisieren eines Masterimages

Wenn Sie PvD nach einer Aktualisierung des Masterimages aktivieren, muss der Bestand des Datenträgers aktualisiert und ein neuer Snapshot erstellt werden.

Wenn Sie eine Anwendung installieren, die Binärdateien im Benutzerprofil des Administrators ablegt, ist die Anwendung nicht für Benutzer freigegebener virtueller Desktops (einschließlich solcher, die auf gepoolten Maschinenkatalogen basieren und mit PvD-Maschinenkatalogen gepoolt sind) verfügbar, da Masterimages nicht von Benutzern sondern von Administratoren verwaltet werden. Benutzer müssen solche Anwendungen selber installieren.

Es ist ratsam, nach jedem Schritt in diesem Verfahren einen Snapshot des Images zu erstellen:

1. Aktualisieren Sie das Masterimage, indem Sie auf der Maschine Anwendungen oder Betriebssystemupdates installieren und das System konfigurieren.
   Bei Masterimages, die auf Windows XP basieren und die Sie mit persönlichen vDisks bereitstellen möchten, müssen Sie sicherstellen, dass keine Dialogfelder offen sind (z. B. Meldungen zur Bestätigung von Softwareinstallationen oder Aufforderungen, nicht signierte Treiber zu verwenden). Offene Dialogfelder auf Masterimages in dieser Umgebung verhindern, dass sich der VDA beim Delivery Controller registriert. Sie können Aufforderungen für nicht signierte Treiber in der Systemsteuerung verhindern. Navigieren Sie zu "System > Hardware > Treibersignierung" und wählen Sie die Option zum Ignorieren von Warnungen.
2. Fahren Sie die Maschine herunter. Klicken Sie bei Windows 7-Maschinen auf Abbrechen, wenn Citrix Personal vDisk das Herunterfahren behindert.
3. Klicken Sie im Citrix Personal vDisk-Dialogfeld auf Bestand aktualisieren. Dieser Vorgang kann einige Minuten dauern. Wichtig: Wenn Sie das anschließende Herunterfahren unterbrechen (selbst wenn Sie nur eine kleine Änderung am Image vornehmen), stimmt der Bestand der persönlichen vDisk nicht mehr mit dem Masterimage überein. Dies führt dazu, dass das Personal vDisk-Feature nicht mehr funktioniert. Wenn Sie das Herunterfahren unterbrechen, müssen Sie die Maschine neu starten, herunterfahren und auf "Bestand aktualisieren" klicken, wenn Sie dazu aufgefordert werden.
4. Erstellen Sie, nachdem der Bestandvorgang die Maschine heruntergefahren hat, einen Snapshot des Masterimages.

Sie können einen Bestand in eine Netzwerkfreigabe exportieren und ihn anschließend in ein Masterimage importieren. Weitere Informationen finden Sie unter Exportieren und Importieren eines PvD-Bestands.

Konfigurieren von Drosselungseinstellungen für Verbindungen

Der Citrix Brokerdienst steuert den Energiezustand der Maschinen, die Desktops und Anwendungen bereitstellen. Der Brokerdienst kann mehrere Hypervisors über einen Delivery Controller steuern. Die Interaktion zwischen einem Controller und dem Hypervisor wird durch Broker-Energieaktionen gesteuert. Aktionen, die den Energiezustand einer Maschine ändern, wird eine Priorität zugewiesen und dann werden sie über einen Drosselungsmechanismus an den Hypervisor gesendet, damit es nicht zur Überlastung kommt. Die folgenden Einstellungen wirken sich auf die Drosselung aus. Diese Werte werden festgelegt, indem Sie eine Verbindung (Seite "Erweitert") in Studio bearbeiten.

Konfigurieren von Drosselungswerten für eine Verbindung

1. Wählen Sie im Studio-Navigationsbereich Konfiguration > Hosting.
2. Wählen Sie die Verbindung und dann im Aktionsbereich Verbindung bearbeiten.

3. Sie können die folgenden Werte ändern:
   - **Gleichzeitige Aktionen (alle Typen)**: Das zulässige Maximum für gleichzeitig ausgeführte Energieaktionen. Diese Einstellung wird als absoluter Wert und als Prozentsatz der Verbindung mit dem Hypervisor angegeben. Der niedrigere der beiden Werte wird verwendet.
     Standard = 100 absolut, 20%

   - **Gleichzeitige Updates für Personal vDisk-Bestand**: Das zulässige Maximum für gleichzeitige Personal vDisk-Energieaktionen. Diese Einstellung wird als absoluter Wert und als Prozentsatz der Verbindung angegeben. Der niedrigere der beiden Werte wird verwendet.
     Standard = 50 absolut, 25%

     Sie kalkulieren den absoluten Wert, indem Sie den Gesamtwert für IOPS (TIOPS) bestimmen, den der Datenträger des Endbenutzers unterstützt (dies sollte vom Hersteller festgelegt sein oder berechnet werden). Veranschlagen Sie 350 IOPS pro VM (IOPS/VM), um die Anzahl der VMs zu bestimmen, die jeweils auf dem Datenträger aktiv sein können. Sie berechnen diesen Wert, indem Sie den Gesamtwert für IOPS durch IOPS/VM teilen.

     Beispiel: Wenn der Wert für den Datenträger des Endbenutzers 14.000 IOPS ist, ist die Anzahl der aktiven VMs 14.000 IOPS : 350 IOPS/VM = 40.

   - **Höchstanzahl neue Aktionen pro Minute**: Die maximale Anzahl der neuen Energieaktionen, die pro Minute an den Hypervisor gesendet werden können. Sie wird als absoluter Wert angegeben.
     Standard = 10

Identifizieren der optimalen Werte für diese Einstellungen in der Bereitstellung:

1. Messen Sie mit den Standardwerten die Reaktionszeit für das Imageupdate eines Testkatalogs. Dies ist die Differenz zwischen der Startzeit eines Imageupdates (T1) und dem Zeitpunkt, wenn der VDA auf der letzten Maschine des Katalogs beim Controller registriert wird (T2). Reaktionszeit = T2 – T1.
2. Messen Sie die Ein- und Ausgabevorgänge pro Sekunde (IOPS) auf dem Hypervisorspeicher während des Imageupdates. Diese Daten können als Benchmark für die Optimierung dienen. (Die Standardwerte sind möglicherweise die beste Einstellung. Unter Umständen erreicht das System den maximalen IOPS-Wert, sodass die Einstellungswerte herabgesetzt werden müssen.)
3. Ändern Sie den Wert für "Gleichzeitige Updates für Personal vDisk-Bestand" wie unten beschrieben und lassen Sie alle anderen Einstellungen unverändert.
   1. Erhöhen Sie den Wert um 10 und messen Sie die Reaktionszeit nach jeder Änderung. Fahren Sie fort, den Wert um 10 zu erhöhen und messen Sie das Ergebnis, bis die Reaktionszeit abnimmt oder keine Änderung mehr auftritt.
   2. Wenn durch das Erhöhen des Werts im vorherigen Schritt keine Verbesserung erzielt wurde, verringern Sie den Wert schrittweise um 10 und messen Sie die Reaktionszeit nach jeder Verringerung. Wiederholen Sie diesen Vorgang, bis sich die Reaktionszeit nicht mehr ändert oder verbessert. Dieser Wert ist wahrscheinlich der optimale Wert für die PvD-Energieaktion.
4. Wenn Sie den Einstellungswert für die PvD-Energieaktion festgelegt haben, optimieren Sie nacheinander die Werte für die gleichzeitigen Aktionen (alle Typen) und die Höchstanzahl der neuen Aktionen pro Minute. Folgen Sie den oben erläuterten Schritten (schrittweises Erhöhen und Verringern der Werte), um verschiedene Werte zu testen.

Verwenden von Microsoft System Center Configuration Manager 2007 mit PvD

System Center Configuration Manager (Configuration Manager) 2012 erfordert keine besondere Konfiguration und kann auf die gleiche Weise wie alle anderen Anwendungen auf dem Masterimage installiert werden. Die folgenden Informationen gelten nur für System Center Configuration Manager 2007. Configuration Manager-Versionen vor Configuration Manager 2007 werden nicht unterstützt.

Führen Sie die folgenden Schritte aus, um die Configuration Manager 2007 Agent-Software in einer PvD-Umgebung zu verwenden.

1. Installieren Sie den Client-Agent auf dem Masterimage.
    1. Installieren Sie den Configuration Manager-Client auf dem Masterimage.
    2. Beenden Sie den ccmexec-Dienst (SMS-Agent) und deaktivieren Sie ihn.
    3. Löschen Sie SMS- oder Clientzertifikate wie folgt aus dem Zertifikatspeicher des lokalen Computers:
        - Gemischter Modus: Certificates (Lokaler Computer)\SMS\Certificates
        - Einheitlicher Modus
            - Certificates (Lokaler Computer)\Personal\Certificates
            - Löschen Sie das Clientzertifikat, das von Ihrer Zertifizierungsstelle ausgestellt wurde (normalerweise eine interne PKI).
    4. Löschen Sie C:\Windows\smscfg.ini oder benennen Sie die Datei um.
2. Entfernen Sie Informationen, die den Client eindeutig identifizieren.
    1. (Optional) Löschen Sie die Protokolldateien unter C:\Windows\System32\CCM\Logs oder verschieben Sie sie.
    2. Installieren Sie ggf. den Virtual Delivery Agent und nehmen Sie den PvD-Bestand auf.
    3. Fahren Sie das Masterimage herunter, erstellen Sie einen Snapshot und erstellen Sie dann mit diesem Snapshot einen Maschinenkatalog.
3. Überprüfen Sie Personal vDisk und starten Sie die Dienste. Führen Sie diese Schritte einmal auf jedem PvD-Desktop aus, nachdem er zum ersten Mal gestartet wurde. Dazu können Sie beispielsweise ein Domänen-GPO verwenden.
    - Bestätigen Sie, dass PvD aktiv ist, indem Sie prüfen, ob der Registrierungsschlüssel HKLM\Software\Citrix\personal vDisk\config\virtual vorhanden ist.
    - Stellen Sie den ccmexec-Dienst (SMS-Agent) auf "Automatic" ein und starten Sie den Dienst. Der Configuration Manager-Client kontaktiert den Configuration Manager-Server und ruft neue, eindeutige Zertifikate und GUIDs ab.

Tools

Feb 29, 2016

Mit den folgenden Tools und Hilfsprogrammen können Sie PvD-Vorgänge anpassen, vereinfachen und überwachen.

Benutzerdefinierte Regeldateien

Mit den von PvD bereitgestellten benutzerdefinierten Regeldateien können Sie das folgende Standardverhalten von PvD-Imageupdates ändern:

- Die Sichtbarkeit von Dateien auf der PvD
- Die Art der Zusammenführung von vorgenommenen Änderungen
- Einstellungen zur Beschreibbarkeit der Dateien

Detaillierte Anweisungen zu den benutzerdefinierten Regeldateien und dem CoW-Feature finden Sie in den Kommentaren zu den Dateien, die sich unter C:\ProgramData\Citrix\personal vDisk\Config auf der Maschine befinden, auf der PvD installiert ist. Die Dateien mit dem Namen custom_* erläutern die Regeln und wie sie aktiviert werden.

Ändern der Größe und poolstats-Skripts

Es gibt zwei Skripts zum Überwachen und Verwalten der Größe der PvDs. Sie befinden sich im Ordner "Support\Tools\Scripts" auf dem XenDesktop-Installationsmedium. Sie können auch das Überwachungstool für PvD-Imageupdates verwenden, das sich im Ordner "Support\Tools\Scripts\PvdTool" befindet. Weitere Informationen finden Sie unter http://blogs.citrix.com/2014/06/02/introducing-the-pvd-image-update-monitoring-tool/.

Verwenden Sie "resize-personalvdisk-pool.ps1" zum Vergrößern der PvDs in allen Desktops eines Katalogs. Die folgenden Snap-Ins oder Module für den Hypervisor müssen auf der Maschine installiert werden, auf der Studio ausgeführt wird:

- XenServer erfordert XenServerPSSnapin
- vCenter erfordert vSphere PowerCli
- System Center Virtual Machine Manager erfordert die VMM-Konsole

Mit "personal-vdisk-poolstats.ps1" können Sie den Status von Imageupdates überprüfen sowie den Speicherplatz für Anwendungen und Benutzerprofile in einer PvD-Gruppe. Führen Sie das Skript vor dem Update eines Images aus, um zu prüfen, ob Desktops genug Speicherplatz haben. Dadurch werden Fehler während des Updates verhindert. Für das Skript muss die Windows Management Instrumentation (WMI-In)-Firewall auf den PvD-Desktops aktiviert sein. Sie können die Firewall auf dem Masterimage aktivieren oder über GPO.

Wenn ein Imageupdate fehlschlägt, zeigt der Eintrag in der Spalte "Update" die Ursache an.

Zurücksetzen des Anwendungsbereichs

Wenn ein Desktop durch die Installation einer fehlerhaften Anwendung oder aus einem anderen Grund beschädigt wird, können Sie den Anwendungsbereich der PvD auf den (leeren) Herstellerstandard zurücksetzen. Beim Zurücksetzen bleiben die Benutzerprofildaten erhalten.

Zurücksetzen des Anwendungsbereichs der PvD:

- Melden Sie sich am Desktop des Benutzers als Administrator an. Starten Sie eine Eingabeaufforderung und führen Sie den Befehl C:\Programme\Citrix\Personal vDisk\bin\CtxPvD.exe -s Reset aus.
- Navigieren Sie in Citrix Director zum Desktop des Benutzers. Klicken Sie auf Reset Personal vDisk und anschließend auf OK.

Exportieren und Importieren eines PvD-Bestands

Der Imageupdateprozess ist ein zentraler Teil der Bereitstellung neuer Images auf PvD-Desktops und umfasst Anpassungen, damit vorhandene persönliche vDisks mit dem neuen Basisimage funktionieren. Bei Bereitstellungen, die Maschinenerstellungsdienste (MCS) verwenden, können Sie einen Bestand von einer aktiven VM auf eine Netzwerkfreigabe exportieren und dann in ein Masterimage importieren. Mit diesem Bestand auf dem Masterimage wird eine Differenz berechnet. Obwohl das Feature zum Exportieren bzw. Importieren des Bestands nicht verwendet werden muss, kann es die Leistung des Imageupdateprozesses verbessern.

Sie müssen ein Administrator sein, um das Feature zum Exportieren/Importieren des Bestands zu verwenden. Authentifizieren Sie sich für den Export/Import ggf. bei der Dateifreigabe mit "net use". Der Benutzerkontext muss auf alle für den Export/Import verwendeten Dateifreigaben zugreifen können.

- Führen Sie zum Exportieren eines Bestands den Exportbefehl als Administrator auf einer Maschine aus, auf der sich ein VDA mit aktivierter PvD befindet (Mindestversion 7.6):
  Ctxpvdsvc.exe exportinventory "<Pfad zum Exportspeicherort>"

  Die Software erkennt den Speicherort des aktuellen Bestands und exportiert den Bestand an den angegebenen Speicherort in einen Ordner mit dem Namen "ExportedPvdInventory". Hier ein Auszug aus der Befehlsausgabe:
  C:\Program Files\Citrix\personal vDisk\bin> .\CtxPvDSvc.exe exportinventory \\share location\ExportedInventory Current inventory source location C:\CitrixPvD\Settings\Inventory\VER-LAS ... Exportin
- Zum Importieren eines zuvor exportierten Bestands führen Sie den Importbefehl als Administrator auf dem Masterimage aus:

Importieren

Führen Sie den Importbefehl als Administrator auf dem Masterimage aus.

Ctxpvdsvc.exe importinventory "<Pfad zum exportierten Bestand>"

Der <Pfad zum exportierten Bestand> muss der vollständige Pfad für die Bestandsdateien sein; in der Regel ist das <Netzwerkspeicherort\ExportedPvdInventory>.

Der Bestand wird aus dem Importspeicherort abgerufen (zuvor wurde er mit dem Befehl zum Exportieren des Bestands hierher exportiert) und in den Bestandsspeicher auf dem Masterimage importiert. Hier ein Auszug aus der Befehlsausgabe:
C:\Program Files\Citrix\personal vDisk\bin> .\CtxPvDSvc.exe importinventory \\share location\ExportedInventory\ExportedPvdInventory Importing inventory \\share location\ExportedInventory\ExportedPv
Nach dem Exportvorgang sollte die Netzwerkfreigabe die folgenden Dateinamen enthalten. Nach dem Importvorgang sollte der Bestandsspeicher auf dem Masterimage die gleichen Dateinamen enthalten.

- Components.DAT
- files_rules
- folders_rules
- regkey_rules
- RINGTHREE.DAT
- S-1-5-18.DAT
- SAM.DAT
- SECURITY.DAT
- SNAPSHOT.DAT

- SOFTWARE.DAT
- SYSTEM.CurrentControlSet.DAT
- VDCATALOG.DAT
- vDiskJournalData

Sichern und Wiederherstellen

Wichtig: Die Skripts verschieben die PvDs nicht an einen neuen Speicherort. Diesen Vorgang müssen Sie auf eine andere Weise ausführen.
Zwei PowerShell-Skripts im Ordner "Support\Tools\Scripts" auf dem Installationsmedium des Produkts ermöglichen das Sichern und Wiederherstellen persönlicher vDisks. Mit den Skripts zum Sichern und Wiederherstellen können Sie vorhandene PvDs und Benutzerzuweisungen von einem Katalog zu einem anderen migrieren. Dies kann nützlich sein, wenn Sie den PvD-Speicher ändern müssen. Das Skript zum Sichern erstellt eine XML-Datei mit Metadaten aus einem bestehenden Katalog. Die Metadaten enthalten den aktuellen Pfad der PvDs im Speicher und die Benutzerzuweisungen zu den PvDs. Das Skript zum Wiederherstellen verwendet die XML-Datei, um die PvDs einem neuen Katalog zuzuweisen und ihnen die richtigen Benutzer zuzuordnen.
- migration-backup.ps1 zeichnet die Zuordnung zwischen jedem Benutzer und dessen persönlicher vDisk in einem Maschinenkatalog auf und speichert diese Informationen in einer XML-Datei.
- migration-restore.ps1 erstellt mit der XML-Datei den Desktop des Benutzers in einem Maschinenkatalog neu.

Vor dem Sichern und Wiederherstellen beachten Sie Folgendes:
- Die Skripts verwenden die Hypervisor-API. Daher muss das PowerShell-Snap-In des Hypervisors auf dem Controller, auf dem die Skripts ausgeführt werden, installiert sein.
- Führen Sie die Skripts von einem Speicherort aus, der Zugriff auf den Controller hat, auf dem der Maschinenkatalog erstellt wurde.
- Die Skripts werden auf folgenden Hypervisor-Plattformen unterstützt: Citrix XenServer, Microsoft Hyper-V und VMware ESX.

Sichern eines Maschinenkatalogs

Führen Sie ein Backup durch, wenn ein Maschinenkatalog geändert wird. Sie können ein Backup durchführen, während die Maschinen im Katalog aktiv sind.

Verwenden Sie migration-backup.ps1 zum Sichern beliebiger Maschinenkataloge, die persönliche vDisks enthalten. Das Skript fordert die Angabe des Namens des Maschinenkatalogs und der Verbindungsinformationen für den Hypervisor an. Anschließend durchläuft es sämtliche Benutzern zugewiesene Maschinen im Maschinenkatalog und speichert für jede Maschine die Zuordnung zwischen persönlichem vDisk-Speicher und dem jeweiligen Benutzer. Diese Informationen werden in einer XML-Datei gespeichert, die folgende Struktur hat:

- PvDMigration.hypervisor.Type unterstützt VMware ESX, Citrix XenServer und Microsoft Hyper-V.
- PvDMigration.PVD speichert Informationen dazu, wo die persönliche vDisk gespeichert und welchem Benutzer sie zugeordnet ist.
- PvDMigration.PVD.DiskId ist der eindeutige Bezeichner der vDisk auf dem Hypervisor, auf dem das Backup erstellt wurde.
- PvDMigration.PVD.DiskName ist der Name der VHD- bzw. VMDK-Datei.
- PvDMigration.PVD.SRName ist der Name des Speicheranbieters, wenn das Backup erstellt wurde.
- PvDMigration.PVD.SRID ist der eindeutige Bezeichner des Speicheranbieters auf dem Hypervisor, auf dem das Backup erstellt wurde.
- PvDMigration.PVD.UserName ist der Name des Benutzers, der der vDisk zugeordnet ist.
- PvDMigration.PVD.UserSid ist die SID des Benutzers, der der vDisk zugeordnet ist.
- PvDMigration.PVD.State ist der Status der vDisk. Der Status kann "backed up" oder "processed" lauten. Er lautet "backed up" nach dem ersten Backup und ändert sich in "processed", wenn die XML-Datei für eine Wiederherstellung vom Backup verwendet wurde.

Wiederherstellen eines Maschinenkatalogs

Beachten Sie vor dem Wiederherstellen Folgendes:
- Sie können nur einen Maschinenkatalog wiederherstellen, der dasselbe Masterimage hat wie der gesicherte Maschinenkatalog.
- Sie müssen ein neues Masterimage erstellen, indem Sie den Bestand des Masterimages aktualisieren, auf dessen Basis der gesicherte Maschinenkatalog erstellt wurde.

Stellen Sie mit migration-restore.ps1 beliebige Maschinenkataloge mit persönlichen vDisks wieder her. Das Skript erfordert folgende Eingaben:
- Während des Backups erstellte XML-Datei.
- Name des Maschinenkatalogs, der wiederhergestellt wird.
- Name des Speicherorts an dem die nicht zugewiesenen persönlichen vDisks gespeichert sind. Dies ist in der XML-Datei aufgelistet.
- Hypervisor-Verbindungsinformationen.

Das Skript migration-restore.ps1 findet alle nicht zugewiesenen Maschinen im Maschinenkatalog und weist ihnen Benutzer zu. Außerdem fügt es die persönlichen vDisks der Benutzer den Maschinen an.

Beispielszenario 1: Wiederherstellung eines Maschinenkatalogs und seiner persönlichen vDisks mit neuen Maschinennamen

In diesem Szenario werden ein ganzer Maschinenkatalog und die persönlichen vDisks, die den enthaltenen Maschinen angefügt sind, wiederhergestellt. Die Maschinen erhalten neue Namen. Dies kann auftreten, wenn der Hypervisor oder ein Speicherhost ausgefallen ist oder wenn Benutzer in eine neue Infrastruktur migriert werden.
1. Führen Sie migration-backup.ps1 aus, um die Zuweisung zwischen Benutzern und persönlichen vDisks in der XML-Datei aufzuzeichnen.
2. Verschieben oder sammeln Sie mit einer Backuplösung die persönlichen vDisks aus dem ursprünglichen Maschinenkatalog auf einen Datenträger:
   - VMware ESX oder Microsoft Hyper-V: Persönliche vDisks sind in dem vom Controller festgelegten Speicher in einem Ordner, der den Namen der Maschine enthält, dem die vDisk angefügt ist.
   - Citrix XenServer: Persönliche vDisks sind im Stamm des vom Controller festgelegten Speichers. Der Name jeder vDisk ist eine GUID.
3. Stellen Sie die persönlichen vDisks aus dem ursprünglichen Maschinenkatalog mit einer Speicherbackuplösung wieder her:
   - ESX oder Hyper-V: Platzieren Sie die vDisks in einen neuen Ordner auf der neuen Speicherressource. Alternativ können Sie die vDisks im ursprünglichen Pfad auf der neuen Speicherressource lassen.
   - XenServer: Platzieren Sie die vDisks im Stamm der neuen Speicherressource.
4. Erstellen Sie einen Provisioning Services-vDisk- oder Maschinenerstellungsdienste-Snapshot des Masterimages, mit dem Sie den ausgefallenen Maschinenkatalog erstellt haben.
5. Führen Sie Bestand aktualisieren über das Startmenü auf der vDisk oder dem Snapshot aus.
6. Erstellen Sie den Maschinenkatalog in Studio neu und verwenden Sie dabei eine andere Benennungskonvention als für den ausgefallenen ursprünglichen Maschinenkatalog. Dadurch wird ein Katalog neuer Maschinen mit jeweils einer neuen persönlichen vDisk erstellt, die die Sitedatenbank erkennt.
7. Stellen Sie sicher, dass der neu erstellte Maschinenkatalog der richtigen Bereitstellungsgruppe zugewiesen ist.
8. Stellen Sie sicher, dass die Bereitstellungsgruppe im Wartungsmodus ist und die enthaltenen Maschinen heruntergefahren sind.
9. Bearbeiten Sie die vom Backupskript generierte XML-Datei:
   - ESX oder Hyper-V: Wenn Sie vDisks in Schritt 3 in einem neuen Ordner auf der neuen Speicherressource wiederhergestellt haben, ersetzen Sie für jeden PVD-Abschnitt in der Datei den Ordnernamen in DiskName durch den Speicherort der wiederhergestellten vDisks. Wenn Sie die vDisks im ursprünglichen Pfad im neuen Speicher wiederhergestellt haben, überspringen Sie diesen Schritt.
   - XenServer: Überspringen Sie diesen Schritt.
10. Führen Sie auf dem Controller migration-restore.ps1 aus und geben Sie den Namen der XML-Datei und den Speicherort der gesicherten vDisks an.

Beispielszenario 2: Wiederherstellung eines Maschinenkatalogs und seiner persönlichen vDisks unter Wiederverwenden der bestehenden Maschinennamen

In diesem Szenario werden ein ganzer Maschinenkatalog und die persönlichen vDisks, die den enthaltenen Maschinen angefügt sind, wiederhergestellt. Die bestehenden Namen der (ausgefallenen) Maschinen werden wiederverwendet. Dieses Szenario ist möglich, wenn der Hypervisor oder ein Speicherhost ausgefallen ist.

1. Führen Sie migration-backup.ps1 aus, um die Zuordnung zwischen Benutzern und persönlichen vDisks aufzuzeichnen.
2. Verschieben oder sammeln Sie mit einer Backuplösung die persönlichen vDisks aus dem ursprünglichen Maschinenkatalog auf einen Datenträger:
   - ESX oder Hyper-V: Persönliche vDisks sind in dem vom Controller festgelegten Speicher in einem Ordner, der den Namen der Maschine enthält, dem die vDisk angefügt ist.
   - XenServer: Persönliche vDisks sind im Stamm des vom Controller festgelegten Speichers. Der Name jeder vDisk ist eine GUID.
3. Stellen Sie die persönlichen vDisks aus dem ursprünglichen Maschinenkatalog mit einer Speicherbackuplösung wieder her:
   - ESX oder Hyper-V: Platzieren Sie die vDisks in einen neuen Ordner auf der neuen Speicherressource.
   - XenServer: Platzieren Sie die vDisks im Stamm der neuen Speicherressource.
4. Erstellen Sie einen Provisioning Services-vDisk- oder Maschinenerstellungsdienste-Snapshot des Masterimages, mit dem Sie den ausgefallenen Maschinenkatalog erstellt haben.
5. Führen Sie Bestand aktualisieren über das Startmenü auf der vDisk oder dem Snapshot aus.
6. Erstellen Sie den Maschinenkatalog in Studio neu und verwenden Sie dabei die gleiche Benennungskonvention wie für den ausgefallenen Maschinenkatalog. Dadurch wird ein Katalog neuer Maschinen mit jeweils einer neuen persönlichen vDisk erstellt, die die Sitedatenbank erkennt.
7. Stellen Sie sicher, dass der neu erstellte Maschinenkatalog der richtigen Bereitstellungsgruppe zugewiesen ist.
8. Stellen Sie sicher, dass die Desktopgruppe im Wartungsmodus ist und die enthaltenen Maschinen heruntergefahren sind.
9. Bearbeiten Sie die vom Backupskript generierte XML-Datei:
   - ESX oder Hyper-V: Ersetzen Sie für jeden PVD-Abschnitt in der Datei den Ordnernamen in DiskName durch den Speicherort der wiederhergestellten vDisks.
   - XenServer: Überspringen Sie diesen Schritt.
10. Führen Sie das Skript migration-restore.ps1 auf dem Controller aus und verwenden Sie die geänderte XML-Datei als Eingabe. Das Skript fügt die vDisks an, ohne sie zu verschieben.
11. Überprüfen Sie, ob die Benutzerdaten erfolgreich wiederhergestellt wurden.

Beispielszenario 3: Wiederherstellung einer Teilmenge persönlicher vDisks in einem Maschinenkatalog

In diesem Szenario sind nur einige der persönlichen vDisks in einem Maschinenkatalog ausgefallen und werden wiederhergestellt. Die virtuellen Maschinen im Katalog sind nicht ausgefallen.

1. Führen Sie migration-backup.ps1 aus, um die Zuweisung zwischen Benutzern und persönlichen vDisks in der XML-Datei aufzuzeichnen.
2. Die XML-Datei enthält einen PVD-Abschnitt für jeden Benutzer im Maschinenkatalog. Entfernen Sie alle Benutzer, deren persönliche vDisks nicht wiederhergestellt werden müssen, und die zugehörigen Abschnitte aus der Datei.
3. Stellen Sie die persönlichen vDisks mit einer Backuplösung aus dem ursprünglichen Maschinenkatalog wie in einem der anderen Szenarios beschrieben wieder her:
   - Zum Verwenden neuer Maschinennamen folgen Sie Beispielszenario 1.
   - Zur Erhalten bestehenden Maschinennamen folgen Sie Beispielszenario 2.
4. Stellen Sie sicher, dass der Katalog genügend nicht zugewiesene Maschinen hat. Fügen Sie, falls erforderlich, Maschinen hinzu. Sie benötigen eine neue Maschine für jeden Benutzer, dessen vDisk Sie wiederherstellen möchten.
5. Stellen Sie sicher, dass die Desktopgruppe im Wartungsmodus ist und die enthaltenen Maschinen heruntergefahren sind.
6. Führen Sie auf dem Controller migration-restore.ps1 mit der geänderten XML-Datei als Eingabe aus.
7. Überprüfen Sie, ob die Benutzerdaten erfolgreich wiederhergestellt wurden.

Anzeigen, Meldungen und Problembehandlung

Feb 29, 2016

Wenn Sie in Studio eine PvD-aktivierte Maschine in einem Maschinenkatalog auswählen, können Sie auf der Registerkarte "PvD" den Überwachungsstatus während Imageupdates sowie die geschätzte Abschlusszeit und den Fortschritt verfolgen. Folgende Zustandsanzeigen sind während eines Imageupdates möglich: Ready, Preparing, Waiting, Failed und Requested.

Ein Imageupdate kann aus verschiedenen Gründen fehlschlagen, einschließlich zu wenig Speicherplatz oder weil ein Desktop die PvD nicht rechtzeitig findet. Wenn Studio angibt, dass ein Imageupdate fehlgeschlagen ist, wird ein Fehlercode mit beschreibendem Text angezeigt, um Sie bei der Problembehandlung zu unterstützen. Verwenden Sie das Überwachungstool für PvD-Imageupdates oder das Skript "personal-vdisk-poolstats.ps1" zum Überwachen des Imageupdatevorgangs und um Fehlercodes für das Problem zu erhalten.

Wenn ein Imageupdate fehlschlägt, finden Sie in den folgenden Protokolldateien weitere Informationen zur Problembehandlung:

- PvD-Dienstprotokoll: C:\ProgramData\Citrix\personal vDisk\Logs\PvDSvc.log.txt
- PvD-Aktivierungsprotokoll: P:\PVDLOGS\PvDActivation.log.txt

Der aktuelle Inhalt ist am Ende der Protokolldatei.

Fehlermeldungen: 7.6 und höher

Die folgenden Fehler gelten nur für PvD Version 7.6 und höher:

- **Ein interner Fehler ist aufgetreten. Weitere Informationen finden Sie in den Personal vDisk-Protokollen. Fehlercode% Disk (% s)**
  Dieser Code gilt für alle nicht kategorisierten Fehler und hat daher keinen numerischen Wert. Alle unerwarteten Fehler während der Bestandserstellung oder dem Update von Personal vDisk sind mit diesem Fehlercode gekennzeichnet.
  - Sammeln Sie die Protokolle und wenden Sie sich an den Citrix Support.
  - Wenn dieser Fehler während der Aktualisierung des Katalogs auftritt, führen Sie ein Rollback des Katalogs auf die vorherige Version des Masterimages aus.
- **Die Regeldateien enthalten Syntaxfehler. Weitere Informationen finden Sie in den Protokollen.**
  Fehlercode 2. Die Regeldatei enthält Syntaxfehler. Die Personal vDisk-Protokolldatei enthält den Namen der Regeldatei und die Zeile, in der der Syntaxfehler gefunden wurde. Beheben Sie den Syntaxfehler in der Regeldatei und wiederholen Sie den Vorgang.

- **Der in Personal vDisk gespeicherte Bestand, der der vorherigen Version des Masterimages entspricht, ist beschädigt oder nicht lesbar.**
  Fehlercode 3. Der letzte Bestand ist in "UserData.V2.vhd" unter "\ProgramData\CitrixPvD\Settings\Inventory\VER-LAST" gespeichert. Stellen Sie den Bestand entsprechend der letzten Version des Masterimages wieder her, indem Sie den Ordner "VER-LAST" von einer funktionierenden PvD-Maschine importieren, die der vorherigen Version des Masterimages zugeordnet ist.

- **Der in Personal vDisk gespeicherte Bestand, der der vorherigen Version des Masterimages entspricht, ist eine höhere Version.**
  Fehlercode 4. Die Ursache ist eine PvD-Versionsinkompatibilität zwischen dem letzten Masterimage und dem aktuellen Masterimage. Installieren Sie die aktuelle Version von Personal vDisk auf dem Masterimage und aktualisieren Sie den Katalog erneut.

- **Änderungsjournalüberlauf erkannt.**
  Fehlercode 5. Ein USN-Journalüberlauf wurde durch zahlreiche Änderungen am Masterimage während der Bestandserstellung verursacht. Wenn dieses Problem nach mehreren Versuchen weiterhin auftritt, ermitteln Sie mit Process Monitor, ob die Drittanbietersoftware während der Erstellung des Bestands zahlreiche Dateien erstellt oder löscht.

- **Personal vDisk konnte keinen an das System angeschlossenen Datenträger zum Speichern von Benutzerdaten finden.**
  Fehlercode 6. Überprüfen Sie zunächst, ob die PvD über die Hypervisor-Konsole mit der VM verbunden ist. Dieser Fehler tritt häufig auf, weil Software zum Vermeiden von Datenverlust den Zugriff auf die PvD verhindert. Wenn die PvD mit der VM verbunden ist, fügen Sie eine Ausnahme für den verbundenen Datenträger in der Konfiguration der Software zum Vermeiden von Datenverlust hinzu.

- **Das System wurde nach der Installation noch nicht neu gestartet. Starten Sie es neu, damit die Änderungen übernommen werden.**
  Fehlercode 7. Starten Sie den Desktop neu und wiederholen Sie den Vorgang.

- **Beschädigte Installation. Installieren Sie Personal vDisk neu.**
  Fehlercode 8. Installieren Sie Personal vDisk neu und versuchen Sie es noch einmal.

- **Der Personal vDisk-Bestand ist nicht auf dem aktuellen Stand. Aktualisieren Sie den Bestand auf dem Masterimage und versuchen Sie es noch einmal.**
  Fehlercode 9. Der Personal vDisk-Bestand wurde vor dem Herunterfahren des Desktops nicht auf dem Masterimages aktualisiert. Starten Sie das Masterimage neu und fahren Sie den Desktop mit der Option "Persönliche vDisk aktualisieren" herunter. Erstellen Sie dann einen neuen Snapshot und aktualisieren Sie damit den Katalog.

- **Beim Start von Personal vDisk ist ein interner Fehler aufgetreten Weitere Informationen finden Sie in den Personal vDisk-Protokollen.**
  Fehlercode 10. Die Ursache ist möglicherweise, dass der PvD-Treiber aufgrund eines internen Fehlers oder Beschädigung der persönlichen vDisk keine Virtualisierungssitzung starten kann. Starten Sie den Desktop über den Controller neu. Wenn das Problem weiterhin auftritt, sammeln Sie die Protokolle und wenden Sie sich an den Citrix Support.

- **Personal vDisk-Timeout bei dem Versuch, ein Speichermedium für die Personalisierungseinstellungen der Benutzer zu finden.**
  Fehlercode 11. Dieser Fehler tritt auf, wenn der PvD-Treiber den PvD-Datenträger nicht innerhalb von 30 Sekunden nach dem Neustart findet. Die Ursache ist normalerweise ein nicht unterstützter SCSI-Controllertyp oder Speicherlatenz. Wenn dieses Problem bei allen Desktops im Katalog auftritt, ändern Sie den der Vorlagen-VM bzw. Master-VM zugeordneten SCSI-Controllertyp in einen Typ, der von Personal vDisk unterstützt wird. Wenn dieses Problem nur bei einigen Desktops im Katalog auftritt, wird dies möglicherweise durch Speicherlatenz-Spitzen verursacht, weil zahlreiche Desktops gleichzeitig gestartet werden. Beschränken Sie die Einstellung für die maximale Anzahl aktiver Energieaktionen für die Hostverbindung.

- **Personal vDisk wurde deaktiviert, da das System nicht sicher heruntergefahren wurde. Starten Sie die Maschine neu.**
  Fehlercode 12. Möglicherweise kann ein Desktop bei aktivierter PvD den Startvorgang nicht abschließen. Starten Sie den Desktop neu. Wenn das Problem weiterhin auftritt, beobachten Sie den Startvorgang des Desktops über die Hypervisor-Konsole und prüfen Sie, ob der Desktop abstürzt. Wenn ein Desktop während des Starts abstürzt, stellen Sie die PvD aus einem Backup (wenn vorhanden) wieder her oder setzen Sie die PvD zurück.

- **Der zum Bereitstellen von Personal vDisk angegebene Laufwerksbuchstabe ist nicht verfügbar.**
  Fehlercode 13. Die Ursache ist möglicherweise, dass Personal vDisk den PvD-Datenträger nicht über das vom Administrator angegebene Laufwerk bereitstellen kann. Der PvD-Datenträger kann nicht bereitgestellt werden, wenn der Laufwerksbuchstabe bereits von anderer Hardware verwendet wird. Wählen Sie einen anderen Buchstaben als Bereitstellungspunkt für die persönliche vDisk aus.

- **Fehler beim Installieren von Personal vDisk-Kernelmodustreibern.**
  Fehlercode 14. Personal vDisk installiert Treiber während der ersten Bestandsaktualisierung nach der Installation. Einige Antivirenprodukte verhindern die Installation von Treibern außerhalb eines Installationsprogramms. Deaktivieren Sie vorübergehend den in Echtzeit ausgeführten Antivirenscan oder fügen Sie der Antivirensoftware während der ersten Bestandserstellung Ausnahmen für die PvD-Treiber hinzu.

- **Es konnte kein Snapshot des Systemvolumes erstellt werden. Stellen Sie sicher, dass der Volumeschattenkopie-Dienst aktiviert ist.**
  Fehlercode 15. Dieser Fehler kann auftreten, weil der Volumeschattenkopie-Dienst deaktiviert ist. Aktivieren Sie den Volumeschattenkopie-Dienst und versuchen Sie noch einmal, den Bestand aufzunehmen.

- **Fehler beim Aktivieren des Änderungsjournals. Warten Sie einige Minuten und versuchen Sie es noch einmal.**
  Fehlercode 16. Personal vDisk verwendet das Änderungsjournal für das Verfolgen von Änderungen am Masterimage. Wenn PvD bei einer Bestandsaktualisierung erkennt, dass das Änderungsjournal deaktiviert ist, versucht PvD, es zu aktivieren. Der Fehler tritt auf, wenn die Aktivierung fehlschlägt. Warten Sie ein paar Minuten und versuchen Sie es noch einmal.

- **Nicht genügend freier Speicherplatz auf dem Systemvolume.**
  Fehlercode 17. Für das Imageupdate ist nicht genug freier Speicherplatz auf dem Laufwerk C des Desktops vorhanden. Erweitern Sie das Systemvolume oder entfernen Sie nicht verwendete Dateien vom Systemvolume. Das Imageupdate sollte nach dem nächsten Neustart erneut beginnen.

- **Es ist nicht genügend freier Speicherplatz im Personal vDisk-Speicher. Erweitern Sie den Personal vDisk-Speicher.**
  Fehlercode 18. Es ist nicht genug freier Speicherplatz auf dem Laufwerk der persönlichen vDisk während des Imageupdatevorgangs vorhanden. Erweitern Sie den Personal vDisk-Speicher oder entfernen Sie nicht verwendete Dateien aus dem Personal vDisk-Speicher. Das Imageupdate sollte nach dem nächsten Neustart erneut beginnen.

- **Der Personal vDisk-Speicher ist überbucht. Erweitern Sie den Personal vDisk-Speicher.**
  Fehlercode 19. Es ist nicht genug freier Speicherplatz auf dem Laufwerk der persönlichen vDisk für die in vollem Umfang bereitgestellte "UserData.V2.vhd" vorhanden. Erweitern Sie den Personal vDisk-Speicher oder entfernen Sie nicht verwendete Dateien aus dem Personal vDisk-Speicher.

- **Fehlerhafte Systemregistrierung.**
  Fehlercode 20. Die Systemregistrierung ist beschädigt, nicht lesbar oder fehlt. Setzen Sie die persönliche vDisk zurück oder stellen Sie sie von einem früheren Backup wieder her.

- **Beim Zurücksetzen von Personal vDisk ist ein interner Fehler aufgetreten. Weitere Informationen finden Sie in den Personal vDisk-Protokollen.**
  Fehlercode 21. Dieser Code gilt für alle Fehler, die beim Zurücksetzen von Personal vDisk auftreten. Sammeln Sie die Protokolle und wenden Sie sich an den Citrix Support.

- **Personal vDisk konnte nicht zurückgesetzt werden, da nicht genügend freier Speicherplatz im persönlichen vDisk-Speicher ist.**

Fehlercode 22. Es ist nicht genug freier Speicherplatz auf dem Laufwerk der persönlichen vDisk während eines Zurücksetzungsvorgangs vorhanden. Erweitern Sie den Personal vDisk-Speicher oder entfernen Sie nicht verwendete Dateien aus dem Personal vDisk-Speicher.

Fehlermeldungen: vor Version 7.6

Die folgenden Fehler gelten nur für PvD 7.x-Versionen vor Version 7.6:

- **Start fehlgeschlagen. Personal vDisk konnte kein Speichermedium für die Personalisierungseinstellungen der Benutzer finden.**
  Die PvD-Software konnte die Personal vDisk (standardmäßig Laufwerk P:) nicht finden oder nicht als den vom Administrator bei der Erstellung des Katalogs ausgewählten Bereitstellungspunkt bereitstellen.
  - Prüfen Sie, ob Sie im PvD-Dienstprotokoll den folgenden Eintrag finden: "PvD 1 status --> 18:183".
  - Wenn Sie eine ältere Version als PvD Version 5.6.12 verwenden, löst ein Upgrade auf die aktuelle Version das Problem.
  - Wenn Sie Version 5.6.12 oder höher verwenden, prüfen Sie mit dem Datenträgerverwaltungstool (diskmgmt.msc), ob das Laufwerk P: als nicht bereitgestelltes Volume vorhanden ist. Wenn es vorhanden ist, führen Sie chkdsk auf dem Volume aus, um festzustellen, ob es fehlerhaft ist. Versuchen Sie, das Volume mit chkdsk wiederherzustellen.
- **Start fehlgeschlagen. Fehler beim Start von Citrix Personal vDisk. Weitere Informationen ... Statuscode: 7, Fehlercode: 0x70**
  Statuscode 7 bedeutet, dass ein Fehler beim Update der PvD aufgetreten ist. Es gibt die folgenden Fehler:

Fehlercode	Beschreibung
0x20000001	Fehler beim Speichern des Vergleichspakets, wahrscheinlich aufgrund von Speicherplatzmangel auf der virtuellen Festplatte.
0x20000004	Unzureichende Privilegien zum Aktualisieren der PvD.
0x20000006	Fehler beim Laden der Struktur aus dem PvD-Image oder dem PvD-Bestand, wahrscheinlich aufgrund eines fehlerhaften PvD-Images oder PvD-Bestands.
0x20000007	Fehler beim Laden des Dateisystembestands, wahrscheinlich aufgrund eines fehlerhaften PvD-Images oder PvD-Bestands.
0x20000009	Fehler beim Öffnen der Datei mit dem Dateisystembestand, wahrscheinlich aufgrund eines fehlerhaften PvD-Images oder PvD-Bestands.
0x2000000B	Fehler beim Speichern des Vergleichspakets, wahrscheinlich aufgrund von Speicherplatzmangel auf der virtuellen Festplatte.
0x20000010	Fehler beim Laden des Vergleichspakets.
0x20000011	Regeldateien fehlen.
0x20000021	Fehlerhafter PvD-Bestand.
0x20000027	Der Katalog "MojoControl.dat" ist fehlerhaft.

Fehlercode	Beschreibung
0x2000002B	PvD-Bestand fehlerhaft oder fehlt.
0x2000002F	Fehler beim Registrieren des vom Benutzer installierten MOF beim Imageupdate. Lösung: Upgrade auf Version 5.6.12.
0x20000032	Suchen Sie in PvDactivation.log.txt nach dem letzten Eintrag mit einem Win32-Fehlercode.
0x20	Fehler beim Bereitstellen des Anwendungscontainers für Imageupdate. Lösung: Upgrade auf Version 5.6.12.
0x70	Nicht genügend Speicherplatz auf dem Datenträger.

- **Start fehlgeschlagen. Fehler beim Start von Citrix Personal vDisk [oder Personal vDisk hat einen internen Fehler festgestellt]. Weitere Informationen... Statuscode 20, Fehlercode 0x20000028**
  Die persönliche vDisk wurde gefunden, eine PvD-Sitzung konnte jedoch nicht erstellt werden.

  Sammeln Sie die Protokolle und prüfen Sie das Protokoll "SysVol-IvmSupervisor.log" auf Sitzungserstellungsfehler:
  1. Suchen Sie nach dem Protokolleintrag "IvmpNativeSessionCreate: failed to create native session, status XXXXX".
  2. Wenn der Status 0xc00002cf ist, können Sie das Problem lösen, indem Sie eine neue Version des Masterimages zum Katalog hinzufügen. Dieser Statuscode bedeutet, dass ein USN-Journalüberlauf aufgrund zahlreicher Änderungen nach einer Bestandsaktualisierung aufgetreten ist.
  3. Starten Sie den betroffenen virtuellen Desktop neu. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support von Citrix.
- **Start fehlgeschlagen. Citrix Personal vDisk wurde deaktiviert, da das System nicht sicher heruntergefahren wurde. Wählen Sie "Noch einmal versuchen". Wenn das Problem weiterhin besteht, wenden Sie sich an den Systemadministrator.**
  Die gepoolte VM kann den Start nicht ausführen, solange die PvD aktiviert ist. Stellen Sie zuerst fest, warum der Start nicht ausgeführt werden kann. Eine mögliche Ursache ist die Anzeige eines blauen Bildschirms aus einem der folgenden Gründe:
  - Ein nicht kompatibles Antivirenprodukt ist auf dem Masterimage vorhanden, z. B. alte Versionen von Trend Micro.
  - Der Benutzer hat Software installiert, die mit PvD nicht kompatibel ist. Dies ist zwar unwahrscheinlich, aber Sie können es überprüfen, indem Sie dem Katalog eine neue Maschine hinzufügen und testen, ob sie neu startet.
  - Das PvD-Image ist fehlerhaft. Dieser Fehler wurde in Version 5.6.5 beobachtet.

  Prüfen, ob die gepoolte VM einen blauen Bildschirm anzeigt oder ob sie vorzeitig neu startet:
  - Melden Sie sich bei der Maschine über die Hypervisor-Konsole an.
  - Klicken Sie auf Noch einmal versuchen und warten Sie, bis die Maschine heruntergefahren ist.
  - Starten Sie die Maschine über Studio.
  - Beobachten Sie die Maschinenkonsole während des Starts mit der Hypervisor-Konsole.

  Weitere Problembehandlungsschritte:
  - Senden Sie das Speicherabbild der Maschine, die den blauen Bildschirm hat, zur Analyse an den technischen Support von Citrix.
  - Prüfen Sie auch die der PvD zugeordneten Ereignisprotokolle auf Fehler:
    1. Stellen Sie "UserData.V2.vhd" (im Stamm von Laufwerk P:) mithilfe von DiskMgmt.msc bereit, indem Sie auf Aktion > Virtuelle Festplatte anfügen klicken.
    2. Starten Sie "Eventvwr.msc".
    3. Öffnen Sie das Systemereignisprotokoll (Windows\System32\winevt\logs\system.evtx) aus UserData.V2.vhd, indem

Sie auf Aktion > Gespeichertes Protokoll öffnen klicken.

4. Öffnen Sie das Anwendungsereignisprotokoll (Windows\System32\winevt\logs\application.evtx) aus UserData.V2.vhd, indem Sie auf Aktion > Gespeichertes Protokoll öffnen klicken.

- **Die persönliche vDisk kann nicht gestartet werden. Die persönliche vDisk konnte nicht gestartet werden, da der Bestand nicht aktualisiert worden ist. Aktualisieren Sie den Bestand auf dem Masterimage und versuchen Sie es noch einmal. Statuscode: 15, Fehlercode: 0x0**
  Der Administrator hat beim Erstellen oder Aktualisieren des PvD-Katalogs den falschen Snapshot ausgewählt (d. h. das Masterimage wurde beim Erstellen des Snapshots nicht mit Persönliche vDisk aktualisieren heruntergefahren).

Von Personal vDisk protokollierte Ereignisse

Wenn Personal vDisk nicht aktiviert ist, können Sie die folgenden Ereignisse in der Windows-Ereignisanzeige anzeigen. Wählen Sie im linken Bereich den Knoten Anwendungen, die Quelle im rechten Bereich ist Citrix Personal vDisk. Wenn Personal vDisk aktiviert ist, werden diese Ereignisse nicht angezeigt.

Die Ereignis-ID 1 bedeutet, dass es sich um eine Informationsmeldung handelt. ID 2 steht für einen Fehler. Möglicherweise werden nicht alle Ereignisse in jeder Personal vDisk-Version verwendet.

Ereignis-ID	Beschreibung
1	Status von Personal vDisk: Bestandsaktualisierung gestartet.
1	Status von Personal vDisk: Bestandsaktualisierung abgeschlossen. GUID: %s.
1	Status von Personal vDisk: Imageupdate gestartet.
1	Status von Personal vDisk: Imageupdate abgeschlossen.
1	Zurücksetzen wird durchgeführt.
1	OK.
2	Status von Personal vDisk: Bestandsaktualisierung fehlgeschlagen mit: %s.
2	Status von Personal vDisk: Imageupdate fehlgeschlagen mit: %s.
2	Status von Personal vDisk: Imageupdate fehlgeschlagen, interner Fehler.
2	Status von Personal vDisk: Bestandsaktualisierung fehlgeschlagen: interner Fehler.
2	Personal vDisk wurde unsachgemäß beendet und daher deaktiviert.
2	Imageupdate fehlgeschlagen. Fehlercode %d.

Ereignis-ID	Beschreibung
2	Personal vDisk hat einen internen Fehler festgestellt. Statuscode[%d] Fehlercode[0x%X].
2	Zurücksetzung von Personal vDisk fehlgeschlagen.
2	Datenträger zum Speichern der angepassten Benutzereinstellungen kann nicht gefunden werden.
2	Zum Erstellen eines Personal vDisk-Containers ist nicht genug Speicherplatz auf dem Datenträger vorhanden.

Entfernen von Komponenten

Feb 29, 2016

Zum Entfernen von Komponenten empfiehlt Citrix die Verwendung der Windows-Funktion zum Entfernen oder Ändern von Programmen. Alternativ können Sie Komponenten über die Befehlszeile oder mit einem auf dem Installationsmedium enthaltenen Skript entfernen.

Beim Entfernen von Komponenten werden keine Voraussetzungen entfernt und keine Firewalleinstellungen geändert. Wenn Sie einen Controller entfernen, werden die SQL-Serversoftware und die Datenbanken nicht entfernt.

Bevor Sie einen Controller entfernen, müssen Sie ihn aus der Site entfernen. Vor dem Entfernen von Studio oder Director empfiehlt Citrix das Schließen dieser Anwendungen.

Wenn Sie einen Controller von einer früheren Bereitstellung mit dem Web Interface aktualisiert haben, müssen Sie zuerst die Webinterface-Komponente separat entfernen. Das Webinterface kann nicht mit dem Installationsprogramm entfernt werden.

Entfernen von Komponenten mit der Windows-Funktion zum Entfernen oder Ändern von Programmen

Gehen Sie mit der Windows-Funktion zum Entfernen oder Ändern von Programmen wie folgt vor:

- Zum Entfernen eines Controllers, von Studio, Director, eines Lizenzservers oder von StoreFront wählen Sie Citrix XenApp oder Citrix XenDesktop , klicken Sie mit der rechten Maustaste und wählen Sie Deinstallieren. Das Installationsprogramm wird gestartet und Sie können die zu entfernenden Komponenten markieren.
  Alternativ können Sie StoreFront entfernen, indem Sie mit der rechten Maustaste auf Citrix StoreFront klicken und dann Deinstallieren auswählen.
- Klicken Sie zum Entfernen eines VDAs auf Citrix Virtual Delivery Agent , klicken Sie mit der rechten Maustaste und wählen Sie Deinstallieren. Das Installationsprogramm wird gestartet und Sie können die zu entfernenden Komponenten markieren.
- Zum Entfernen des universellen Druckservers wählen Sie Citrix Universeller Druckserver, klicken Sie mit der rechten Maustaste und wählen Sie Deinstallieren.

Entfernen von Kernkomponenten über die Befehlszeile

Führen Sie auf dem Installationsmedium im Setupverzeichnis \x64\XenDesktop den Befehl XenDesktopServerSetup.exe aus.

- Zum Entfernen einer oder mehrerer Komponenten verwenden Sie die Optionen "/remove" und "/components".
- Zum Entfernen aller Komponenten verwenden Sie die Option "/removeall".

Informationen zu Befehl und Parametern finden Sie unter Installieren über die Befehlszeile.

Mit dem folgenden Befehl wird beispielsweise Studio entfernt:

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /remove /components studio
```

Entfernen eines VDAs über die Befehlszeile

Führen Sie auf dem Installationsmedium im Setupverzeichnis \x64\XenDesktop den Befehl XenDesktopServerSetup.exe aus.

- Zum Entfernen einer oder mehrerer Komponenten verwenden Sie die Optionen "/remove" und "/components".
- Zum Entfernen aller Komponenten verwenden Sie die Option "/removeall".

Informationen zu Befehl und Parametern finden Sie unter Installieren über die Befehlszeile.

Mit dem folgenden Befehl werden beispielsweise der VDA und Receiver entfernt:
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /removeall
Informationen zum Entfernen von VDAs mit einem Skript in Active Directory finden Sie unter Installieren oder Entfernen von Virtual Delivery Agents mit Skripts.

Upgrades und Migration

Feb 29, 2016

Upgrades

Bei Upgrades werden Bereitstellungen auf die neuesten Komponentenversionen aktualisiert, ohne dass neue Maschinen oder Sites erstellt werden müssen. Ein solches Upgrade wird als direktes Upgrade bezeichnet. Sie können ein Upgrade folgender Versionen durchführen:

- Von XenDesktop 5 (oder einer höheren Version) auf die aktuelle XenDesktop-Version
- Von XenApp 7.5 auf die aktuelle XenApp-Version

Sie können auch einen XenApp 6.5-Workerserver auf einen aktuellen XenApp 7.6 für Windows-Serverbetriebssysteme aktualisieren. Dies ist eine zusätzliche Aktivität bei der Migration von XenApp 6.5.

Aktualisieren einer XenDesktop 5-Farm (oder höher) oder einer XenApp 7.5-Site

1. Führen Sie das Installationsprogramm auf den Maschinen aus, auf denen die Kernkomponenten und VDAs installiert sind. Die Software ermittelt, ob ein Upgrade zur Verfügung steht und installiert die aktuelle Version.
2. Verwenden Sie das aktualisierte Studio zum Aktualisieren der Datenbank und der Site.

Weitere Informationen finden Sie unter Upgrade einer Bereitstellung.

Weitere Informationen zur Installation von Hotfixes für Controller finden Sie im Knowledge Center-Artikel CTX201988.

Aktualisieren eines XenApp 6.5-Workerserver auf einen aktuellen VDA:

1. Führen Sie das Produktinstallationsprogramm auf dem XenApp 6.5-Workerserver aus. Die Software entfernt den Server aus der XenApp 6.5-Farm, dann wird die XenApp 6.5-Software entfernt und ein aktueller VDA für Windows-Serverbetriebssysteme wird installiert.
2. Fügen Sie den Server nach dem Upgrade den Maschinenkatalogen und Bereitstellungsgruppen der aktuellen Site hinzu.

Weitere Informationen finden Sie unter Upgrade eines XenApp 6.5-Workers auf einen neuen VDA für Windows-Serverbetriebssysteme.

Migration

Durch Migration werden Daten von einer früheren Bereitstellung in die aktuelle Version verschoben. Sie können sowohl eine XenApp 6.5- als auch eine XenDesktop 4-Bereitstellung migrieren. Eine Migration umfasst die Installation aktueller Komponenten und das Erstellen einer neuen Site, das Exportieren der Daten aus der älteren Farm und dann das Importieren der Daten in die neue Site.

Migrieren von XenApp 6.5

1. Installieren Sie die Kernkomponenten und erstellen Sie eine neue XenApp-Site.
2. Exportieren Sie Richtlinien- und/oder Farmdaten vom XenApp 6.5-Controller mit PowerShell-Cmdlets in XML-Dateien. Sie können den Inhalt der XML-Dateien bearbeiten, um die zu importierenden Informationen anzupassen.
3. Importieren Sie in der neuen Site die Richtlinien- und/oder Anwendungsdaten mit PowerShell-Cmdlets und den XML-Dateien.
4. Schließen Sie die nach der Migration erforderlichen Schritte für die neue Site ab.

Weitere Informationen finden Sie unter Migrieren von XenApp 6.x

Migrieren von XenDesktop 4

1. Installieren Sie die Kernkomponenten und erstellen Sie eine neue XenDesktop-Site.
2. Exportieren Sie mit dem Exportbefehl die Farmdaten von der XenDesktop 4-Farm in eine XML-Datei. Sie können den Inhalt der XML-Dateien bearbeiten, um die zu importierenden Informationen anzupassen.
3. Importieren Sie in der neuen Site die Farmdaten mit dem Importbefehl und der XML-Datei.
4. Schließen Sie die nach der Migration erforderlichen Schritte für die neue Site ab.

Weitere Informationen finden Sie unter Migrieren von XenDesktop 4.

Upgrade einer Bereitstellung

Feb 29, 2016

Dieser Abschnitt enthält folgende Themen:

- Einführung
- Aktualisierbare Produktkomponenten
- Anforderungen, Einschränkungen und Vorbereitung
- Hinweise zu heterogenen Umgebungen
- VDAs auf Maschinen mit Windows XP oder Windows Vista
- VDAs auf Maschinen mit Windows 8.x oder Windows 7
- Unterstützung gemischter VDAs
- Aktualisierungsreihenfolge

Einführung

Sie können bestimmte Bereitstellungen aktualisieren, ohne zunächst neue Maschinen oder Sites erstellen zu müssen. Ein solches Upgrade wird als direktes Upgrade bezeichnet. Sie können ein Upgrade folgender Versionen durchführen:

- Von XenDesktop 5 (oder einer höheren Version) auf die neueste freigegebene ("aktuelle") XenDesktop-Version
- Von XenApp 7.5 (oder einer höheren Version) auf die neueste freigegebene ("aktuelle") XenApp-Version

Sie können mit dem aktuellen XenApp-Installationsprogramm auch einen XenApp 6.5-Workerserver auf einen aktuellen VDA für Windows-Serverbetriebssysteme aktualisieren. Dies ist eine zusätzliche Aktivität bei der Migration von XenApp 6.5. Weitere Informationen finden Sie unter Upgrade eines XenApp 6.5-Workers auf einen neuen VDA für Windows-Serverbetriebssysteme.

Zum Starten eines Upgrades führen Sie das Installationsprogramm in der neuen Version aus, um zuvor installierte Kernkomponenten (Delivery Controller, Citrix Studio, Citrix Director, Citrix Lizenzserver) sowie Virtual Delivery Agents zu aktualisieren. Das Installationsprogramm ermittelt, welche Komponenten ein Upgrade erfordern und startet dann das Upgrade auf Ihren Befehl hin. Nach dem Upgrade der Komponenten verwenden Sie die neu aktualisierte Version von Studio zum Durchführen des Upgrades der Site-Datenbank und der Site.

Im vorliegenden Dokument bezieht sich "Produkt", sofern nicht anders angegeben, auf XenApp 7.x oder XenDesktop 7.x.

Aktualisierbare Produktkomponenten

Mit dem Produktinstallationsprogramm und Studio können Sie folgende Komponenten aktualisieren:

- Delivery Controller 5 oder höher
- VDA 5.0 SP1 oder höher
  - Im Gegensatz zu früheren VDA-Releases müssen Sie für das Upgrade der VDAs das Produktinstallationsprogramm verwenden, MSI-Dateien können nicht verwendet werden.
  - Wenn das Installationsprogramm auf der Maschine Receiver für Windows erkennt (Receiver.exe), erfolgt ein Upgrade auf die Receiver-Version auf dem Installationsmedium des Produkts.

    - Wenn das Installationsprogramm Receiver für Windows Enterprise (CitrixReceiverEnterprise.exe) auf einer Maschine erkennt, wird das Programm auf Receiver für Windows Enterprise 3.4 aktualisiert
- Director 1 oder höher
- Datenbank: Es erfolgen ein Upgrade des Schemas und eine Migration der Daten der Sitedatenbank (sowie der Konfigurationsprotokollierungsdatenbank und der Überwachungsdatenbank, sofern eine frühere 7.x-Version aktualisiert wird).
- Personal vDisk

Aktualisieren Sie, falls erforderlich, anhand der Informationen in der Feature-/Produktdokumentation die folgenden Elemente:

- Provisioning Services (für XenApp 7.x und XenDesktop 7.x empfiehlt Citrix, dass Sie die aktuelle freigegebene Version verwenden; die unterstützte Mindestversion ist Provisioning Services 7.0).
    - Aktualisieren Sie den Provisioning Services-Server mit dem parallelen Serverupgrade und die Clients mit der vDisk-Versionsverwaltung.
    - Provisioning Services 7.x unterstützt nicht das Erstellen von neuen Desktops mit Versionen von XenDesktop 5. Obwohl vorhandene Desktops weiterhin funktionieren, können Sie daher mit Provisioning Services 7.x erst dann neue Desktops erstellen, wenn Sie für XenDesktop ein Upgrade durchgeführt haben. Wenn Sie eine heterogene Umgebung mit XenDesktop 5.6 und XenDesktop 7.x-Sites planen, führen Sie daher kein Upgrade von Provisioning Services auf Version 7 durch.
- Microsoft System Center Virtual Machine Manager SCVMM. Das aktuelle Produkt unterstützt SCVMM 2012 und SCVMM 2012 SP1. XenDesktop 5.x unterstützt frühere Versionen. Verwenden Sie zur Minimierung von Ausfallzeiten die folgende Upgradereihenfolge:
    1. Wenn Sie Controller mit Versionen vor XenDesktop 5.6 FP1 haben, aktualisieren Sie diese auf XenDesktop 5.6 FP1 (siehe XenDesktop-Dokumentation für Version 5.6 FP1).
    2. Aktualisieren Sie die SCVMM-Server auf SCVMM 2012 (Anweisungen finden Sie in der Dokumentation von Microsoft).
    3. Aktualisieren Sie die XenDesktop-Komponenten auf die aktuelle Version.
    4. Falls gewünscht, können Sie ein Upgrade des SCVMM-Servers auf SCVMM 2012 SP1 durchführen.
- StoreFront:

Anforderungen, Einschränkungen und Vorbereitung

- Sie müssen die grafische Benutzeroberfläche oder die Befehlszeilenschnittstelle des Installationsprogramms für das Upgrade der Kernkomponenten und VDAs verwenden. Sie können keine Daten von einer früheren Version importieren oder migrieren.
- Wenn Sie Komponenten auf die neue Version aktualisieren, andere Komponenten (auf anderen Maschinen) jedoch nicht, wird von Studio eine Erinnerung ausgegeben. Beispiel: Wenn ein Upgrade neue Versionen von Controller und Studio enthält und Sie nur den Controller aktualisieren (jedoch das Installationsprogramm auf der Maschine, auf der Studio installiert ist, nicht ausführen) lässt Studio eine Verwaltung der Site erst dann wieder zu, wenn Sie auch für Studio ein Upgrade durchgeführt haben.
- Stellen Sie vor dem Upgrade des Citrix Lizenzservers sicher, dass Ihr Subscription Advantage-Datum für die neue Produktversion gültig ist. Wenn Sie ein Upgrade einer früheren 7.x-Produktversion durchführen, muss das Datum mindestens 2015.1118 sein.
- Sie können kein Upgrade von XenDesktop Express Edition durchführen. Beschaffen und installieren Sie eine Lizenz für eine derzeit unterstützte Edition und führen Sie anschließend ein Upgrade durch.
- Vor Beginn einer Upgradeaktivität sichern Sie die Datenbank (siehe CTX135207), damit Sie sie im Falle eines Problems

nach dem Datenbankupgrade wieder herstellen können.
- Optional können Sie Vorlagen sichern und evtl. verwendete Hypervisors aktualisieren.
- Wenn Sie Sites einer früheren Version neben Sites der aktuellen Version beibehalten müssen, lesen Sie den Abschnitt Hinweise zu heterogenen Umgebungen.
- Wenn Sie VDAs unter Windows XP oder Windows Vista installiert haben, lesen Sie den Abschnitt VDAs auf Maschinen mit Windows XP oder Windows Vista.
- Wenn Sie nicht alle VDAs auf die aktuelle Version aktualisieren möchten, lesen Sie Unterstützung gemischter VDAs.
- Enthält Ihre Bereitstellung Webinterface, empfiehlt Citrix die Verwendung von StoreFront.
- Auf den Maschinen, auf denen Sie die Produktkomponenten aktualisieren, müssen Sie sowohl Domänenbenutzer als auch lokaler Administrator sein.
- Lesen Sie den Abschnitt zur Upgradereihenfolge, damit Sie mögliche Ausfälle einplanen und das Risiko entschärfen können.

In folgenden Situationen ist kein Upgrade möglich:

- Bei einer Early Release- oder Technology Preview-Version
- Bei einer XenApp-Version vor 7.5 (außer Sie ersetzen XenApp 6.5-Software auf einem Server mit einem aktuellen VDA für Serverbetriebssysteme, siehe Migrieren von XenApp 6.x)
- Bei einer XenDesktop-Version vor Version 5.6, siehe Migrieren von XenDesktop 4.
- Von XenApp auf XenDesktop oder von XenDesktop auf XenApp

Hinweise zu heterogenen Umgebungen

Wenn Ihre Umgebung Sites/Farmen mit mehreren Produktversionen enthält (heterogene Umgebung), empfiehlt Citrix die Verwendung von StoreFront zum Aggregieren von Anwendungen und Desktops aus den unterschiedlichen Produktversionen (Beispiel: Sie haben eine XenDesktop 7.1-Site und eine XenDesktop 7.5-Site). Weitere Informationen finden Sie in der Dokumentation zu StoreFront.

- Im Allgemeinen werden von der aktuellen Studio- bzw. Director-Version nur aktuelle Sites verwaltet bzw. überwacht. (Diese Version von Director kann zwar XenDesktop 5.x-VDAs überwachen, jedoch sind einige Daten, u. a. die Anmeldedauer, für diese VDAs nicht verfügbar.) Sie können beispielsweise keine XenDesktop 7.1-Site mit Studio 7.6 verwalten. Analog dazu können Sie eine XenDesktop 7.6-Site nicht mit Studio 7.1 verwalten.
- Verwenden Sie in einer heterogenen Umgebung weiterhin Studio und Director für das jeweilige Release. Die verschiedenen Versionen müssen jedoch auf separaten Maschinen installiert sein.
- Sie können aktuelle VDAs in Bereitstellungen mit älteren Controllerversionen verwenden. Allerdings sind in diesem Fall neue Features des aktuellen Releases möglicherweise nicht verfügbar. Weitere Informationen finden Sie unter "Hinweise zu gemischten VDAs" weiter unten.
- Sites mit Controllern der Version 5.x und VDAs der Version 7.x sollten in diesem Zustand nur vorübergehend verbleiben. Im Idealfall sollten Sie das Upgrade aller Komponenten so schnell wie möglich durchführen.
- Wenn Sie XenDesktop 5.6 und XenDesktop 7.x-Sites parallel ausführen und für beide Provisioning Services verwenden möchten, stellen Sie entweder eine neue Version von Provisioning Services für die Verwendung mit der 7.x-Site bereit oder aktualisieren Sie die aktuelle Version von Provisioning Services. In diesem Fall können Sie jedoch keine neuen Arbeitslasten in der XenDesktop 5.6-Site mehr bereitstellen.
- Führen Sie ein Upgrade einer eigenständigen Studio-Version erst dann durch, wenn Sie zur Verwendung der neuen Version bereit sind.

VDAs auf Maschinen mit Windows XP oder Windows Vista

Sie können kein Upgrade von VDAs auf Maschinen mit Windows XP oder Windows Vista auf eine 7.x-Version durchführen. Sie müssen VDA 5.6 FP1 mit bestimmten Hotfixes verwenden. Anweisungen hierfür finden Sie unter CTX140941. Obwohl ältere VDAs in einer 7.x-Site funktionieren, können zahlreiche Features nicht verwendet werden. Beispiele:

- Features in Studio, die eine neuere VDA-Version erfordern
- Konfiguration von App-V-Anwendungen über Studio
- Konfiguration von Receiver StoreFront-Adressen über Studio
- Automatische Unterstützung der Microsoft Windows-KMS-Lizenzierung bei Verwendung von Maschinenerstellungsdiensten Siehe CTX128580.
- Informationen in Director:
  - Anmeldezeiten und Anmeldeende-Ereignisse, die sich auf die Anmeldungsdauer auswirken, in den Ansichten "Dashboard", "Trends" und "Benutzerdetails"
  - Eine Aufschlüsselung der Anmeldedauer für HDX-Verbindungs- und Authentifizierungszeiten sowie Zeitdauerangaben für Profil- und GPO-Ladevorgänge, Anmeldeskript und die Herstellung interaktiver Sitzungen
  - Einige Kategorien der Fehlerraten für Maschinen und Verbindungen
  - Aktivitätsmanager in der Ansicht "Helpdesk" und "Benutzerdetails"

Citrix empfiehlt ein Reimaging der Windows XP- und Windows Vista-Maschinen unter einer unterstützten Betriebssystemversion und die anschließende Installation der aktuellen VDA-Version.

VDAs auf Maschinen mit Windows 8.x oder Windows 7

Für ein Upgrade von VDAs auf Maschinen mit Windows 8.x oder Windows 7 auf Windows 10 empfiehlt Citrix ein Reimaging der Maschinen mit Windows 7 und 8.x auf Windows 10 und die anschließende Installation der VDAs für Windows 10. Ist ein Reimaging nicht möglich, deinstallieren Sie den VDA vor dem Upgrade des Betriebssystems, da er ansonsten einen nicht unterstützten Zustand annimmt.

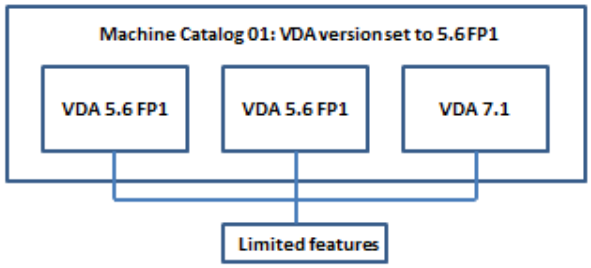
Unterstützung gemischter VDAs

Für ein Upgrade des Produkts auf eine neuere Version empfiehlt Citrix, dass Sie alle Kernkomponenten und VDAs aktualisieren, damit Sie alle neuen und verbesserten Features der Edition verwenden können. Beispiel: Zur Verwendung der Features Sitzungsvorabstart, Sitzungsfortbestehen und nicht authentifizierte Benutzer des Releases 7.6 müssen die VDAs mindestens in Version 7.6 vorliegen.

In einigen Umgebungen ist ein Upgrade aller VDAs auf die aktuelle Version möglicherweise nicht möglich. In diesem Fall können Sie beim Erstellen eines Maschinenkatalogs die auf den Maschinen installierte VDA-Version angeben. Standardmäßig ist für diese Einstellung die neueste empfohlene VDA-Version festgelegt. Sie müssen eine Änderung dieser Einstellung nur dann in Betracht ziehen, wenn der Maschinenkatalog Maschinen mit früheren VDA-Versionen enthält. Das

Vorhandensein mehrerer VDA-Versionen im selben Maschinenkatalog kann jedoch unerwünschte Auswirkungen haben.

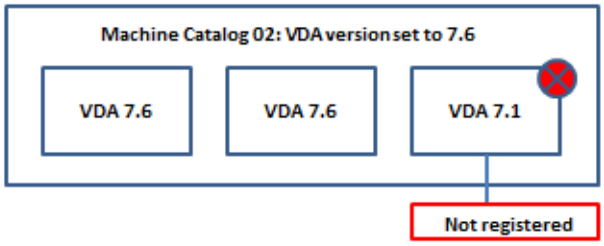
Wie oben erwähnt muss in Bereitstellungen mit Windows XP- und Windows Vista-Systemen eine frühere VDA-Version verwendet werden. Für den Maschinenkatalog, der die entsprechenden Maschinen enthält, muss VDA Version 5.6 FP1 festgelegt werden. Die VDAs können sich erfolgreich beim Controller registrieren, doch die Maschinen können viele der neuen Features der 7.x-Versionen (einschließlich StoreFront) nicht verwenden. Das Gleiche gilt für Maschinen mit VDAs der Version 7.x, die Sie einem solchen Katalog hinzufügen. Dies wird in der folgenden Abbildung dargestellt.



Wenn Sie wie im o. g. Fall ältere VDAs weiterhin verwenden müssen, fassen Sie diese in einem eigenen Maschinenkatalog zusammen.

Wenn ein Maschinenkatalog mit der standardmäßig empfohlenen VDA-Versionseinstellung erstellt wird und auf Maschinen in dem Katalog eine frühere VDA-Version installiert ist, können sich diese Maschinen nicht beim Controller registrieren und funktionieren nicht.

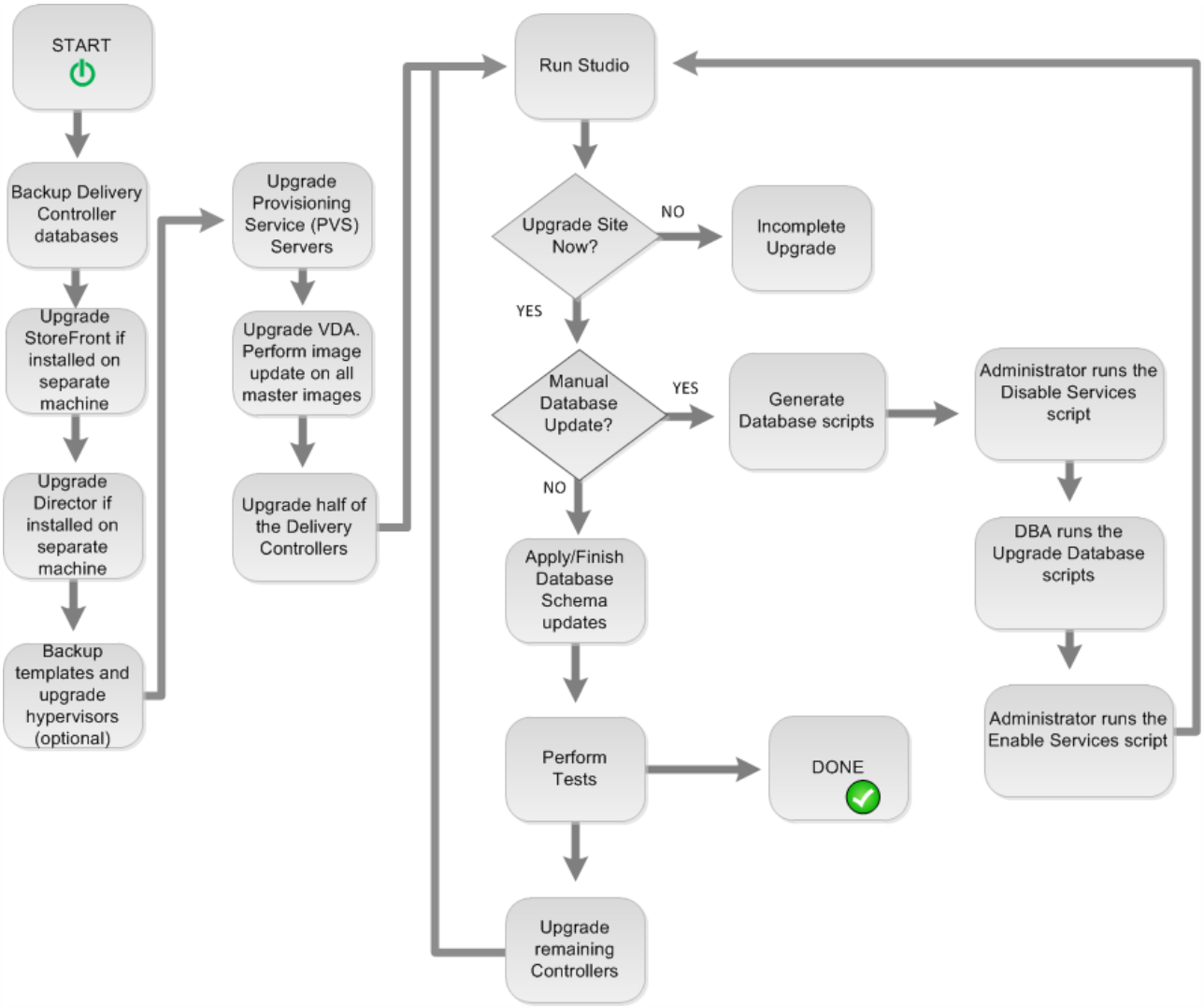
Beispiel (aktuelle VDA-Version sei 7.6): Sie erstellen einen Maschinenkatalog mit der VDA-Standardeinstellung: "7.6 (für die neuesten Features empfohlen)". Sie fügen dem Katalog drei Maschinen hinzu, zwei mit VDA 7.6 und eine mit VDA 7.1.



Die Maschine mit VDA 7.1 kann sich in diesem Fall nicht beim Controller registrieren. Wenn Sie kein Upgrade dieses VDAs durchführen können, können Sie einen separaten Maschinenkatalog mit einer VDA-Einstellung von Version 7.0 oder höher erstellen und diesem die Maschine hinzufügen. Die Maschine kann dann zwar die neuen Features der Version 7.6 nicht nutzen, sie kann sich jedoch beim Controller registrieren.

Aktualisierungsreihenfolge

Die Reihenfolge für das Upgrade ist nachfolgend aufgeführt, Erläuterungen folgen. Wenn Komponenten auf unterschiedlichen Maschinen installiert sind, führen Sie das Installationsprogramm auf jeder dieser Maschinen durch.



Aktualisieren von Komponenten

Zum Ausführen der grafischen Oberfläche des Installationsprogramms melden Sie sich bei der Maschine an und legen Sie anschließend das Installationsmedium ein oder stellen Sie das ISO-Laufwerk für das neue Release bereit. Doppelklicken Sie auf **AutoSelect**. Anweisungen zur Verwendung der Befehlszeilenschnittstelle finden Sie unter "Installieren über die Befehlszeile".

1. Wenn mehrere Kernkomponenten (z. B. Controller, Studio und Lizenzserver) auf dem gleichen Server installiert sind und für mehrere dieser Komponenten eine neue Version verfügbar ist, werden alle beim Ausführen des Installationsprogramms auf dem Server aktualisiert. Wenn Kernkomponenten auf anderen Maschinen als dem Controller installiert sind, führen Sie das Installationsprogramm auf diesen Maschinen aus (empfohlene Reihenfolge: Lizenzserver, StoreFront und dann Director).
2. Aktualisieren Sie die Provisioning Services-Server und -Clients (Anweisungen hierzu finden Sie in der Dokumentation zu Provisioning Services).
3. Führen Sie das Produktinstallationsprogramm auf Maschinen mit VDAs aus. Sie können zwar ein Upgrade der VDAs vor oder nach dem Upgrade des Controllers durchführen, Citrix empfiehlt jedoch ein Upgrade vor dem des Controllers, damit anschließend neue Features schnell aktiviert werden können.
   Wenn Sie ein Upgrade für VDAs von einer früheren 7.x-Version auf physischen Maschinen (einschließlich Remote-PC-

Zugriff-Maschinen) durchführen, verwenden Sie die Befehlszeilenschnittstelle mit dem folgenden Parameter: /EXCLUDE "Personal vDisk","Machine Identity Service". Beispiel:

C:\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /EXCLUDE "Personal vDisk","Machine Identity Service"

4. Führen Sie das Produktinstallationsprogramm auf der Hälfte der Controller aus. (Damit werden auch alle anderen Kernkomponenten auf diesen Servern aktualisiert.) Wenn Ihre Site beispielsweise vier Controller enthält, führen Sie das Installationsprogramm auf zwei Controllern aus.
   - Dadurch dass die Hälfte der Controller aktiv bleibt, können Benutzer auf die Site zugreifen. Die VDAs können sich bei den anderen Controllern registrieren. Zeitweise wird die Site möglicherweise mit reduzierter Kapazität ausgeführt, da weniger Controller verfügbar sind. Durch das Upgrade wird nur für das Einrichten neuer Clientverbindungen während der letzten Datenbankaktualisierungsschritte eine kurze Unterbrechung verursacht. Die aktualisierten Controller können Anforderungen erst verarbeiten, wenn die gesamte Site aktualisiert wurde.
   - Wenn die Site nur einen Controller hat, ist sie während des Upgrades nicht funktionsfähig.
5. Ist Studio auf einer anderen Maschine installiert als einer der im vorherigen Schritt aktualisierten Controller, führen Sie das Installationsprogramm auf der Maschine aus, auf der Studio installiert ist.
6. Führen Sie über die neu aktualisierte Studio-Version ein Upgrade der Sitedatenbank aus. Einzelheiten finden Sie unter Aktualisieren der Datenbank und Site.
7. Wählen Sie in der neu aktualisierten Studio-Version im Navigationsbereich **Citrix Studio** *Sitename* aus. Wählen Sie die Registerkarte **Häufige Aufgaben**. Wählen Sie **Upgrade der übrigen Delivery Controller durchführen**.
8. Nach Abschluss des Upgrades und Bestätigen von dessen Durchführung schließen Sie Studio und öffnen Sie es erneut.
9. Wählen Sie auf der Seite "Häufige Aufgaben" im Abschnitt "Sitekonfiguration" die Option **Registrierung durchführen** aus. Durch das Registrieren der Controller werden diese für die Site verfügbar.
10. Nach Auswahl von **Fertig stellen** im Anschluss an das Upgrade können Sie sich optional für die Teilnahme beim Programm zur Verbesserung der Benutzerfreundlichkeit von Citrix (Customer Experience Improvement Program, CEIP) registrieren, durch das anonyme Informationen zu Ihrer Bereitstellung gesammelt werden. Diese Informationen werden Verbesserung von Qualität, Zuverlässigkeit und Leistung des Produkts verwendet.
11. Nach dem Upgrade von Komponenten, Datenbank und Site führen Sie mit Studio folgende Arbeitsgänge durch:
    - Testen Sie die neu aktualisierte Site. Wählen Sie in Studio im Navigationsbereich **Citrix Studio** *Sitename*. Wählen Sie die Registerkarte **Häufige Aufgaben** und dann **Site testen**. Diese Tests werden automatisch nach dem Upgrade der Datenbank ausgeführt, Sie können sie jedoch jederzeit wiederholen.
    - Aktualisieren Sie alle Masterimages, die den aktualisierten VDA verwenden.
    - Aktualisieren Sie Maschinenkataloge und Bereitstellungsgruppen.

Aktualisieren von Sitedatenbank und Site

Nach dem Upgrade der Kernkomponenten und VDAs verwenden Sie die neu aktualisierte Studio-Version für ein automatisches oder manuelles Upgrade von Datenbank und Site.

- 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 im Artikel "Datenbanken".
- Hat der Benutzer diese Berechtigungen nicht, werden bei einem manuellen Datenbankupgrade Skripts generiert. Der Studio-Benutzer führt einige dieser Skripts über Studio aus, andere werden vom Datenbankadministrator mit einem Tool wie SQL Server Management Studio ausgeführt. Bei der manuellen Ausführung von SQL-Skripts sollten sie mit dem SQLCMD-Hilfsprogramm oder mit SQL Management Studio im SQLCMD-Modus ausgeführt werden. Andernfalls können Fehler aufgrund von Ungenauigkeiten auftreten.

Wichtig: Citrix empfiehlt dringend, die Datenbank vor dem Upgrade zu sichern (siehe CTX135207).

Während des Datenbankupgrades sind die Produktdienste deaktiviert. Während dieser Zeit können Controller keine neuen Verbindungen für die Site verhandeln. Planen Sie daher sorgfältig.

Nach dem Upgrade der Datenbank und der Aktivierung der Produktdienste testet Studio Umgebung und Konfiguration und generiert einen HTML-Bericht. Wenn Probleme identifiziert werden, können Sie die Datenbank aus dem Backup wiederherstellen. Wenn die Probleme beseitigt sind, können Sie die Datenbank erneut aktualisieren.

Automatisches Upgrade von Datenbank und Site Starten Sie die aktualisierte Studio-Version. Sobald Sie das automatische Upgrade der Site gestartet und bestätigt haben, dass Sie bereit sind, beginnt das Upgrade von Datenbank und Site.

Manuelles Upgrade von Datenbank und Site Bei diesem Vorgang werden Skripts generiert.

1. Starten Sie die aktualisierte Studio-Version. Sobald Sie das manuelle Upgrade der Site ausgewählt haben, prüft der Assistent die Kompatibilität des Lizenzservers und fordert eine Bestätigung an. Wenn Sie bestätigt haben, dass Sie die Datenbank gesichert haben, erstellt der Assistent Skripts und eine Checkliste der Upgradeschritte und zeigt diese an.
2. Führen Sie die folgenden Skripts in der angegebenen Reihenfolge aus:

Skript	Beschreibung
DisableServices.ps1	PowerShell-Skript, das vom Studio-Benutzer auf einem Controller ausgeführt werden muss und die Produktdienste deaktiviert
UpgradeSiteDatabase.sql	SQL-Skript, das vom Datenbankadministrator mit einem Tool wie SQL Server Management Studio auf dem Server mit der Sitedatenbank ausgeführt werden muss
UpgradeMonitorDatabase.sql	SQL-Skript, das vom Datenbankadministrator mit einem Tool wie SQL Server Management Studio auf dem Server mit der Überwachungsdatenbank ausgeführt werden muss
UpgradeLoggingDatabase.sql	SQL-Skript, das vom Datenbankadministrator mit einem Tool wie SQL Server Management Studio auf dem Server mit der Konfigurationsprotokollierungsdatenbank ausgeführt werden muss Führen Sie dieses Skript nur aus, wenn diese Datenbank geändert wird (z. B. nach dem Anwenden eines Hotfixes).
EnableServices.ps1	PowerShell-Skript, das vom Studio-Benutzer auf einem Controller ausgeführt werden muss und die Produktdienste aktiviert

3. Wenn Sie alle angezeigten Checklistenaufgaben erledigt haben, wählen Sie **Upgrade abschließen und zu 'Häufige Aufgaben' zurückkehren**.

Upgrade eines XenApp 6.5-Workers auf einen neuen VDA

Feb 29, 2016

Wenn Sie das Installationsprogramm des aktuellen Produkts auf einem XenApp 6.5-Workerserver ausführen, werden folgende Aktionen durchgeführt:

- Der Server wird aus der XenApp 6.5-Farm entfernt (für diese Aufgabe wird automatisch die Befehlszeile des XenApp 6.5-Installationsprogramms aufgerufen)
- Die XenApp 6.5-Software wird entfernt
- Ein neuer (XenApp 7.6 oder ein höheres unterstütztes Release) VDA für Windows-Serverbetriebssysteme wird installiert

Wenn Sie die grafische Benutzeroberfläche des Installationsprogramms verwenden, werden Sie durch denselben Assistenten geführt wie bei der Installation von VDAs für Windows-Serverbetriebssysteme in der neuen XenApp-Site. Auch die Befehlszeile verwendet die gleichen Befehle und Parameter, die Sie für die Installation anderer VDAs verwenden.

Hinweis: Sie können zwar einen XenApp 6.5-Workerserver aktualisieren, die Installation des aktuellen VDAs auf einer "sauberen" Maschine bietet jedoch mehr Sicherheit.

Durch die Installation der XenApp-Kernkomponenten und der anderen VDAs sind Sie wahrscheinlich bereits mit dem Installationsprogramm vertraut. Starten Sie das Installationsprogramm (Installieren über die grafische Oberfläche) oder führen Sie den Befehl auf dem XenApp 6.5-Workerserver aus (Installieren von VDA über die Befehlszeile).

Gut zu wissen:

- Diese Upgrade ist auf XenApp 6.5-Servern gültig, die im Servermodus "nur Sitzungsmodus" konfiguriert wurden (auch Nur-Sitzungsserver oder Workerserver genannt).
- Das Deinstallieren von XenApp 6.5 erfordert mehrere Serverneustarts. Wenn Sie die Befehlszeile verwenden, können Sie mit der Option /NOREBOOT diese automatische Aktion unterdrücken. Sie müssen den Server jedoch neu starten, damit die Deinstallation und die nachfolgende Neuinstallation ausgeführt werden können.
- Wenn während der XenApp-Deinstallation ein Fehler auftritt, prüfen Sie das in der Fehlermeldung angegebene Deinstallationsfehlerprotokoll. Deinstallationsprotokolldateien befinden sich im Ordner "%TEMP%\Citrix\XenDesktop Installation\XenApp 6.5 Uninstall Log Files\".
- Nach dem Upgrade überprüfen Sie IMA- und HDX-spezifische Systemeinstellungen und Registrierungseinträge. Einige Einstellungen gelten ggf. nicht mehr oder funktionieren anders.
- Nach dem Upgrade der XenApp 6.5-Workerserver erstellen Sie mit Studio in der neuen XenApp-Site Maschinenkataloge (oder bearbeiten Sie vorhandene Kataloge) für die aktualisierten Worker.
- Wenn Sie Richtlinien- und Anwendungseinstellungen von einem XenApp 6.5-Controllerserver migriert haben (siehe Migrieren von XenApp 6.x), weisen Sie die Bereitstellungsgruppen mit den migrierten veröffentlichten Anwendungen dem Maschinenkatalog zu, in dem diese Anwendungen in XenApp 6.5 gehostet wurden.

Problembehandlung

Symptome: Fehler beim Entfernen der XenApp 6.5-Software. Das Deinstallationsprotokoll enthält die Meldung:"Error 25703. An error occurred while plugging XML into Internet Information Server. Setup cannot copy files to your IIS Scripts directory. Please make sure that your IIS installation is correct."

- Ursache: Das Problem tritt auf Systemen auf, wenn (1) Sie während der XenApp 6.5-Erstinstallation angegeben haben, dass der Citrix XML-Dienst (CtxHttp.exe) keinen Port gemeinsam mit IIS verwenden soll, und (2) .NET Framework 3.5.1 installiert ist.
- Lösung:
  1. Entfernen Sie die Webserver (IIS)-Rolle mit dem Windows-Assistenten zum Entfernen von Rollen. (Sie können die Webserver (IIS)-Rolle später wieder installieren.)
  2. Starten Sie den Server neu.
  3. Deinstallieren Sie Folgendes mit der Windows-Funktion zum Installieren und Deinstallieren:
     1. Citrix XenApp 6.5
     2. Microsoft Visual C++ 2005 Redistributable (x64), Version 8.0.56336
  4. Starten Sie den Server neu.
  5. Installieren Sie den VDA für Windows-Serverbetriebssysteme mit dem XenApp-Installationsprogramm.

Migrieren von XenApp 6.x

Feb 29, 2016

Wichtig: Lesen Sie den gesamten Artikel, bevor Sie mit der Migration beginnen.

Das Tool für die Migration von XenApp 6.x (das Migrationstool) ist eine Sammlung von PowerShell-Skripts und Cmdlets, die Richtliniendaten und Farmdaten für XenApp 6.x (6.0 und 6.5) migrieren. Dazu führen Sie auf dem XenApp 6.x-Controllerserver Export-Cmdlets aus, die die Daten in XML-Dateien zusammenfassen. Anschließend führen Sie vom XenApp 7.6-Controller aus die Import-Cmdlets aus, die mit den beim Export gesammelten Daten Objekte erstellen.

Eine Videoübersicht über das Migrationstool ist hier verfügbar.

Unten ist die Abfolge des Migrationsvorgangs zusammengefasst. Details werden später erläutert.

1. Auf einem XenApp 6.0- oder 6.5-Controller:
   1. Importieren Sie die PowerShell-Exportmodule.
   2. Exportieren Sie mit den Export-Cmdlets die Richtlinien- und/oder Farmdaten in XML-Dateien.
2. Kopieren Sie die XML-Dateien (und den Ordner mit den Symbolen, wenn sie für den Export nicht in die XML-Dateien eingebettet werden) auf den XenApp 7.6-Controller.
3. Auf dem XenApp 7.6-Controller:
   1. Importieren Sie die PowerShell-Importmodule.
   2. Importieren Sie mit den Import-Cmdlets die Richtlinien- und/oder Farmdaten (Anwendungen), wobei Sie die XML-Dateien als Eingabe verwenden.
4. Führen Sie die nach der Migration erforderlichen Schritte aus.

Vor der eigentlichen Migration können Sie die XenApp 6.x-Einstellungen exportieren und eine Exportvorschau in der XenApp 7.6-Site ausführen. Die Vorschau lässt mögliche Schwachstellen erkennen, damit Sie die Probleme vor der eigentlichen Migration beheben können. Bei einer Vorschau kann sich beispielsweise herausstellen, dass eine Anwendung mit dem gleichen Namen bereits in der neuen XenApp 7.6-Site vorhanden ist. Sie können die bei der Vorschau erstellten Protokolldateien bei der Migration als Leitfaden verwenden.

Sofern nicht anders angegeben, bezieht sich der Begriff 6.x auf XenApp 6.0 oder 6.5.

Neue Features in diesem Release

Dieses Dezember 2014-Release (Version 20141125) enthält die folgenden Updates:

- Wenn bei der Verwendung des Migrationstools für eine XenApp 6.x-Farm Probleme auftreten, veröffentlichen Sie einen Bericht im Supportforum http://discussions.citrix.com/forum/1411-xenapp-7x/, sodass Citrix eine Untersuchung durchführen und das Tool verbessern kann.
- Neues Paketformat: Die Datei XAMigration.zip enthält jetzt zwei separate Pakete: ReadIMA.zip und ImportFMA.zip. Zum Exportieren von einem XenApp 6.x-Server benötigen Sie nur die ReadIMA.zip. Zum Importieren auf einen XenApp 7.6.x-Server benötigen Sie nur die ImportFMA.zip.
- Das Cmdlet "Export-XAFarm" unterstützt einen neuen Parameter (EmbedIconData), durch den das Kopieren der Symboldaten in verschiedene Dateien nicht mehr nötig ist.
- Das Cmdlet "Import-XAFarm" unterstützt drei neue Parameter:
  - MatchServer: Zum Importieren von Anwendungen von Servern, deren Namen mit einem Ausdruck übereinstimmen
  - NotMatchServer: Zum Importieren von Anwendungen von Servern, deren Namen nicht mit einem Ausdruck übereinstimmen
  - IncludeDisabledApps: Zum Importieren von deaktivierten Anwendungen
- Vorab gestartete Anwendungen werden nicht importiert.
- Das Cmdlet "Export-Policy" ist für XenDesktop 7.x.

Migrationstoolpaket

Das Migrationstool ist auf der Citrix Downloadsite unter XenApp 7.6 verfügbar. Die Datei XAMigration.zip enthält zwei separate, unabhängige Pakete:

- ReadIMA.zip: enthält die Dateien zum Exportieren von Daten aus der XenApp 6.x-Farm sowie freigegebene Module.

Modul bzw. Datei	Beschreibung
ExportPolicy.psm1	PowerShell-Skriptmodul zum Exportieren von XenApp 6.x-Richtlinien in eine XML-Datei.

Modul bzw. Datei	Beschreibung
ExportXAFarm.psm1	PowerShell-Skriptmodul zum Exportieren von XenApp 6.x-Farmeinstellungen in eine XML-Datei.
ExportPolicy.psd1	PowerShell-Manifestdatei für Skriptmodul ExportPolicy.psm1
ExportXAFarm.psd1	PowerShell-Manifestdatei für Skriptmodul ExportXAFarm.psm1
LogUtilities.psm1	Freigegebenes PowerShell-Skriptmodul mit Protokollierungsfunktionen
XmlUtilities.psd1	PowerShell-Manifestdatei für Skriptmodul XmlUtilities.psm1
XmlUtilities.psm1	Freigegebenes PowerShell-Skriptmodul mit XML-Funktionen

- ImportFMA.zip: enthält die Dateien zum Importieren von Daten aus der XenApp 7.6-Farm sowie freigegebene Module.

Modul bzw. Datei	Beschreibung
ImportPolicy.psm1	PowerShell-Skriptmodul zum Importieren von Richtlinien nach XenApp 7.6.
ImportXAFarm.psm1	PowerShell-Skriptmodul zum Importieren von Richtlinien nach XenApp 7.6.
ImportPolicy.psd1	PowerShell-Manifestdatei für Skriptmodul ImportPolicy.psm1
ImportXAFarm.psd1	PowerShell-Manifestdatei für Skriptmodul ImportXAFarm.psm1
PolicyData.xsd	XML-Schema für Richtliniendaten.
XAFarmData.xsd	XML-Schema für XenApp-Farmdaten.
LogUtilities.psm1	Freigegebenes PowerShell-Skriptmodul mit Protokollierungsfunktionen
XmlUtilities.psd1	PowerShell-Manifestdatei für Skriptmodul XmlUtilities.psm1
XmlUtilities.psm1	Freigegebenes PowerShell-Skriptmodul mit XML-Funktionen

Einschränkungen

- Nicht alle Richtlinieneinstellungen werden importiert; siehe Nicht importierte Richtlinieneinstellungen. Einstellungen, die nicht unterstützt werden, werden ignoriert und in der Protokolldatei angegeben.
- Zwar werden alle Anwendungsdetails während des Exportvorgangs in der XML-Ausgabedatei gesammelt, aber nur auf Servern installierte Anwendungen werden in die XenApp 7.6-Site importiert. Veröffentlichte Desktops, Inhalte und die meisten gestreamten Anwendungen werden nicht unterstützt (Informationen zu Ausnahmen finden Sie unter Schrittweise Anleitungen: Importieren von Daten) im Abschnitt zu den Import-XAFarm-Cmdlet-Parametern.
- Anwendungsserver werden nicht importiert.
- Viele Anwendungseigenschaften werden nicht importiert wegen der Unterschiede zwischen der XenApp 6.x Independent Management Architecture (IMA) und der XenApp 7.6 FlexCast Management Architecture (FMA). Weitere Informationen hierzu finden Sie unter Zuordnung von Anwendungseigenschaften.
- Während des Imports wird eine Bereitstellungsgruppe erstellt. Weitere Informationen zum Filtern des importierten Inhalts mit Parametern finden Sie unter Erweiterte Verwendung.
- Nur Citrix Richtlinieneinstellungen, die mit der AppCenter-Verwaltungskonsole erstellt wurden, werden importiert. Citrix Richtlinieneinstellungen, die mit Windows Gruppenrichtlinienobjekten erstellt wurden, werden nicht importiert.
- Die Migrationsskripts sind nur für die Migrationen von XenApp 6.x auf XenApp 7.6 vorgesehen.
- Mehr als fünffach verschachtelte Ordner werden von Studio nicht unterstützt und werden nicht importiert. Wenn die Ordnerstruktur Ihrer Anwendung Ordner mit mehr als fünf Ebenen von Unterordnern enthält, reduzieren Sie vor dem Importieren die Anzahl der verschachtelten Ordnerebenen.

Sicherheitsüberlegungen

Die durch die Exportskripts erstellten XML-Dateien können vertrauliche Informationen über Ihre Umgebung und Organisation enthalten, z. B. Benutzernamen, Servernamen und andere XenApp-Farm-, Anwendungs- und Richtlinienkonfigurationsdaten. Speichern und verwenden Sie diese Dateien in einer sicheren Umgebung.

Prüfen Sie die XML-Dateien sorgfältig, bevor Sie sie als Eingabe für den Import von Richtlinien und Anwendungen verwenden, um sicherzustellen, dass sie keine unbefugten Änderungen enthalten.

Richtlinienobjektzuweisungen (bisher "Richtlinienfilter") steuern die Anwendung von Richtlinien. Nach dem Importieren von Richtlinien prüfen Sie die Objektzuweisungen für jede Richtlinie sorgfältig, um sicherzustellen, dass durch den Import keine Sicherheitsrisiken entstanden sind. Nach dem Import können auf die Richtlinie verschiedene Gruppen von Benutzern, IP-Adressen oder Clientnamen angewendet werden. Die Einstellungen zum Zulassen und Verweigern haben möglicherweise nach dem Import eine andere Bedeutung.

Protokollierung und Fehlerbehandlung

Die Skripts sorgen für umfangreiche Protokollierung, wobei die Ausführung aller Cmdlets, informative Meldungen, die Ergebnisse der Cmdlet-Ausführung sowie Warnungen und Fehler aufgezeichnet werden.

- Die Verwendung der Citrix PowerShell-Cmdlets wird größtenteils protokolliert. Alle PowerShell-Cmdlets in den Importskripts, die neue Siteobjekte erstellen, werden protokolliert.
- Der Skriptausführungsverlauf wird protokolliert, einschließlich der Objekte, die verarbeitet werden.
- Große Aktionen, die sich auf den Flussstatus auswirken, werden protokolliert, einschließlich über die Befehlszeile geleitete Flüsse.
- Alle Meldungen, die auf der Konsole gedruckt werden, einschließlich Warnungen und Fehler werden protokolliert.
- Jede Zeile wird mit einem Zeitstempel versehen, der auf die Millisekunde genau ist.

Citrix empfiehlt, dass Sie beim Ausführen der Export- und Import-Cmdlets jeweils eine Protokolldatei angeben.

Wenn Sie keinen Protokolldateinamen angeben, wird die Protokolldatei im Basisordner des aktuellen Benutzers (in der PowerShell-Variable $HOME angegeben) gespeichert. Wenn dieser Ordner nicht vorhanden ist, wird die Protokolldatei im aktuellen Ausführungsordner des Skripts gespeichert. Der Standardname der Protokolldatei ist "XFarmYYYYMMDDHHmmSS-xxxxxx", wobei die letzten sechs Ziffern eine zufällige Zahl sind.

Standardmäßig werden die gesamten Fortschrittsinformationen angezeigt. Um die Anzeige zu unterdrücken, legen Sie den NoDetails-Parameter in den Export- und Import-Cmdlets fest.

Bei einem Fehler wird die Ausführung eines Skripts im Allgemeinen angehalten. Wenn der Fehler behoben ist, können Sie das Cmdlet noch einmal ausführen.

Bedingungen, die nicht als Fehler gelten, werden protokolliert und oft als Warnung gemeldet, während die Skriptausführung fortgesetzt wird. Beispielsweise werden nicht unterstützte Anwendungstypen als Warnung gemeldet und nicht importiert. Anwendungen, die bereits in der XenApp 7.6-Site vorhanden sind, werden nicht importiert. Richtlinieneinstellungen, die in XenApp 7.6 veraltet sind, werden nicht importiert.

Die Migrationsskripts verwenden viele PowerShell-Cmdlets und nicht alle möglichen Fehler werden protokolliert. Zusätzliche Protokollierungsfunktionen sind mit den PowerShell-Protokollierungsfeatures verfügbar. Beispielsweise wird alles, was auf dem Bildschirm gedruckt wird, in PowerShell-Aufzeichnungen protokolliert. Weitere Informationen finden Sie in der Hilfe zu den Cmdlets "Start-Transcript" und "Stop-Transcript".

Anforderungen, Vorbereitungen und Best Practices

Wichtig: Lesen Sie den gesamten Artikel, bevor Sie mit der Migration beginnen.
Sie sollten die grundlegenden PowerShell-Konzepte der Ausführungsrichtlinie, Module, Cmdlets und Skripts verstehen. Obwohl umfangreiche Erfahrung in der Erstellung von Skripts nicht erforderlich ist, sollten Sie die ausgeführten Cmdlets verstehen. Mit dem Cmdlet "Get-Help" können Sie sich die Hilfe zu jedem Migrations-Cmdlet ansehen, bevor Sie es ausführen. Beispiel:

```
Get-Help -full Import-XAFarm
```

Geben Sie eine Protokolldatei in der Befehlszeile an und überprüfen Sie die Protokolldatei jedes Mal, nachdem Sie ein Cmdlet ausgeführt haben. Wenn ein Skript fehlschlägt, identifizieren Sie den Fehler mit der Protokolldatei und beheben Sie ihn. Führen Sie dann das Cmdlet noch einmal aus.

Gut zu wissen:

- Zur Vereinfachung der Bereitstellung von Anwendungen während der Ausführung beider Bereitstellungen (vorhandene XenApp 6.x-Farm und neue XenApp 7.6-Site) können Sie beide Bereitstellungen in StoreFront oder dem Webinterface aggregieren. Weitere Informationen zu Ihrem StoreFront- oder Webinterface-Release finden Sie in der Dokumentation in den eDocs (Verwalten > Store erstellen).
- Für die Handhabung der Anwendungssymboldaten gibt es zwei Möglichkeiten:
  - Wenn Sie den Parameter "EmbedIconData" im Cmdlet "Export-XAFarm" angeben, werden exportierte Anwendungssymboldaten in der XML-Ausgabedatei eingebettet.
  - Wenn Sie den Parameter "EmbedIconData" im Cmdlet "Export-XAFarm" nicht angeben, werden exportierte Anwendungssymboldaten werden in einem Ordner gespeichert. Der Name des Ordners wird durch Anfügen der Zeichenfolge "-icons" an den Basisnamen der XML-Ausgabedatei erstellt. Wenn der Parameter "XmlOutputFile" beispielsweise "FarmData.xml" ist, wird der Ordner "FarmData-icons" zum Speichern der Anwendungssymbole erstellt.
    Die Symboldatendateien in diesem Ordner sind TXT-Dateien, die nach den Browsernamen der veröffentlichten Anwendungen benannt sind (die Dateien sind zwar TXT-Dateien, die gespeicherten Daten sind jedoch verschlüsselte binäre Symboldaten, die vom Importskript zum erneuten Erstellen des Anwendungssymbols gelesen werden können). Wenn der Symbolordner während des Importvorgangs nicht im selben Verzeichnis gefunden wird wie die

XML-Importdatei, werden allgemeine Symbole für die importierten Anwendungen verwendet.

- Die Namen der Skriptmodule, Manifestdateien, freigegebenen Module und Cmdlets sind ähnlich. Verwenden Sie die Tabulatortaste vorsichtig, damit es nicht zu Fehlern kommt. Beispiel: Export-XAFarm ist ein Cmdlet. ExportXAFarm.psd1 und ExportXAFarm.psm1 sind Dateien, die nicht ausgeführt werden können.
- In den nachfolgenden schrittweisen Anleitungen sind die meisten Parameterwerte für <string> mit Anführungszeichen versehen. Diese sind optional für Zeichenfolgen, die nur aus einem Wort bestehen.

Für den Export des XenApp 6.x-Servers gilt Folgendes:

- Der Export muss auf einem XenApp 6.x-Server ausgeführt werden, der mit dem Servermodus Controller- und Sitzungshostmodus (üblicherweise Controller genannt) konfiguriert wurde.
- Zum Ausführen der Export-Cmdlets müssen Sie XenApp-Administrator mit der Berechtigung zum Lesen von Objekten sein. Sie müssen auch über die erforderlichen Windows-Berechtigungen zum Ausführen von PowerShell-Skripts verfügen. Schrittweise Anleitungen finden Sie unten.
- Stellen Sie sicher, dass die XenApp 6.x-Farm funktionsfähig ist, bevor Sie mit dem Export beginnen. Sichern Sie die Farmdatenbank. Überprüfen Sie die Integrität der Farm mit dem Dienstprogramm "Citrix IMA Helper" (CTX133983): Führen Sie von der Registerkarte für den IMA Datastore aus einen Master Check aus (und lösen Sie alle ungültigen Einträge mit der Option "DSCheck" auf). Durch das Reparieren von Problemen vor der Migration werden Fehler beim Export vermieden. Wenn ein Server beispielsweise nicht richtig aus der Farm entfernt wird, bleiben seine Daten möglicherweise in der Datenbank vorhanden, was zu Fehlern bei den Cmdlets im Exportskript führen kann (z. B. Get-XAServer -ZoneName). Wenn die Cmdlets fehlschlagen, schlägt das Skript fehl.
- Sie können die Export-Cmdlets auf einer funktionierenden Farm ausführen, die aktive Benutzerverbindungen hat. Die Exportskripts lesen nur die statische Farmkonfiguration und die Richtliniendaten.

Für den Import auf den XenApp 7.6-Server gilt Folgendes:

- Sie können Daten in XenApp 7.6-Bereitstellungen (und höhere unterstützte Versionen) importieren. Sie müssen einen XenApp 7.6-Controller und Studio installieren und eine Site erstellen, bevor Sie die aus der XenApp 6.x-Farm exportierten Daten importieren. VDAs sind zwar zum Importieren von Einstellungen nicht erforderlich, sie gestatten jedoch das Verfügbarmachen von Anwendungsdateitypen.
- Zum Ausführen der Import-Cmdlets müssen Sie XenApp-Administrator mit der Berechtigung zum Lesen und Erstellen von Objekten sein. Ein Volladministrator hat diese Berechtigungen. Sie müssen auch über die erforderlichen Windows-Berechtigungen zum Ausführen von PowerShell-Skripts verfügen. Schrittweise Anleitungen finden Sie unten.
- Während eines Imports dürfen keine anderen Benutzerverbindungen aktiv sein. Die Importskripts erstellen viele neue Objekte und wenn andere Benutzer gleichzeitig Änderungen an der Konfiguration vornehmen, können Unterbrechungen auftreten.

Sie können Daten exportieren und dann den Parameter "-Preview " für das Import-Cmdlet verwenden, um eine Vorschau des Imports zu sehen, ohne dass tatsächliche Importvorgänge stattfinden. In den Protokollen wird genau angegeben, was während eines tatsächlichen Importvorgangs passieren würde. Wenn Fehler auftreten, können Sie diese beheben, bevor Sie einen tatsächlichen Import durchführen.

Schrittweise Anleitungen: Exportieren von Daten

Ein Video des Exports ist hier verfügbar.

Führen Sie die folgenden Schritte aus, um Daten aus einem XenApp 6.x-Controller in XML-Dateien zu exportieren.

1. Laden Sie das Paket mit dem Migrationstool (XAMigration.zip) von der Citrix Downloadsite herunter. Speichern Sie es der Einfachheit halber in einer Netzwerkfreigabe, damit von der XenApp 6.x-Farm und der XenApp 7.6-Site darauf zugegriffen werden kann. Entzippen Sie XAMigration.zip in der Netzwerkfreigabe. Sie sollten nun zwei ZIP-Dateien haben: ReadIMA.zip und ImportFMA.zip.
2. Melden Sie sich am XenApp 6.x-Controller als XenApp-Administrator mit mindestens Lesezugriff und Windows-Berechtigung zum Ausführen von PowerShell-Skripts an.
3. Kopieren Sie die Datei ReadIMA.zip von der Netzwerkfreigabe auf den XenApp 6.x-Controller. Entzippen und extrahieren Sie ReadIMA.zip auf dem Controller in einen Ordner (z. B.: C:\XAMigration).
4. Öffnen Sie eine PowerShell-Konsole und legen Sie das aktuelle Verzeichnis als Skriptspeicherort fest. Beispiel:
   cd C:\XAMigration
5. Überprüfen Sie die Skriptausführungsrichtlinie durch Ausführen von Get-ExecutionPolicy.
6. Legen Sie die Skriptausführungsrichtlinie mindestens auf "RemoteSigned" fest, damit die Skripts ausgeführt werden können. Beispiel:
   Set-ExecutionPolicy RemoteSigned
7. Importieren Sie die Moduldefinitionsdateien "ExportPolicy.psd1" und "ExportXAFarm.psd1":
   Import-Module .\ExportPolicy.psd1

   Import-Module .\ExportXAFarm.psd1

   Gut zu wissen:
   - Wenn Sie nur Richtliniendaten exportieren möchten, können Sie nur die Moduldefinitionsdatei "ExportPolicy.psd1" importieren. Genauso gilt, wenn Sie nur Farmdaten exportieren möchten, importieren Sie nur "ExportXAFarm.psd1".
   - Beim Importieren der Moduldefinitionsdateien werden auch die erforderlichen PowerShell-Snap-Ins hinzugefügt.
   - Importieren Sie nicht die Skriptdateien mit der Erweiterung .psm1.
8. Führen Sie zum Exportieren von Richtliniendaten das Cmdlet Export-Policy aus.

Parameter	Beschreibung
-XmlOutputFile "<string>.xml"	Name der XML-Ausgabedatei. Diese Datei enthält die exportierten Daten. Sie muss die Erweiterung .xml haben. Die Datei darf nicht vorhanden sein, aber wenn Sie den Pfad angeben, muss der übergeordnete Pfad vorhanden sein. Standardwert: Keiner. Dieser Parameter ist erforderlich.
-LogFile " <string>"	Name der Protokolldatei. Eine Erweiterung ist optional. Die Datei wird erstellt, wenn sie nicht vorhanden ist. Wenn die Datei vorhanden ist und der Parameter "NoClobber" ebenfalls angegeben ist, wird ein Fehler generiert, sonst wird der Inhalt der Datei überschrieben. Standardwert: siehe Protokollierung und Fehlerbehandlung
-NoLog	Keine Protokollausgabe erstellen. Dieser Parameter überschreibt den Parameter "LogFile", wenn er ebenfalls angegeben ist. Standardwert: False; Protokollausgabe wird erstellt
-NoClobber	Vorhandene Protokolldatei, die im Parameter "LogFile" angegeben wurde, nicht überschreiben. Wenn die Protokolldatei nicht vorhanden ist, hat dieser Parameter keine Auswirkung. Standardwert: False; eine vorhandene Protokolldatei wird überschrieben
-NoDetails	Keine ausführlichen Berichte zur Skriptausführung an die Konsole senden. Standardwert: False; ausführliche Berichte werden an der Konsole gesendet
-SuppressLogo	Meldung "XenApp 6.x to XenApp/XenDesktop 7.6 Migration Tool Version #yyyyMMdd-hhmm#" nicht auf Konsole drucken. Diese Meldung, in der die Skriptversion angegeben wird, kann bei der Problembehandlung hilfreich sein, daher empfiehlt Citrix, diesen Parameter wegzulassen. Standardwert: False; die Meldung wird auf der Konsole gedruckt

Beispiel: Das folgende Cmdlet exportiert Richtlinieninformationen in die XML-Datei "MyPolicies.xml". Der Vorgang wird in der Datei "MyPolicies.log" protokolliert.

```
Export-Policy -XmlOutputFile ".\MyPolicies.XML"  -LogFile ".\MyPolicies.Log"
```

9. Führen Sie zum Exportieren von Farmdaten das Cmdlet Export-XAFarm aus und geben Sie dabei eine Protokolldatei und eine XML-Datei an.

Parameter	Beschreibung
-XmlOutputFile "<string>.xml"	Name der XML-Ausgabedatei. Diese Datei enthält die exportierten Daten. Sie muss die Erweiterung .xml haben. Die Datei darf nicht vorhanden sein, aber wenn Sie den Pfad angeben, muss der übergeordnete Pfad vorhanden sein. Standardwert: Keiner. Dieser Parameter ist erforderlich.
-LogFile " <string>"	Name der Protokolldatei. Eine Erweiterung ist optional. Die Datei wird erstellt, wenn sie nicht vorhanden ist. Wenn die Datei vorhanden ist und der Parameter "NoClobber" ebenfalls angegeben ist, wird ein Fehler generiert, sonst wird der Inhalt der Datei überschrieben. Standardwert: siehe Protokollierung und Fehlerbehandlung
-NoLog	Keine Protokollausgabe erstellen. Dieser Parameter überschreibt den Parameter "LogFile", wenn er ebenfalls angegeben ist. Standardwert: False; Protokollausgabe wird erstellt
-NoClobber	Vorhandene Protokolldatei, die im Parameter "LogFile" angegeben wurde, nicht überschreiben. Wenn die Protokolldatei nicht vorhanden ist, hat dieser Parameter keine Auswirkung. Standardwert: False; eine vorhandene Protokolldatei wird überschrieben
-NoDetails	Keine ausführlichen Berichte zur Skriptausführung an die Konsole senden.

Parameter	Beschreibung
	Standardwert: False; ausführliche Berichte werden an der Konsole gesendet
-SuppressLogo	Meldung "XenApp 6.x to XenApp/XenDesktop 7.6 Migration Tool Version #yyyyMMdd-hhmm#" nicht auf Konsole drucken. Diese Meldung, in der die Skriptversion angegeben wird, kann bei der Problembehandlung hilfreich sein, daher empfiehlt Citrix, diesen Parameter wegzulassen. Standardwert: False; die Meldung wird auf der Konsole gedruckt
-IgnoreAdmins	Administratorinformationen nicht exportieren. Informationen zur Verwendung finden Sie unter Erweiterte Verwendung. Standardwert: False; Administratorinformationen werden exportiert
-IgnoreApps	Anwendungsinformationen nicht exportieren. Informationen zur Verwendung finden Sie unter Erweiterte Verwendung. Standardwert: False; Anwendungsinformationen werden exportiert
-IgnoreServers	Serverinformationen nicht exportieren. Standardwert: False; Serverinformationen werden exportiert
-IgnoreZones	Zoneninformationen nicht exportieren. Standard: False; Zoneninformationen werden exportiert
-IgnoreOthers	Daten wie Folgende nicht exportieren: Konfigurationsprotokollierung, Lastauswertungsprogramme, Lastausgleichsrichtlinien, Druckertreiber und Workergruppen. Standardwert: False; andere Informationen werden exportiert Hinweis: Der Schalter -IgnoreOthers ermöglicht das Durchführen eines Exports, wenn ein Fehler vorliegt, der keine Auswirkungen auf die exportierten oder importierten Daten hat.
-AppLimit <integer>	Anzahl der Anwendungen, die exportiert werden. Informationen zur Verwendung finden Sie unter Erweiterte Verwendung. Standardwert: Alle Anwendungen werden exportiert
-EmbedIconData	Anwendungssymboldaten in die gleiche XML-Datei einbetten wie die anderen Objekte. Standard: Symbole werden separat gespeichert. Weitere Informationen finden Sie unter Anforderungen, Vorbereitungen und Best Practices.
-SkipApps <integer>	Anzahl der Anwendungen, die übersprungen werden. Informationen zur Verwendung finden Sie unter Erweiterte Verwendung. Standardwert: Keine Anwendungen werden übersprungen

Beispiel: Das folgende Cmdlet exportiert Farminformationen in die XML-Datei "MyFarm.xml". Der Vorgang wird in der Datei "MyFarm.log" protokolliert. Ein Ordner mit dem Namen "MyFarm-icons" wird zum Speichern der Datendateien für die Anwendungssymbole erstellt. Dieser Ordner ist am gleichen Speicherort wie "MyFarm.xml".

```
Export-XAFarm -XmlOutputFile ".\MyFarm.XML"  -LogFile".\MyFarm.Log"
```

Nachdem die Ausführung der Exportskripts abgeschlossen ist, enthalten die in den Befehlszeilen angegebenen XML-Dateien die Richtliniendaten und die XenApp-Farmdaten. Die Anwendungssymboldateien enthalten die Symboldatendateien und die Protokolldatei gibt an, was sich beim Export ereignet hat.

Schrittweise Anleitungen: Importieren von Daten

Ein Video des Imports ist hier verfügbar.

Sie können eine Importvorschau ausführen (indem Sie das Cmdlet "Import-Policy" oder "Import-XAFarm" mit dem Preview-Parameter ausführen) und die Protokolldateien überprüfen, bevor Sie einen tatsächlichen Import ausführen.

Führen Sie die folgenden Schritte aus, um Daten mit den beim Export erstellten XML-Dateien in eine XenApp 7.6-Site zu importieren.

1. Melden Sie sich als Administrator mit Lese- und Schreibrechten und Windows-Berechtigung zum Ausführen von PowerShell-Skripts am XenApp 7.6-Controller an.
2. Wenn Sie das Paket mit dem Migrationstool (XAMigration) noch nicht in der Netzwerkfreigabe entzippt haben, führen Sie den Vorgang nun aus. Kopieren Sie die Datei ImportFMA.zip von der Netzwerkfreigabe auf den XenApp 7.6-Controller. Entzippen und extrahieren Sie ImportFMA.zip auf dem Controller in einen Ordner (z. B.: C:\XAMigration).
3. Kopieren Sie die XML-Dateien (die während des Exports erstellten Ausgabedateien) vom XenApp 6.x-Controller in den Speicherort auf dem XenApp 7.6-Controller, wo Sie die Dateien aus ImportFMA.zip extrahiert haben.
   Wenn Sie die Anwendungssymboldaten beim Ausführen des Cmdlets "Export-XAFarm" nicht in die XML-Ausgabedatei eingebettet haben, kopieren Sie den Ordner mit den Symboldaten in den gleichen Speicherort auf dem XenApp 7.6-Controller, in den Sie die XML-Ausgabedateien kopiert haben und in dem sich die extrahierten Dateien aus ImportFMA.zip befinden.
4. Öffnen Sie eine PowerShell-Konsole und legen Sie das aktuelle Verzeichnis als Skriptspeicherort fest.
   cd C:\XAMigration
5. Überprüfen Sie die Skriptausführungsrichtlinie durch Ausführen von Get-ExecutionPolicy.
6. Legen Sie die Skriptausführungsrichtlinie mindestens auf "RemoteSigned" fest, damit die Skripts ausgeführt werden können. Beispiel:
   Set-ExecutionPolicy RemoteSigned
7. Importieren Sie die PowerShell-Moduldefinitionsdateien "ImportPolicy.psd1" und "ImportXAFarm.psd1":
   Import-Module .\ImportPolicy.psd1

   Import-Module .\ImportXAFarm.psd1

   Gut zu wissen:
   - Wenn Sie nur Richtliniendaten importieren möchten, können Sie nur die Moduldefinitionsdatei "ImportPolicy.psd1" importieren. Genauso gilt, wenn Sie nur Farmdaten importieren möchten, importieren Sie nur "ImportXAFarm.psd1".
   - Beim Importieren der Moduldefinitionsdateien werden auch die erforderlichen PowerShell-Snap-Ins hinzugefügt.
   - Importieren Sie nicht die Skriptdateien mit der Erweiterung .psm1.
8. Wenn Sie Richtliniendaten importieren, führen Sie das Cmdlet Import-Policy aus. Geben Sie dabei die XML-Datei mit den exportierten Richtliniendaten an.

Parameter	Beschreibung
-XmlInputFile "<string>.xml"	Name der XML-Eingabedatei. Diese Datei enthält Daten, die mit dem Cmdlet "Export-Policy" gesammelt wurden. Sie muss die Erweiterung .xml haben. Standardwert: Keiner. Dieser Parameter ist erforderlich.
-XsdFile "<string>"	Name der XSD-Datei. Mit dieser Datei überprüfen die Importskripts die Syntax der XML-Eingabedatei. Informationen zur Verwendung finden Sie unter Erweiterte Verwendung. Standardwert: PolicyData.XSD
-LogFile "<string>"	Name der Protokolldatei. Wenn Sie Exportprotokolldateien auf diesen Server kopiert haben, sollten Sie einen anderen Namen für die Protokolldatei des Import-Cmdlets verwenden. Standardwert: siehe Protokollierung und Fehlerbehandlung
-NoLog	Keine Protokollausgabe erstellen. Dieser Parameter überschreibt den Parameter "LogFile", wenn er ebenfalls angegeben ist. Standardwert: False; Protokollausgabe wird erstellt
-NoClobber	Vorhandene Protokolldatei, die im Parameter "LogFile" angegeben wurde, nicht überschreiben. Wenn die Protokolldatei nicht vorhanden ist, hat dieser Parameter keine Auswirkung. Standardwert: False; eine vorhandene Protokolldatei wird überschrieben
-NoDetails	Keine ausführlichen Berichte zur Skriptausführung an die Konsole senden. Standardwert: False; ausführliche Berichte werden an der Konsole gesendet
-SuppressLogo	Meldung "XenApp 6.x to XenApp/XenDesktop 7.6 Migration Tool Version #yyyyMMdd-hhmm#" nicht auf Konsole drucken. Diese Meldung, in der die Skriptversion angegeben wird, kann bei der Problembehandlung hilfreich sein, daher empfiehlt Citrix, diesen Parameter wegzulassen.

Parameter	Beschreibung
	Standardwert: False; die Meldung wird auf der Konsole gedruckt
-Preview	Führen Sie eine Importvorschau aus: Daten werden aus der XML-Eingabedatei gelesen, aber es werden keine Objekte in die Site importiert. In der Protokolldatei und Konsole wird protokolliert, was während der Importvorschau vorgegangen ist. Eine Vorschau zeigt Administratoren, was während eines echten Imports passieren würde. Standardwert: False; ein echter Import wird ausgeführt

Beispiel: Mit dem folgenden Cmdlet werden Richtliniendaten aus der XML-Datei "MyPolicies.xml" importiert. Der Vorgang wird in der Datei "MyPolicies.log" protokolliert.

```
Import-Policy -XmlInputFile ".\MyPolicies.XML"  -LogFile ".\MyPolicies.Log"
```

9. Wenn Sie Anwendungen importieren, führen Sie das Cmdlet Import-XAFarm aus. Geben Sie dabei eine Protokolldatei und die XML-Datei mit den exportierten Farmdaten an.

Parameter	Beschreibung
-XmlInputFile "<string>.xml"	Name der XML-Eingabedatei. Diese Datei enthält Daten, die mit dem Cmdlet "Export-XAFarm" gesammelt wurden. Sie muss die Erweiterung .xml haben. Standardwert: Keiner. Dieser Parameter ist erforderlich.
-XsdFile "<string>"	Name der XSD-Datei. Mit dieser Datei überprüfen die Importskripts die Syntax der XML-Eingabedatei. Informationen zur Verwendung finden Sie unter Erweiterte Verwendung. Standardwert: XAFarmData.XSD
-LogFile "<string>"	Name der Protokolldatei. Wenn Sie Exportprotokolldateien auf diesen Server kopiert haben, sollten Sie einen anderen Namen für die Protokolldatei des Import-Cmdlets verwenden. Standardwert: siehe Protokollierung und Fehlerbehandlung
-NoLog	Keine Protokollausgabe erstellen. Dieser Parameter überschreibt den Parameter "LogFile", wenn er ebenfalls angegeben ist. Standardwert: False; Protokollausgabe wird erstellt
-NoClobber	Vorhandene Protokolldatei, die im Parameter "LogFile" angegeben wurde, nicht überschreiben. Wenn die Protokolldatei nicht vorhanden ist, hat dieser Parameter keine Auswirkung. Standardwert: False; eine vorhandene Protokolldatei wird überschrieben
-NoDetails	Keine ausführlichen Berichte zur Skriptausführung an die Konsole senden. Standardwert: False; ausführliche Berichte werden an der Konsole gesendet
-SuppressLogo	Meldung "XenApp 6.x to XenApp/XenDesktop 7.6 Migration Tool Version #yyyyMMdd-hhmm#" nicht auf Konsole drucken. Diese Meldung, in der die Skriptversion angegeben wird, kann bei der Problembehandlung hilfreich sein, daher empfiehlt Citrix, diesen Parameter wegzulassen. Standardwert: False; die Meldung wird auf der Konsole gedruckt
-Preview	Führen Sie eine Importvorschau aus: Daten werden aus der XML-Eingabedatei gelesen, aber es werden keine Objekte in die Site importiert. In der Protokolldatei und Konsole wird protokolliert, was während der Importvorschau vorgegangen ist. Eine Vorschau zeigt Administratoren, was während eines echten Imports passieren würde. Standardwert: False; ein echter Import wird ausgeführt
-DeliveryGroupName "<string>"	Bereitstellungsgruppenname für alle importierten Anwendungen. Informationen zur Verwendung finden Sie unter Erweiterte Verwendung.

Parameter	Beschreibung
	Standardwert: "<xenapp-farm-name> - Delivery Group"
-MatchFolder "<string>"	Import von Anwendungen in Ordnern, deren Namen mit der Zeichenfolge (String) übereinstimmen. Informationen zur Verwendung finden Sie unter Erweiterte Verwendung. Standardwert: Keine Übereinstimmung
-NotMatchFolder "<string>"	Import von Anwendungen in Ordnern, deren Namen mit der Zeichenfolge (String) nicht übereinstimmen. Informationen zur Verwendung finden Sie unter Erweiterte Verwendung. Standardwert: Keine Übereinstimmung
-MatchServer "<string>"	Import von Anwendungen auf Servern, deren Namen mit der Zeichenfolge (String) übereinstimmen. Informationen zur Verwendung finden Sie unter Erweiterte Verwendung.
-NotMatchServer "<string>"	Import von Anwendungen auf Servern, deren Namen nicht mit der Zeichenfolge (String) übereinstimmen. Informationen zur Verwendung finden Sie unter Erweiterte Verwendung. Standardwert: Keine Übereinstimmung
-MatchWorkerGroup "<string>"	Import von Anwendungen, die für Workergruppen veröffentlicht wurden und deren Namen mit der Zeichenfolge (String) übereinstimmen. Informationen zur Verwendung finden Sie unter Erweiterte Verwendung. Standardwert: Keine Übereinstimmung
-NotMatchWorkerGroup "<string>"	Import von Anwendungen, die für Workergruppen veröffentlicht wurden und deren Namen nicht mit der Zeichenfolge (String) übereinstimmen. Informationen zur Verwendung finden Sie unter Erweiterte Verwendung. Standardwert: Keine Übereinstimmung
-MatchAccount "<string>"	Import von Anwendungen, die für Benutzerkonten veröffentlicht wurden und deren Namen mit der Zeichenfolge (String) übereinstimmen. Informationen zur Verwendung finden Sie unter Erweiterte Verwendung. Standardwert: Keine Übereinstimmung
-NotMatchAccount "<string>"	Import von Anwendungen, die für Benutzerkonten veröffentlicht wurden und deren Namen nicht mit der Zeichenfolge (String) übereinstimmen. Informationen zur Verwendung finden Sie unter Erweiterte Verwendung. Standardwert: Keine Übereinstimmung
-IncludeStreamedApps	Import von Anwendungen des Typs "StreamedToClientOrServerInstalled". (Keine anderen gestreamten Anwendungen werden importiert.) Standard: Gestreamte Anwendungen werden nicht importiert
-IncludeDisabledApps	Import von Anwendungen, die als deaktiviert markiert sind. Standard: Deaktivierte Anwendungen werden nicht importiert

Beispiel: Das folgende Cmdlet importiert Anwendungen aus der XML-Datei "MyFarm.xml". Der Vorgang wird in der Datei "MyFarm.log" protokolliert.

```
Import-XAFarm -XmlInputFile ".\MyFarm.XML"  -LogFile ".\MyFarm.Log"
```

10. Führen Sie nach dem Abschluss des Imports die nach der Migration erforderlichen Aufgaben durch.

Aufgaben nach der Migration

Nach dem erfolgreichen Import von XenApp 6.x-Richtlinien und Farmeinstellungen in eine XenApp 7.6-Site stellen Sie mit den folgenden Richtlinien sicher, dass die Daten richtig importiert wurden.

- **Richtlinien und Richtlinieneinstellungen**

Das Importieren von Richtlinien ist im Prinzip ein Kopiervorgang mit Ausnahme von veralteten Einstellungen und Richtlinien, die nicht importiert werden. Mit der Prüfung nach der Migration werden die beiden Seiten verglichen.

1. In der Protokolldatei werden alle importierten und ignorierten Richtlinien und Einstellungen aufgeführt. Überprüfen Sie zuerst die Protokolldatei und identifizieren Sie die Einstellungen und Richtlinien, die nicht importiert wurden.
2. Vergleichen Sie die XenApp 6.x-Richtlinien mit den nach XenApp 7.6 importierten Richtlinien. Die Werte der Einstellungen sollten gleich bleiben (außer bei veralteten Richtlinieneinstellungen, siehe nächster Schritt).
   - Bei einer kleinen Anzahl von Richtlinien können Sie einen visuellen Vergleich der Richtlinien im XenApp 6.x AppCenter und in XenApp 7.6 Studio durchführen.
   - Bei einer großen Anzahl von Richtlinien ist ein visueller Vergleich u. U. nicht möglich. Verwenden Sie in solchen Fällen das Export-Cmdlet (Export-Policy), um die XenApp 7.6-Richtlinien in eine andere XML-Datei zu exportieren. Vergleichen Sie dann mit einem Textvergleichsprogramm (z. B. Windiff) die Daten der Datei mit den Daten in der XML-Datei, die zum Richtlinienexport aus XenApp 6.x verwendet wurde.
3. Der Abschnitt Nicht importierte Richtlinieneinstellungen enthält Informationen dazu, was sich beim Import geändert haben könnte. Wenn eine XenApp 6.x-Richtlinie nur veralteten Einstellungen enthält, wird die gesamte Richtlinie nicht importiert. Beispiel: Wenn eine XenApp 6.x-Richtlinie nur HMR-Testeinstellungen enthält, wird die Richtlinie vollständig ignoriert, da es keine entsprechende Einstellung in XenApp 7.6 gibt.
   Einige XenApp 6.x-Richtlinieneinstellungen werden nicht mehr unterstützt, aber vergleichbare Funktionen wurden in XenApp 7.6 implementiert. In XenApp 7.6 können Sie beispielsweise einen Neustartzeitplan für Serverbetriebssystemmaschinen konfigurieren, indem Sie eine Bereitstellungsgruppe bearbeiten. Diese Funktionalität wurde zuvor über Richtlinieneinstellungen implementiert.
4. Lesen Sie sich noch einmal durch, wie Filter in einer XenApp 7.6-Site im Gegensatz zu XenApp 6.x angewendet werden. Durch die wesentlichen Unterschiede zwischen der XenApp 6.x-Farm und der XenApp 7.6-Site kann sich die Wirkung von Filtern ändern.

- **Filter**

Überprüfen Sie sorgfältig die Filter für die einzelnen Richtlinien. Damit sie in XenApp 7.6 weiterhin genauso funktionieren wie in XenApp 6.x, sind u. U. Änderungen erforderlich.

Filter	Überlegungen
Zugriffssteuerung	Die Zugriffssteuerung sollte die gleichen Werte wie die ursprünglichen XenApp 6.x-Filter enthalten und ohne Änderungen funktionieren.
Citrix CloudBridge	Ein einfacher Boolescher Wert, der ohne Änderungen funktionieren sollte.
Client-IP-Adresse	Listet Client-IP-Adressbereiche auf. Jeder Bereich ist entweder zugelassen oder verweigert. Das Importskript behält die Werte bei, aber Änderungen können erforderlich sein, wenn sich andere Clients mit den XenApp 7.6-VDA-Maschinen verbinden.
Clientname	Ähnlich wie beim Client-IP-Adressenfilter behält das Importskript die Werte bei. Es können jedoch Änderungen erforderlich sein, wenn sich andere Clients mit den XenApp 7.6-VDA-Maschinen verbinden.
Organisationseinheit	Die Werte werden beibehalten, wenn die Organisationseinheiten beim Import aufgelöst werden können. Überprüfen Sie diesen Filter sorgfältig, besonders wenn die XenApp 6.x- und XenApp 7.6-Maschinen in unterschiedlichen Domänen sind. Wenn Sie die Filterwerte nicht richtig konfigurieren, wird die Richtlinie möglicherweise auf einen falschen Satz Organisationseinheiten angewendet. Die Organisationseinheiten werden nur durch Namen dargestellt, daher ist es möglich, dass eine Organisationseinheit zu einer Organisationseinheit aufgelöst wird, die andere Mitglieder enthält als die Organisationseinheit in der XenApp 6.x-Domäne. Selbst wenn einige Werte des Organisationseinheitsfilters beibehalten werden, prüfen Sie die Werte sorgfältig.
Benutzer oder Gruppe	Die Werte werden beibehalten, wenn die Konten beim Import aufgelöst werden können. Ähnlich wie Organisationseinheiten werden die Konten nur nach Namen aufgelöst. Wenn die XenApp 7.6-Site eine Domäne mit den gleichen Domänen- und Benutzernamen enthält, wobei es sich aber tatsächlich um zwei verschiedene Domänen und Benutzer handelt, entsprechen die aufgelösten Konten möglicherweise nicht den Domänenbenutzern in XenApp 6.x. Wenn Sie die Filterwerte nicht richtig überprüfen und ändern, kann es zur falschen Anwendung von Richtlinien kommen.
Workergruppe	Workergruppen werden in XenApp 7.6 nicht unterstützt. Verwenden Sie die Bereitstellungsgruppe, den Bereitstellungsgruppentyp und die Tagfilter, die in XenApp 7.6 unterstützt werden (nicht in XenApp 6.x). • Bereitstellungsgruppe: Ermöglicht die Anwendung von Richtlinien basierend auf Bereitstellungsgruppen. Jeder Filtereintrag gibt eine Bereitstellungsgruppe an und kann zugelassen oder verweigert werden. • Bereitstellungsgruppentyp: Ermöglicht die Anwendung von Richtlinien basierend auf Bereitstellungsgruppentypen. Jeder Filter

Filter	Überlegungen
	gibt einen Bereitstellungsgruppentyp an und kann zugelassen oder verweigert werden. • Tag: Gibt die Richtlinienanwendung basierend auf Tags an, die für VDA-Maschinen erstellt wurden. Jedes Tag kann zugelassen oder verweigert werden.

Filter, die Domänenbenutzeränderungen umfassen, müssen besonders sorgfältig überprüft werden, wenn die XenApp 6.x-Farm in einer anderen Domäne ist als die XenApp 7.6-Site. Da das Importskript nur die Zeichenfolgen von Domänen- und Benutzernamen verwendet, um Benutzer in der neuen Domäne aufzulösen, werden einige Konten möglicherweise aufgelöst und andere nicht. Obwohl nicht sehr wahrscheinlich ist, dass verschiedene Domänen und Benutzer den gleichen Namen haben, sollten Sie unbedingt die Filter sorgfältig überprüfen, um sicherzustellen, dass sie korrekte Werte enthalten.

- **Anwendungen**
  Die Skripts zum Import von Anwendungen importieren nicht nur Anwendungen, sondern sie erstellen auch Objekte, z. B. Bereitstellungsgruppen. Wenn der Anwendungsimport mehrere Durchläufe umfasst, können sich die Originalhierarchien der Anwendungsordner erheblich ändern.
  1. Lesen Sie als Erstes die Migrationsprotokolldateien, die Informationen dazu enthalten, welche Anwendungen importiert oder ignoriert wurden und welche Cmdlets zum Erstellen der Anwendungen verwendet wurden.
  2. Für jede Anwendung gilt Folgendes:
     - Sehen Sie sich das Protokoll an und prüfen Sie, ob die grundlegenden Eigenschaften beim Importieren beibehalten wurden. Bestimmen Sie mit den Informationen unter Zuordnung von Anwendungseigenschaften, welche Eigenschaften ohne Änderungen importiert, nicht importiert oder mit den XenApp 6.x-Anwendungsdaten initialisiert wurden.
     - Überprüfen Sie die Benutzerliste. Das Importskript importiert automatisch die explizite Liste der Benutzer in die Liste "Sichtbarkeit beschränken" der Anwendung in XenApp 7.6. Stellen Sie sicher, dass die Liste unverändert ist.
  3. Anwendungsserver werden nicht importiert. Dies bedeutet, dass auf keine der importierten Anwendungen zugegriffen werden kann. Den Bereitstellungsgruppen, die diese Anwendungen enthalten, müssen Maschinenkataloge mit den Maschinen zugewiesen werden, auf denen die ausführbaren Images der veröffentlichten Anwendungen sind. Für jede Anwendung gilt Folgendes:
     - Stellen Sie sicher, dass der Name der ausführbaren Datei und das Arbeitsverzeichnis auf eine ausführbare Datei verweisen, die auf den Maschinen vorhanden ist, die der Bereitstellungsgruppe (über die Maschinenkataloge) zugewiesen sind.
     - Überprüfen Sie einen Befehlszeilenparameter (dies kann ein beliebiges Objekt sein, z. B. Dateiname, Umgebungsvariable oder der Name einer ausführbaren Datei). Stellen Sie sicher, dass der Parameter für alle Maschinen in den Maschinenkatalogen, die der Bereitstellungsgruppe zugewiesen sind, gültig ist.
- **Protokolldateien**
  Die Protokolldateien sind die wichtigsten Referenzressourcen beim Import und Export. Aus diesem Grund werden bestehende Protokolldateien standardmäßig nicht überschrieben und Standardprotokolldateien haben eindeutige Namen.

  Im Abschnitt "Protokollierung und Fehlerbehandlung" wurde bereits erwähnt, dass die Ausgabe und die Protokolldatei, die Sie erhalten, wenn Sie die verfügbaren zusätzlichen Protokollierungsfunktionen für die PowerShell-Cmdlets "Start-Transcript" und "Stop-Transcript" verwenden (sie protokollieren alles, was in die Konsole eingegeben und gedruckt wird), eine vollständige Referenz der Import- und Exportaktivitäten bieten.

  Mit den Zeitstempeln in den Protokolldateien können Sie bestimmte Probleme diagnostizieren. Wenn beispielsweise ein Export oder Import sehr lange gedauert hat, können Sie feststellen, ob eine fehlerhafte Datenbankverbindung oder das Auflösen von Benutzerkonten viel Zeit in Anspruch genommen haben.

  Aus den in den Protokolldateien aufgezeichneten Befehlen lässt sich auch ermitteln, wie manche Objekte gelesen oder erstellt werden. Beispielsweise werden zum Erstellen einer Bereitstellungsgruppe mehrere Befehle ausgeführt, und zwar nicht nur, um das Bereitstellungsgruppenobjekt selbst zu erstellen, sondern auch andere Objekte, wie die Zugriffsrichtlinienregeln, mit denen Anwendungsobjekte Bereitstellungsgruppen zugewiesen werden.

  Mit der Protokolldatei kann auch ein fehlgeschlagener Export oder Import diagnostiziert werden. Normalerweise ist in den letzten Zeilen der Protokolldatei angegeben, was den Fehler verursacht hat. Die Fehlermeldung ist ebenfalls in der Protokolldatei gespeichert. Mit der Protokolldatei und der XML-Datei zusammen können Sie bestimmen, welches Objekt an dem Fehler beteiligt war.

Nach der Überprüfung und dem Test der Migration haben Sie folgende Möglichkeiten:

1. Upgrade der XenApp 6.5-Workerserver auf aktuelle Virtual Delivery Agents (VDAs) durch Ausführen des Installers für 7.6 auf den Servern. Der Installer entfernt die XenApp 6.5-Software und installiert dann automatisch einen aktuellen VDA. Anweisungen finden Sie unter Upgrade eines XenApp 6.5-Workers auf einen neuen VDA für Windows-Serverbetriebssysteme.
   Bei XenApp 6.0-Workerservern müssen Sie die XenApp 6.0-Software manuell vom Server deinstallieren. Danach können Sie mit dem Installer für 7.6 den aktuellen VDA installieren. Sie können mit dem Installer für 7.6 nicht automatisch die XenApp 6.0-Software entfernen.
2. Erstellen von Maschinenkatalogen (oder Bearbeiten von vorhandenen Katalogen) für die aktualisierten Worker in der neuen XenApp-Site mit Studio.
3. Hinzufügen der aktualisierten Maschinen aus dem Maschinenkatalog zu den Bereitstellungsgruppen, die die auf den VDAs für Windows-Serverbetriebssysteme installierten Anwendungen enthalten.

Erweiterte Verwendung

Standardmäßig exportiert das Cmdlet "Export-Policy" alle Richtliniendaten in eine XML-Datei. Parallel dazu exportiert das Cmdlet "Export-XAFarm" alle Farmdaten in eine XML-Datei. Sie können mit Befehlszeilenparametern genauer steuern, was importiert und exportiert wird.

- **Teilweiser Export von Anwendungen**: Wenn Sie eine große Anzahl von Anwendungen haben und steuern möchten, wie viele in die XML-Datei exportiert werden, verwenden Sie die folgenden Parameter:
  - AppLimit: Gibt die Anzahl der zu exportierenden Anwendungen an.
  - SkipApps: Gibt die Anzahl der zu überspringenden Anwendungen an, bevor Anwendungen exportiert werden.

  Sie können beide Parameter verwenden, um große Mengen von Anwendungen in praktischen Segmenten zu exportieren. Beispiel: Wenn Sie das erste Mal "Export-XAFarm" ausführen, möchten Sie nur die ersten 200 Anwendungen exportieren und geben daher den Wert im Parameter "AppLimit" an.
  Export-XAFarm -XmlOutputFile "Apps1-200.xml" -AppLimit "200"
  Beim nächsten Mal, wenn Sie "Export-XAFarm" ausführen, sollen die nächsten 100 Anwendungen exportiert werden. Sie verwenden den Parameter "SkipApps", um die bereits exportierten Anwendungen (die ersten 200) zu ignorieren, und exportieren mit dem Parameter "AppLimit" die nächsten 100 Anwendungen.
  Export-XAFarm -XmlOutputFile "Apps201-300.xml" -AppLimit "100" -SkipApps "200"
- **Bestimmte Objekte nicht exportieren**: Einige Objekte brauchen nicht exportiert zu werden und können ignoriert werden. Dazu zählen besonders Objekte, die nicht importiert werden. Weitere Informationen hierzu finden Sie unter Nicht importierte Richtlinieneinstellungen und Zuordnung von Anwendungseigenschaften. Mit den folgenden Parametern können Sie den Export unnötiger Objekte verhindern:
  - IgnoreAdmins: Administratorobjekte werden nicht exportiert
  - IgnoreServers: Serverobjekte werden nicht exportiert
  - IgnoreZones: Zonenobjekte werden nicht exportiert
  - IgnoreOthers: Konfigurationsprotokollierungs-, Lastauswertungsprogramm-, Lastausgleichsrichtlinien-, Druckertreiber- und Workergruppenobjekte werden nicht exportiert
  - IgnoreApps: Anwendungen werden nicht exportiert. Hiermit können Sie andere Daten in eine XML-Ausgabedatei exportieren und dann den Export erneut ausführen, um die Anwendungen in eine andere XML-Ausgabedatei zu exportieren.

  Sie können mit diesen Parametern auch Probleme umgehen, die zum Fehlschlagen des Exports führen können. Wenn Sie beispielsweise einen fehlerhaften Server in einer Zone haben, schlägt der Export der Zone möglicherweise fehl. Wenn Sie den Parameter "IgnoreZones" verwenden, wird der Exportvorgang mit anderen Objekten fortgesetzt.

- **Bereitstellungsgruppennamen**: Wenn nicht alle Anwendungen in einer Bereitstellungsgruppe platziert werden sollen (z. B. weil verschiedene Benutzergruppen auf sie zugreifen und sie auf verschiedenen Servern veröffentlicht werden), führen Sie "Import-XAFarm" mehrmals aus und geben Sie dabei jedes Mal unterschiedliche Anwendungen und eine andere Bereitstellungsgruppe an. Sie können Anwendungen nach der Migration zwar mit PowerShell-Cmdlets von einer Bereitstellungsgruppe in eine andere verschieben, jedoch kann das Verschieben von Anwendungen durch selektives Importieren in eindeutige Bereitstellungsgruppen reduziert oder eliminiert werden.
  1. Verwenden Sie den Parameter "DeliveryGroupName" mit dem Cmdlet "Import-XAFarm". Das Skript erstellt die angegebene Bereitstellungsgruppe, wenn sie nicht vorhanden ist.
  2. Verwenden Sie die folgenden Parameter mit regulären Ausdrücken, um die Anwendungen, die in die Bereitstellungsgruppe importiert werden sollen, basierend auf Ordner, Workergruppe Benutzerkontonamen und/oder Servernamen zu filtern. Es empfiehlt sich, den regulären Ausdruck in einzelne oder doppelte Anführungszeichen zu setzen. Weitere Informationen über reguläre Ausdrücke finden Sie unter http://msdn.microsoft.com/en-us/library/hs600312(v=vs.110).aspx.
     - MatchWorkerGroup und NotMatchWorkerGroup: Zum Beispiel bei Anwendungen, die auf Workergruppen veröffentlicht wurden, importiert das folgende Cmdlet Anwendungen in der Workergruppe "Productivity Apps" in eine XenApp 7.6-Bereitstellungsgruppe mit demselben Namen:
       Import-XAFarm –XmlInputFile XAFarm.xml –LogFile XAFarmImport.log –MatchWorkerGroup 'Productivity Apps' –DeliveryGroupName 'Productivity Apps'
     - MatchFolder und NotMatchFolder: Zum Beispiel bei Anwendungen, die in Anwendungsordnern organisiert sind, importiert das folgende Cmdlet Anwendungen im Ordner "Productivity Apps" in eine XenApp 7.6-Bereitstellungsgruppe mit dem gleichen Namen.
       Import-XAFarm –XmlInputFile XAFarm.xml –LogFile XAFarmImport.log –MatchFolder 'Productivity Apps' –DeliveryGroupName 'Productivity Apps'
       Beispielsweise importiert das folgende Cmdlet Anwendungen in Ordnern, deren Name "MS Office Apps" enthält, in die Standardbereitstellungsgruppe.
       Import-XAFarm -XmlInputFile .\THeFarmApps.XML -MatchFolder ".*/MS Office Apps/.*"
     - MatchAccount und NotMatchAccount: Zum Beispiel bei Anwendungen, die für Active Directory-Benutzer oder -Benutzergruppen veröffentlicht wurden, importiert das folgende Cmdlet Anwendungen, die für die Benutzergruppe "Finance Group" veröffentlicht wurden, in eine XenApp 7.6-Bereitstellungsgruppe mit dem Namen "Finance"
       Import-XAFarm –XmlInputFile XAFarm.xml –LogFile XAFarmImport.log –MatchAccount 'DOMAIN\\Finance Group' –DeliveryGroupName 'Finance'
     - MatchServer und NotMatchServer: Zum Beispiel bei Anwendungen, die auf Servern organisiert sind, importiert das folgende Cmdlet Anwendungen von Servern, deren Name nicht "Current" ist, in eine XenApp-Bereitstellungsgruppe mit dem Namen "Legacy."
       Import-XAFarm -XmlInputFile XAFarm.xml -LogFile XAFarmImport.log -NotMatchServer 'Current' -DeliveryGroupName 'Legacy'
- **Anpassung**: PowerShell-Programmierer können eigene Tools erstellen. Sie können z. B. das Exportskript als Bestandstool verwenden und damit die Änderungen in einer XenApp 6.x-Farm verfolgen. Sie können auch die XSD-Dateien ändern oder Ihre eigenen XSD-Dateien erstellen, um zusätzliche Daten oder Daten in unterschiedlichen Formaten in den XML-Dateien zu speichern. Sie können eine nicht standardmäßige XSD-Datei mit jedem der Import-Cmdlets angeben.
  Hinweis: Obwohl Sie Skriptdateien für bestimmte oder höhere Migrationsanforderungen ändern können, ist der Support auf unveränderte Skripts beschränkt. Der technische Support von Citrix empfiehlt, die Skripts in den Originalzustand zurückzuversetzen, um bei Bedarf erwartetes Verhalten ermitteln und Support bereitstellen zu können.

Problembehandlung

- Wenn Sie PowerShell Version 2.0 verwenden und das PowerShell-Anbieter-Snap-In für Citrix Gruppenrichtlinien oder das Citrix Common Commands Snap-In mit dem Cmdlet Add-PSSnapIn hinzugefügt haben, wird möglicherweise die folgende Fehlermeldung angezeigt, wenn Sie Cmdlets zum Exportieren oder Importieren ausführen: "Objekt verweist nicht auf eine Instanz eines Objekts". Dieser Fehler wirkt sich nicht auf die Skriptausführung aus und kann bedenkenlos ignoriert werden.
- Vermeiden Sie es, das PowerShell-Anbieter-Snap-In für Citrix Gruppenrichtlinien in der gleichen Konsolensitzung hinzuzufügen oder zu entfernen, in der Sie die Export- und Importskriptmodule verwenden, da diese Skriptmodule das Snap-In automatisch hinzufügen. Wenn Sie das Snap-In separat hinzufügen oder entfernen, wird u. U. einer der folgenden Fehler angezeigt:
  - "Ein Laufwerk mit dem Namen 'LocalGpo' ist bereits vorhanden." Dieser Fehler tritt auf, wenn das Snap-In zweimal hinzugefügt wird. Beim Laden versucht das Snap-In, das Laufwerk "LocalGpo" bereitzustellen und meldet dann den Fehler.
  - "Es wurde kein Parameter gefunden, der dem Parameternamen 'Controller' entspricht." Dieser Fehler wird angezeigt, wenn das Snap-In nicht hinzugefügt wurde und das Skript versucht, das Laufwerk bereitzustellen. Das Skript erkennt nicht, dass das Snap-In entfernt wurde. Schließen Sie die Konsole und starten Sie eine neue Sitzung. Importieren Sie in der neuen Sitzung die Skriptmodule. Fügen Sie das Snap-In nicht separat hinzu und entfernen Sie es auch nicht separat.
- Wenn Sie beim Importieren der Module mit der rechten Maustaste auf eine PSD1-Datei klicken und dann Öffnen oder Mit PowerShell öffnen wählen, wird das Fenster der PowerShell-Konsole in schneller Abfolge geöffnet und geschlossen, bis Sie den Vorgang anhalten. Sie vermeiden diesen Fehler, indem Sie den vollständigen Namen des PowerShell-Skriptmoduls direkt im PowerShell-Konsolenfenster eingeben (z. B. Import-Module .\ExportPolicy.psd1).
- Wenn beim Ausführen eines Exports oder Imports ein Berechtigungsfehler angezeigt wird, stellen Sie sicher, dass Sie ein XenApp-Administrator mit der Berechtigung zum Lesen von Objekten (beim Export) oder zum Lesen und Erstellen von Objekten (beim Import) sind. Sie müssen auch über die erforderlichen Berechtigungen zum Ausführen von Windows-PowerShell-Skripts verfügen.
- Wenn ein Export fehlschlägt, prüfen Sie, ob die XenApp 6.x-Farm funktionsfähig ist, indem Sie die Dienstprogramme DSMAINT und DSCHECK auf dem XenApp 6.x Controller-Server ausführen.
- Wenn Sie mit den Import-Cmdlets eine Importvorschau ausführen und später bei der tatsächlichen Migration nichts importiert wird, prüfen Sie, ob Sie den Parameter "Preview" aus den Import-Cmdlets entfernt haben.

Nicht importierte Richtlinieneinstellungen

Die folgenden Computer- und Benutzerrichtlinieneinstellungen werden nicht importiert, da sie nicht mehr unterstützt werden. Ungefilterte Richtlinien werden nie importiert. Die Features und Komponenten, die diese Einstellungen unterstützen, wurden entweder durch neue Technologien/Komponenten ersetzt oder sind aufgrund von Änderungen an Architektur oder Plattform nicht relevant.

Nicht importierte Computerrichtlinieneinstellungen

- Verbindungszugriffssteuerungen
- CPU-Managementserverstufe
- DNS-Adressauflösung
- Farmname
- Vollständiges Symbolcaching
- Systemüberwachung, Systemüberwachungstests
- Hostname des Lizenzservers, den Lizenzserverport
- Limit für Benutzersitzungen, Limits für Administratorsitzungen
- Lastauswertungsprogrammname
- Protokollieren von Anmeldelimitereignissen
- Maximaler Prozentsatz der Server mit Anmeldesteuerung
- Speicheroptimierung, Speicheroptimierung - Anwendungsausschlussliste, Speicheroptimierung - Intervall, Speicheroptimierung - Tag des Monats, Speicheroptimierung - Wochentag, Speicheroptimierung - Zeit
- Offlineanwendungsclient vertrauen, Ereignisprotokollierung für Offlineanwendungen, Offlineanwendungslizenzzeitraum, Offlineanwendungsbenutzer
- Eingabeaufforderung für Kennwort
- Benutzerdefinierte Neustartwarnung, Text für benutzerdefinierte Neustartwarnung, Anmeldungen vor Neustart deaktivieren (Zeit), Neustarthäufigkeit, Willkürliches Neustartintervall, Neustartbeginn, Neustartzeit, Neustartwarnungsintervall, Neustartwarnung - Startzeit, Neustartwarnung an Benutzer, Geplante Neustarts
- Spiegeln von Sitzungen *
- XML-Anfragen vertrauen (Konfiguration in StoreFront)
- Virtuelle IP - Adapteradressenfilterung, Virtuelle IP - Liste kompatibler Programme, Virtuelle IP - Erweiterte Kompatibilität, Virtuelle IP - Adapteradressenprogrammliste
- Arbeitslastname
- XenApp-Produktedition, XenApp-Produktmodell
- Port für XML-Dienst

* Ersetzt durch Windows-Remoteunterstützung

Nicht importierte Benutzerrichtlinieneinstellungen

- Client-COM-Ports automatisch verbinden, Client-LPT-Ports automatisch verbinden
- Client-COM-Portumleitung, Client-LPT-Portumleitung

- Clientdruckernamen
- Limit für gleichzeitige Anmeldungen
- Eingaben in gespiegelten Verbindungen *
- Trennentimerintervall - Fortbestehen, Beendentimerintervall - Fortbestehen
- Spiegelungsversuche protokollieren *
- Benutzer bei ausstehenden Spiegelungsverbindungen benachrichtigen *
- PreLaunch-Trennentimerintervall, PreLaunch-Beendentimerintervall
- Sitzungspriorität
- Single Sign-On, Zentraler Speicher für Single Sign-On
- Benutzer, die andere Benutzer spiegeln können; Benutzer, die andere Benutzer nicht spiegeln können *

* Ersetzt durch Windows-Remoteunterstützung

Nicht importierte Anwendungstypen

Die folgenden Anwendungstypen werden nicht importiert:
- Serverdesktops
- Inhalt
- Gestreamte Anwendungen (App-V ist die neue Methode für das Streaming von Anwendungen)

Zuordnung von Anwendungseigenschaften

Das Importskript für Farmdaten importiert nur Anwendungen. Die folgenden Anwendungseigenschaften werden ohne Änderungen importiert.

IMA-Eigenschaft	**FMA-Eigenschaft**
AddToClientDesktop	ShortcutAddedToDesktop
AddToClientStartMenu	ShortcutAddedToStartMenu
ClientFolder	ClientFolder
CommandLineExecutable	CommandLineExecutable
CpuPriorityLevel	CpuPriorityLevel
Beschreibung	Beschreibung
DisplayName	PublishedName
Aktiviert	Aktiviert
StartMenuFolder	StartMenuFolder
WaitOnPrinterCreation	WaitForPrinterCreation
WorkingDirectory	WorkingDirectory
FolderPath	AdminFolderName

Hinweis: IMA und FMA haben unterschiedliche Beschränkungen bei der Länge der Ordnernamen. In IMA ist die Länge der Ordnernamen auf 256 Zeichen beschränkt, in FMA auf 64 Zeichen. Anwendungen, deren Ordnerpfad einen Ordnernamen mit mehr als 64 Zeichen enthält, werden beim Import übersprungen. Das Limit gilt nur für die Ordnernamen im Ordnerpfad. Der gesamte Ordnerpfad kann länger sein als die aufgeführten Limits. Damit Anwendungen beim Importieren nicht übersprungen werden, empfiehlt es sich, die Länge der Anwendungsordnernamen zu prüfen und bei Bedarf vor dem Export zu kürzen.
Die folgenden Anwendungseigenschaften sind standardmäßig initialisiert oder nicht initialisiert oder auf die in den XenApp 6.x-Daten bereitgestellten Werte festgelegt:

FMA-Eigenschaft	**Wert**

FMA-Eigenschaft	Wert
Name	Initialisiert auf den vollständigen Pfadnamen, der die IMA-Eigenschaften "FolderPath" und "DisplayName" enthält, aber die voranstehende Zeichenfolge "Applications\" wurde gekürzt
ApplicationType	HostedOnDesktop
CommandLineArguments	Initialisiert mit den XenApp 6.x-Befehlszeilenargumenten
IconFromClient	Nicht initialisiert, Standardwert = false
IconUid	Initialisiert auf ein Symbolobjekt, das mit XenApp 6.x-Symboldaten erstellt wurde
SecureCmdLineArgumentsEnabled	Nicht initialisiert, Standardwert = true
UserFilterEnabled	Nicht initialisiert, Standardwert = false
UUID	Schreibgeschützt, vom Controller zugewiesen
Sichtbar	Nicht initialisiert, Standardwert = true

Die folgenden Anwendungseigenschaften werden teilweise migriert:

IMA-Eigenschaft	Anmerkungen
FileTypes	Nur in der neuen XenApp-Site existierende Dateitypen werden migriert. Dateitypen, die in der neuen Site nicht existieren, werden ignoriert. Dateitypen werden erst importiert, wenn die Dateitypen in der neuen Site aktualisiert wurden.
IconData	Neue Symbolobjekte werden erstellt, wenn die Symboldaten für die exportierten Anwendungen angegeben wurden.
Accounts	Die Benutzerkonten einer Anwendung werden zwischen der Benutzerliste für die Bereitstellungsgruppe und der Anwendung aufgeteilt. Explizite Benutzer werden zur Initialisierung der Benutzerliste für die Anwendung verwendet. Zudem wird der Benutzerliste für die Bereitstellungsgruppe das Konto "Domänenbenutzer" für die Domäne der Benutzerkonten hinzugefügt.

Die folgenden XenApp 6.x-Eigenschaften werden nicht importiert:

IMA-Eigenschaft	Anmerkungen
ApplicationType	Wird ignoriert.
HideWhenDisabled	Wird ignoriert.
AccessSessionConditions	Ersetzt durch Bereitstellungsgruppenzugriffsrichtlinien.
AccessSessionConditionsEnabled	Ersetzt durch Bereitstellungsgruppenzugriffsrichtlinien.
ConnectionsThroughAccessGatewayAllowed	Ersetzt durch Bereitstellungsgruppenzugriffsrichtlinien.
OtherConnectionsAllowed	Ersetzt durch Bereitstellungsgruppenzugriffsrichtlinien.
AlternateProfiles	FMA unterstützt keine gestreamten Anwendungen.
OfflineAccessAllowed	FMA unterstützt keine gestreamten Anwendungen.
ProfileLocation	FMA unterstützt keine gestreamten Anwendungen.

IMA-Eigenschaft	Anmerkungen
ProfileProgramArguments	FMA unterstützt keine gestreamten Anwendungen.
ProfileProgramName	FMA unterstützt keine gestreamten Anwendungen.
RunAsLeastPrivilegedUser	FMA unterstützt keine gestreamten Anwendungen.
AnonymousConnectionsAllowed	FMA verwendet eine andere Technologie für die Unterstützung nicht authentifizierter (anonymer) Verbindungen.
ApplicationId, SequenceNumber	IMA-eigene Daten.
AudioType	FMA unterstützt keine erweiterten Clientverbindungsoptionen.
EncryptionLevel	SecureICA ist in Bereitstellungsgruppen aktiviert/deaktiviert.
EncryptionRequired	SecureICA ist in Bereitstellungsgruppen aktiviert/deaktiviert.
SslConnectionEnabled	FMA verwendet eine andere TLS-Implementierung.
ContentAddress	FMA unterstützt keinen veröffentlichten Inhalt.
ColorDepth	FMA unterstützt keine erweiterten Fensterformen.
MaximizedOnStartup	FMA unterstützt keine erweiterten Fensterformen.
TitleBarHidden	FMA unterstützt keine erweiterten Fensterformen.
WindowsType	FMA unterstützt keine erweiterten Fensterformen.
InstanceLimit	FMA unterstützt keine Anwendungslimits.
MultipleInstancesPerUserAllowed	FMA unterstützt keine Anwendungslimits.
LoadBalancingApplicationCheckEnabled	FMA verwendet eine andere Technologie für den Lastausgleich.
PreLaunch	FMA verwendet eine andere Technologie für den Sitzungsvorabstart.
CachingOption	FMA verwendet eine andere Technologie für den Sitzungsvorabstart.
ServerNames	FMA verwendet eine andere Technologie.
WorkerGroupNames	FMA unterstützt keine Workergruppen.

Migrieren von XenDesktop 4

Feb 29, 2016

Sie können die Daten und Einstellungen von einer XenDesktop 4-Farm in eine XenDesktop 7.x-Site mit dem Migrationstool übertragen. Dieses ist auf dem Installationsmedium im Ordner "Support > Tools > MigrationTool". Das Tool enthält Folgendes:

- Das Exporttool XdExport für den Export der XenDesktop 4-Farmdaten in eine XML-Datei (Standardname: XdSettings.xml). Das XML-Dateischema ist in der Datei XdFarm.xsd.
- Das Importtool XdImport zum Importieren der Daten unter Ausführen des PowerShell-Skripts Import-XdSettings.ps1.

Das Migrationstool kann nur verwendet werden, wenn beide Bereitstellungen dieselbe Hypervisorversion (beispielsweise XenServer 6.2) und eine Active Directory-Umgebung haben.

Sie können mit diesem Tool nicht XenApp oder XenDesktop 4 nach XenApp migrieren.

Tipp: Sie können ein Upgrade von XenDesktop 5 (oder höheren XenDesktop-Versionen) auf die aktuelle XenDesktop-Version durchführen (siehe Upgrade einer Bereitstellung).

Einschränkungen

Nicht alle Daten und Einstellungen werden exportiert. Die folgenden Konfigurationselemente werden nicht migriert. Sie werden zwar exportiert, aber nicht importiert:

- Administratoren
- Einstellungen für delegierte Administration
- Desktopgruppenordner
- Lizenzierungskonfiguration
- Registrierungsschlüssel

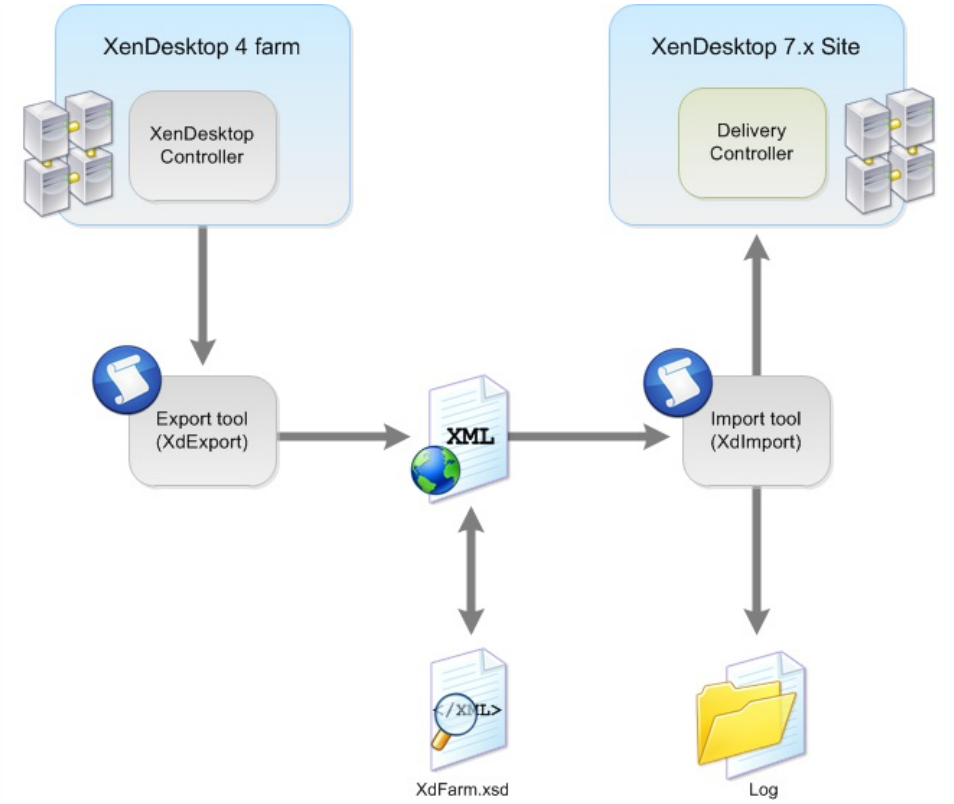
Folgende Anwendungsfälle werden bei der Migration nicht direkt unterstützt:

- Zusammenführen von Richtlinieneinstellungen oder Desktopgruppen- oder Hostingeinstellungen
- Zusammenführen von privaten Desktops in zufällige Bereitstellungsgruppen
- Anpassen vorhandener Komponenteneinstellungen mit Migrationstools

Weitere Informationen finden Sie unter Bei der Migration eingeschlossene und ausgeschlossene Elemente.

Migrationsschritte

In der folgenden Abbildung wird der Migrationsvorgang zusammengefasst.



Der Migrationsprozess besteht aus folgenden Schritten:

1. Aktivieren Sie in der Studio-Konsole auf dem XenDesktop 4-Controller den Wartungsmodus für alle Maschinen, die Sie exportieren möchten.
2. Exportieren Sie Daten und Einstellungen von der XenDesktop 4-Farm mit XdExport in eine XML-Datei (siehe Exportieren aus einer XenDesktop 4-Farm).
3. Bearbeiten Sie die XML-Datei so, dass sie nur die Daten und Einstellungen enthält, die Sie in Ihre XenDesktop-Site importieren möchten (siehe Bearbeiten der XML-Datei des Migrationstools).
4. Importieren Sie die Daten und Einstellungen aus der XML-Datei mit XdImport in Ihre neue XenDesktop-Site (siehe Importieren von XenDesktop 4-Daten).
5. Wiederholen Sie die Schritte 3 und 4, um weitere Änderungen vorzunehmen. Nach dem Vornehmen von Änderungen können Sie zusätzliche Desktops in vorhandene Bereitstellungsgruppen importieren. Verwenden Sie hierzu den Mergedesktops-Parameter beim Import.
6. Führen Sie die nach der Migration erforderlichen Schritte durch (siehe Aufgaben nach der Migration).

Vorbereitung der Migration

Führen Sie vor der Migration die folgenden Schritte durch:

- Informieren Sie sich darüber, welche Daten exportiert und importiert werden können und welche Konsequenzen dies für Ihre Bereitstellung hat. Siehe Bei der Migration eingeschlossene und ausgeschlossene Elemente.
- Citrix empfiehlt, dass Sie manuell eine Sicherungskopie der Sitedatenbank erstellen, damit Sie sie bei Problemen wiederherstellen können.
- Installieren Sie die XenDesktop 7.x-Komponenten und erstellen Sie eine Site einschließlich Datenbank.
- Für die Migration von XenDesktop 4 müssen alle VDAs auf der XenDesktop 5.x-Stufe sein, damit sie mit XenDesktop 4- und XenDesktop 7-Controllern kompatibel sind. Wenn in der Controllerinfrastruktur XenDesktop 7.x vollständig ausgeführt wird, können Windows 7-VDAs auf XenDesktop 7.x aktualisiert werden. Weitere Details finden Sie unter Migrationsbeispiele.

Exportieren aus einer XenDesktop 4-Farm

Feb 29, 2016

Das Exporttool "XdExport" extrahiert Daten aus einer einzelnen XenDesktop 4-Farm und generiert eine XML-Datei aus Darstellungen der Datenwerte.

Das Schema der XML-Datei wird in der Datei XdFarm.xsd bereitgestellt, die im Download des Importtools XdExport.zip und XdImport.zip enthalten ist.

Führen Sie XdExport auf einer Maschine aus, die in der Farm, aus der Daten exportiert werden, als XenDesktop 4-Controller fungiert. Auf dieser Maschine muss das XenDesktop 4-PowerShell SDK installiert sein. Sie müssen über die folgenden Berechtigungen für den Export der Daten verfügen:

- Die Benutzeridentität eines mindestens lesezugriffsberechtigten Citrix Administrators der Farm
- Berechtigung zum Lesen der Registrierung

Obwohl dies nicht empfohlen wird, können Sie das Tool ausführen, während der XenDesktop Controller aktiv verwendet wird (z. B. wenn Benutzer bei VDAs angemeldet sind).

Citrix empfiehlt dringend Folgendes:

- Update des XenDesktop 4-Controllers, auf dem das Tool ausgeführt wird, mit öffentlichen Hotfixes
- Keine Konfigurationsänderungen an der Site während der Export ausgeführt wird (z. B. Entfernen von Desktopgruppen)

1. Laden Sie XdExport.zip herunter und extrahieren Sie die Dateien auf den XenDesktop 4-Controller.
2. Führen Sie an einer Eingabeaufforderung XdExport.exe mit folgenden optionalen Parametern aus:

Parameter	Beschreibung
-Verbose	Generiert Nachrichten, die detaillierte Fortschrittsinformationen liefern.
-FilePath <path>	Der Speicherort der XML-Datei, in die die Farmdaten exportiert werden. Standard = .\XdSettings.xml
-Overwrite	Überschreibt jede in -FilePath angegebene Datei. Wenn Sie diesen Parameter nicht angeben und eine Ausgabedatei bereits vorhanden ist, schlägt das Tool folgender Fehlermeldung fehl: &quot.Fehler: Datei bereits vorhanden. Geben Sie -Overwrite an, um das Überschreiben der Datei zuzulassen. "
-? oder -help	Zeigt eine Beschreibung der Parameter an. Beim Beenden werden keine Daten exportiert.

3. Bei erfolgreicher Ausführung des Tools wird die Meldung Fertig angezeigt. Die Datei XdSettings.xml befindet sich an dem vom Parameter FilePath angegebenen Speicherort. Schlägt das Tool fehl, wird eine Fehlermeldung angezeigt.

Bearbeiten der XML-Datei des Migrationstools

Feb 29, 2016

Vor dem Importieren von Daten in eine XenDesktop 7.x-Site bearbeiten und prüfen Sie den Inhalt der vom Exporttool (XdExport) erstellten XML-Datei, besonders, wenn Sie die Migration in mehreren Phasen durchführen und beim Import einige Benutzer, Bereitstellungsgruppen und Richtlinien anderen vorgezogen haben.

Sie können den Inhalt der Datei mit einem beliebigen Texteditor anzeigen oder ändern. Sie können auch einen speziellen XML-Editor wie Microsoft XML Notepad verwenden.

Bestimmte Elemente des XML-Inhalts müssen in der XML-Datei vorhanden sein, damit sie vom Importtool (XdImport) verarbeitet wird.

Das benötigte XML-Schema ist in der Datei XdFarm.xsd definiert, die im Download des Migrationstools enthalten ist. Beim Arbeiten mit dieser Datei gilt Folgendes:

- In der Datei gibt das Attribut "minOccurs" mit einem Wert von 1 oder höher an, dass bestimmte Elemente vorhanden sein müssen, wenn das übergeordnete Element vorhanden ist.
- Wenn die an das Importtool übergebene XML-Datei ungültig ist, stoppt das Tool und eine Fehlermeldung wird angezeigt, mit deren Hilfe Sie in der XML-Datei nach dem Problem suchen können.

Importieren einer Untergruppe von Desktops oder Bereitstellungsgruppen

Zum Importieren nur einer Untergruppe von Desktopgruppen und Desktops müssen Sie den Inhalt des Elements DesktopGroups bearbeiten. Das Element DesktopGroups kann viele DesktopGroup-Elemente enthalten und in jedem DesktopGroup-Element befindet sich ein Desktops-Element, das zahlreiche Desktop-Elemente enthalten kann.

Löschen Sie das DesktopGroups-Element nicht. Sie können aber alle DesktopGroup-Elemente löschen und es leer lassen. Ebenso muss in jedem DesktopGroup-Element das Desktops-Element vorhanden sein. Es muss aber keine Desktop-Elemente enthalten.

Löschen Sie Desktop- oder DesktopGroup-Elemente, um zu verhindern, dass bestimmte einzelne Maschinen oder ganze Bereitstellungsgruppen importiert werden. Die XML-Datei enthält beispielsweise:

… … … … … … …

Bei diesem Beispiel wird durch die Änderungen verhindert, dass die Gruppe "Group1" importiert wird. Nur Machine3 aus der Gruppe "Group2" wird importiert:

… … …

Verwalten von Bereitstellungsgruppen mit doppelten Namen

In XenDesktop 4 können Desktopgruppen in Ordnern organisiert werden, Desktopgruppen mit dem gleichen Namen können in verschiedenen Ordnern erscheinen und der interne Name einer Desktopgruppe ist der Name, der den Benutzern angezeigt wird. In diesem Release hingegen dürfen Bereitstellungsgruppen nicht in Ordnern platziert werden und jede Bereitstellungsgruppe muss einen eindeutigen internen Namen haben, wobei der Name, der den Benutzern angezeigt wird, sich vom internen Namen unterscheiden kann. Aufgrund dieser Unterschiede müssen Sie möglicherweise Desktopgruppen umbenennen.

In Ihrer XenDesktop 4-Farm können Sie beispielsweise zwei verschiedene Desktopgruppen haben, die zwei verschiedenen Benutzern mit dem Namen "Mein Desktop" angezeigt wird. Dies kann durch Desktopgruppenordner ermöglicht werden. Wenn diese Bereitstellungsgruppen in der XenDesktop 7.x-Site getrennt bleiben sollen, müssen Sie die Namen der Desktopgruppen in der XML-Datei in eindeutige Namen ändern.

Wenn eine Bereitstellungsgruppe in der XenDesktop 7.x-Site über denselben Namen verfügt wie die zu importierende Desktopgruppe und die Bereitstellungsgruppen in der XenDesktop 7.x-Site getrennt bleiben sollen, müssen Sie den Namen der XenDesktop 4-Desktopgruppe in der XML-Datei ändern, damit der Name in der Site eindeutig bleibt. Wenn die zu importierende Desktopgruppe tatsächlich der XenDesktop 7.x-Bereitstellungsgruppe entspricht und die Maschinen in der XML-Datei mit der vorhandenen Desktopgruppe zusammengeführt werden sollen, müssen Sie die Desktopgruppe nicht umbenennen. Geben Sie stattdessen den Parameter -MergeDesktops im Importtool an. Enthält die XML-Datei beispielsweise:

… \Sales … \Finance

Entfernen Sie die doppelten Namen wie folgt:

… \Sales … \Finance

Verwalten von Richtlinienimports

Sie können einzelne Richtlinien aus der XML-Datei löschen und eindeutige Namen festlegen, um doppelte Richtliniennamen zu vermeiden. Das Zusammenführen von Richtlinien wird nicht unterstützt.

- Beim Import von Richtliniendaten werden entweder alle Richtlinien erfolgreich importiert oder es werden keine Richtliniendaten importiert, wenn an irgendeiner Stelle ein Fehler auftritt.
- Der Import zahlreicher Richtlinien mit umfangreichen Einstellungen kann mehrere Stunden dauern.
- Wenn Sie Richtlinien in Batches importieren, können deren ursprüngliche Prioritäten beeinträchtigt werden. Wenn Sie Richtlinien importieren, werden die relativen Prioritäten der importierten Richtlinien beibehalten. Sie erhalten jedoch eine höhere Priorität als bereits in der Site vorhandene Richtlinien. Wenn beispielsweise vier Richtlinien mit den Prioritäten 1 bis 4 in zwei Batches importiert werden sollen, sollten Sie die Richtlinien mit den Prioritäten 3 und 4 zuerst importieren, da der zweiten Gruppe automatisch eine höhere Priorität eingeräumt wird.

Zum ausschließlichen Importieren einer Untergruppe der Richtlinien in die XenDesktop 7.x-Site bearbeiten Sie den Inhalt des Policies-Elements. Das Policies-Element kann zahlreiche Policy-Elemente enthalten. Sie dürfen das Policies-Element nicht löschen. Sie können aber alle Policy-Elemente löschen und es leer lassen. Löschen Sie alle Policy-Elemente, um den Import bestimmter XenDesktop 4-Farmrichtlinien zu vermeiden. Enthält die XML-Datei beispielsweise:

… …

Wenn Sie den Import von XenDesktop 4-Richtlinien verhindern möchten, um mögliche Konflikte mit bereits in der XenDesktop 7.x-Site konfigurierten Richtlinien zu vermeiden, bearbeiten Sie die Datei, indem Sie einzelne Policy-Elemente wie folgt entfernen:

Alternativ können Sie die Datei so bearbeiten, dass die Richtlinie wie folgt mit einem anderen Namen importiert wird:

… …

Importieren von XenDesktop 4-Daten

Feb 29, 2016

Das Importtool "XdImport" liest Einstellungen aus XenDesktop 4, die in der vom Exporttool "XdExport" erzeugten XML-Datei enthalten sind, und wendet diese Einstellungen auf eine vorhandene XenDesktop 7.x-Site an. Das Importtool verwendet das PowerShell-Skript Import-XdSettings.ps1.

Um nur eine Teilmenge der exportierten Daten anzuwenden, bearbeiten Sie die XML-Datei, bevor Sie das Importtool ausführen. Sie können beispielsweise Desktopgruppen und Richtlinien entfernen, die in der XenDesktop 7.x-Bereitstellung nicht benötigt werden. Das Importtool wird erfolgreich ausgeführt, wenn Sie ganze Elemente leer lassen. Sie können beispielsweise alle Desktopgruppen problemlos löschen. Das Tool überprüft vor dem Import der Daten immer die XML-Datei.

Führen Sie XdImport auf jeder Maschine aus, auf der alle XenDesktop 7.x-SDKs installiert sind. Sie müssen Volladministrator für XenDesktop sein, um das Tool auszuführen.

Stellen Sie vor dem Importieren sicher, dass Sie eine XenDesktop 7.x-Site einschließlich Datenbank eingerichtet haben. Citrix empfiehlt, den Import in XenDesktop 7.x durchzuführen, bevor Benutzertests oder eine allgemeine Sitekonfiguration durchgeführt werden. Führen Sie Konfigurationen nur zusammen, wenn die Site nicht verwendet wird.

1. Erstellen Sie eine XenDesktop 7.x-Site.
2. Laden Sie die Datei XdImport.zip herunter und extrahieren Sie die Dateien auf die Maschine, auf der das Tool ausgeführt werden soll.
3. Führen Sie in einer PowerShell-Sitzung Import-XdSettings.ps1 mit folgenden Parametern aus:

Parameter	Beschreibung
-HypervisorConnectionCredentials	(erforderlich). Eine PowerShell-Hashtabelle, in der PSCredential-Instanzen Hypervisoradressen als Voraussetzung für die Erstellung von Hypervisorverbindungen Geben Sie die Anmeldeinformationen für den Hypervisor ein, mit dem die XenDesktop 4-Farm eine Verbindung herstellt. Für einen einzelnen Hypervisor können Sie das Argument folgendermaßen erstellen: $credential = Get-Credential $mappings = @{"http://" =$credential} .\Import-XdSettings.ps1 -FilePath. \XdSettings.xml -HypervisorConnectionCredentials $mappi Die in der Hashtabelle angegebene Adresse muss mit der Adresse in der XML-Datei genau übereinstimmen. Beispiel: Erstellen Sie bei Verwendung eines XenServer- und eines VMware-Hypervisors folgendes Argument: $Xencredential = Get-Credential $VMWcredential = Get-Credential $mappings = @{"http://" = $Xencredential;"http:///SDK" = $VMWcredential} .\Import-XdSetting
-FilePath <path>	(Der Wert für ist erforderlich.) Der Speicherort der XML-Datei, aus der die Farmdaten importiert werden
-AdminAddress	Name des Controllers in der XenDesktop 7.x-Site Standard = localhost
-MergeDesktops	Fügt in der XML-Datei definierte Desktops Bereitstellungsgruppen in der XenDesktop 7.x-Site hinzu, deren Namen mit Gruppen in der XML-Datei übereinstimm hinzugefügt. Wird dieser Parameter nicht angegeben, wird vorhandenen Bereitstellungsgruppen in der XenDesktop 7.x-Site kein Inhalt hinzugefügt.
-SkipMachinePolicy	Das Skript erstellt keine Maschinenrichtlinie mit Einstellungen auf Siteebene. Wenn Sie diesen Parameter nicht angeben und die Maschinenrichtlinie für die Site
-WhatIf	Führt einen Testlauf durch, um festzustellen, was an der XenDesktop 7.x-Site geändert und was ihr hinzugefügt werden würde. Wenn dieser Parameter angeg wird jedoch nicht geändert.
-LogFilePath <path>	Der vollständige Pfad der Protokolldatei. Das Protokoll enthält Text, der alle auf der XenDesktop 7.x-Site durchgeführten Schreibvorgänge beschreibt. Standa
-? oder -help	Zeigt eine Beschreibung von Parametern an. Beim Beenden werden keine Daten importiert.

Wenn die XML-Datei Richtliniendaten enthält, werden alle Richtlinien erfolgreich importiert. Tritt jedoch an irgendeiner Stelle ein Fehler auf, werden keine Richtliniendaten importiert. Der Import zahlreicher Richtlinien mit umfangreichen Einstellungen kann mehrere Stunden dauern.

Nach Abschluss des Skripts wird die Meldung Fertig angezeigt. Nach erfolgreichem Import der Daten aus der XML-Datei können Sie weitere Import- und Exportvorgänge durchführen. Wenn Sie jedoch alle relevanten Daten importiert haben, können Sie die Aufgaben nach der Migration durchführen.

Aufgaben nach der Migration

Feb 29, 2016

Nach dem erfolgreichen Importieren von Daten aus einer XenDesktop 4-Farm in eine XenDesktop 7.x-Site müssen Sie folgende Aufgaben durchführen, bevor Sie die neue Site als Produktionsumgebung nutzen können:

- Aktualisieren Sie die Virtual Delivery Agents (VDAs). Obwohl es nicht erforderlich ist, empfiehlt Citrix, dass Sie zunächst ein Upgrade der VDAs und dann erst ein Upgrade der Controller, von Studio oder von Director durchführen.
  - Windows Vista und Windows XP: Upgrade auf XenDesktop 5. 6 Feature Pack 1 Virtual Desktop Agent
  - Windows 7: Upgrade auf XenDesktop 7.x Virtual Delivery Agent.
- Erstellen Sie die Administratoren, die für die XenDesktop 7.x-Site benötigt werden.
- Citrix empfiehlt, ein Update der Benutzergeräte auf die aktuelle Version von Citrix Receiver durchzuführen, um von Hotfixes zu profitieren und Unterstützung für die aktuellen Funktionen zu erhalten.
- Ändern Sie die importierten Desktops so, dass die registrierungsbasierte Controller-Discovery verwendet wird, und verweisen Sie sie auf die XenDesktop 7.x-Controller mit einer der folgenden Methoden:
  - Entfernen Sie manuell den nicht benötigten Organisationseinheits-GUID-Eintrag aus der Registrierung und fügen Sie einen Registrierungseintrag "ListOfDDCs" hinzu.
  - Richten Sie eine Maschinenrichtlinie ein, um die Liste der Controller auf die Desktops mit der Active Directory-Richtlinie GPMC.msc zu verteilen. Sie können diese Einstellung nicht mit Studio konfigurieren.

  Registrierungsbasierte Controller-Discovery ist die Standardeinstellung für XenDesktop 7.x, Active Directory-basierte Discovery steht aber weiterhin zur Verfügung.

- Optional können Sie die folgenden Registrierungsschlüsseleinstellungen implementieren, die im Abschnitt zu den bewährten Methoden für die registrierungsbasierte Registrierung in XenDesktop unter CTX133384 beschrieben werden:
  - HeartbeatPeriodMS
  - PrepareSessionConnectionTimeoutSec
  - MaxWorkers
  - DisableActiveSessionReconnect
  - ControllersGroupGuid

  Wenn Sie dies unterlassen, werden die XenDesktop 7.x-Standardeinstellungen für diese Schlüssel verwendet.

- Deaktivieren Sie den Wartungsmodus für die importierten Maschinen, sofern diese vor dem Generieren der XML-Datei in XenDesktop 4 im Wartungsmodus waren.
- Überprüfen Sie die XenDesktop 7.x-Einstellungen, um sicherzustellen, dass sie korrekt sind, insbesondere dann, wenn Sie die XML-Datei PortICAConfig unter XenDesktop 4 geändert haben.
- Überprüfen Sie alle Migrationskomponenten, um sicherzustellen, dass die Migration erfolgreich abgeschlossen wurde.

Migrationsbeispiele

Feb 29, 2016

Beispiel 1: Migrieren einer großen XenDesktop 4-Farm in eine XenDesktop 7-Site

In diesem Beispiel wird eine XenDesktop 4-Farm verwendet. Die XenDesktop 4-Farm hat 50 Desktopgruppen, wobei jede Gruppe durchschnittlich 100 Desktops hat. Die XenDesktop 4-Desktops werden über Provisioning Services (PVS) bereitgestellt und die Maschinen werden auf VMware ESX-Hypervisors ausgeführt. Auf allen VMs ist die XenDesktop 4-Version des VDAs installiert.

Migrationsschritte

1. Aktualisieren Sie alle XenDesktop 4-VDAs auf die XenDesktop 5.6 Feature Pack 1-VDA-Software. Dadurch können die VDAs sowohl beim XenDesktop 4-Controller als auch beim XenDesktop 7-Delivery Controller registriert werden.
   - Informationen zu Windows 7-VDAs finden Sie unter Durchführen eines Upgrades von Virtual Desktop Agent auf einer VM oder einem Blade-Computer.
   - Informationen zu VDAs unter Windows XP und Windows Vista finden Sie unter Virtual Desktop Agents unter Windows XP oder Windows Vista.
2. Stellen Sie sicher, dass sich alle Benutzer von der XenDesktop 4-Farm abgemeldet haben.
3. Stellen Sie sicher, dass alle Maschinen in den Wartungsmodus gesetzt wurden.
4. Führen Sie das Exporttool (XdExport) auf der XenDesktop 4-Farm aus.
5. Installieren Sie XenDesktop 7-Komponenten.
   1. Erstellen Sie mit Studio eine Site im vollständigen Produktionsmodus.
   2. Ist Provisioning Services Teil der Bereitstellung, aktualisieren Sie den Provisioning Services-Server und die Provisioning Services-Agents.
   3. Aktualisieren Sie den Lizenzserver und die zugehörigen Lizenzen.
6. Entzippen Sie das Importtool (XdImport) in einem lokalen Verzeichnis auf dem XenDesktop 7-Controller.
7. Kopieren Sie die in Schritt 4 mit dem Exporttool erstellte XML-Datei (XdSettings.xml) in das lokale Verzeichnis.
8. Starten Sie in der PowerShell-Konsole des Studio-Stammknotens der XenDesktop 7-Site eine PowerShell-Sitzung.
9. Führen Sie das Importtool (XdImport) aus, sodass die Anmeldeinformationen der zugeordneten Hypervisors und der Pfad der XML-Datei übergeben werden.
10. Erstellen Sie manuell Administratoreinstellungen über den Administratorknoten in Studio neu. Informationen hierzu finden Sie unter Delegierte Administration.
11. Ändern Sie die importierten Desktops so, dass sie die registrierungsbasierte Controller-Discovery verwenden, und verweisen Sie sie auf den neuen XenDesktop 7-Controller.
12. Für VDAs unter Windows 7 empfiehlt Citrix ein Upgrade zur Verwendung von XenDesktop 7-VDAs für Windows-Desktopbetriebssysteme, damit alle neuen Features genutzt werden können.
    Nach dem Upgrade von VDAs auf XenDesktop 7 für Maschinen in einem Katalog oder einer Bereitstellungsgruppe aktualisieren Sie den Katalog (siehe Verwalten von Maschinenkatalogen) und die Bereitstellungsgruppen (siehe Verwalten von Einstellungen in Bereitstellungsgruppen).
13. Deaktivieren Sie den Wartungsmodus für die Bereitstellungsgruppen.
14. Konfigurieren Sie StoreFront, um die zuvor vom Webinterface bereitgestellten Desktops zur Verfügung zu stellen. Weitere Informationen finden Sie in der StoreFront-Dokumentation.

Beispiel 2: Export einer XenDesktop 4-Farm mit teilweisem Import in eine XenDesktop 7.1-Site

In diesem Beispiel erfolgt die Migration in mehreren Schritten, wobei bei jedem Schritt ein Teil der verbleibenden Desktops

migriert wird. Derzeit wird eine XenDesktop 4-Farm verwendet und eine XenDesktop 7.1-Site wurde bereits erstellt und ist im Einsatz. Die XenDesktop 4-Farm hat 50 Desktopgruppen, wobei jede Gruppe durchschnittlich 100 Desktops hat. Die XenDesktop 4-Desktops werden über Provisioning Services bereitgestellt und die Maschinen werden auf Citrix XenServer-Hypervisors ausgeführt. Auf allen VMs ist die XenDesktop 4-Version des VDAs installiert.

Migrationsschritte

1. Führen Sie das Exporttool (XdExport) auf der XenDesktop 4-Farm aus.
    1. Entzippen Sie das Exporttool (XdExport) auf einem Desktop Delivery Controller in der Farm.
    2. Führen Sie das Exporttool als Citrix Administrator ohne Parameter aus.
2. Kopieren und bearbeiten Sie die resultierende XML-Datei, sodass sie nur die Gruppen und Desktops enthält, die Sie migrieren möchten.
3. Vergewissern Sie sich, dass in der XenDesktop 4-Farm sich alle Benutzer von den zu migrierenden Desktops abgemeldet haben und aktivieren Sie den Wartungsmodus für alle Desktops, die migriert werden sollen.
4. Entzippen Sie das Importtool (XdImport) in einem lokalen Verzeichnis auf dem XenDesktop 7.1-Delivery-Controller.
5. Kopieren Sie die bearbeitete XML-Datei in das lokale Verzeichnis.
6. Starten Sie in der PowerShell-Konsole des Studio-Stammknotens der XenDesktop 7.1-Site eine PowerShell-Sitzung.
7. Führen Sie das Importtool (XdImport) aus, sodass die Anmeldeinformationen der zugeordneten Hypervisors und der Pfad der XML-Datei übergeben werden.
8. Erstellen Sie manuell Administratoreinstellungen über den Administratorknoten in Studio neu. Informationen hierzu finden Sie unter Delegierte Administration.
9. Ändern Sie die importierten Desktops so, dass sie die registrierungsbasierte Controller-Discovery verwenden, und verweisen Sie sie auf den neuen XenDesktop 7.1-Controller.
10. Aktualisieren Sie alle VDAs auf die entsprechende VDA-Software:
    - Windows 7-VDAs:
        - Führen Sie ein Upgrade auf XenDesktop 7-VDAs durch, wie unter Durchführen eines Upgrades von Virtual Desktop Agent auf einer VM oder einem Blade-Computer beschrieben.
        - Nach dem Upgrade der gesamten VDA-Software auf XenDesktop 7 für Maschinen in einem Katalog oder einer Bereitstellungsgruppe aktualisieren Sie den Katalog (siehe Verwalten von Maschinenkatalogen) und die Bereitstellungsgruppen (siehe Verwalten von Einstellungen in Bereitstellungsgruppen).
    - Aktualisieren Sie VDAs, die unter Windows XP oder Windows Vista ausgeführt werden auf XenDesktop 5.6 FP1 (siehe Virtual Desktop Agents unter Windows XP oder Windows Vista).
11. Deaktivieren Sie den Wartungsmodus für die Bereitstellungsgruppen.
12. Konfigurieren Sie StoreFront, um die zuvor vom Webinterface bereitgestellten Desktops zur Verfügung zu stellen. Weitere Informationen finden Sie in der StoreFront-Dokumentation.

Bei der Migration eingeschlossene und ausgeschlossene Elemente

Feb 29, 2016

Eingeschlossene Elemente

In der folgenden, wenn auch nicht vollständigen, Tabelle wird beschrieben, was während der Migration zu diesem Release mit den wichtigsten Daten geschieht. Sofern nicht anders angegeben, werden die jeweiligen Datentypen importiert.

Datentyp	Hinweise
Desktopgruppen	Desktopgruppen werden in diesem Release zu Bereitstellungsgruppen. Symbole von Desktopgruppen werden nicht exportiert. SecureIcaRequired ist auf "True" gesetzt, wenn DefaultEncryptionLevel in XenDesktop 4 nicht auf "Basic" festgelegt ist. Wenn eine Desktopgruppe in der XenDesktop 4-Farm den gleichen Namen wie eine Bereitstellungsgruppe in der XenDesktop 7.x-Site hat, können Sie Desktops der XenDesktop 4-Gruppe einer Bereitstellungsgruppe mit demselben Namen in der Zielsite hinzufügen. Geben Sie hierfür den Parameter MergeDesktops an, wenn Sie das Importtool ausführen. Die Einstellungen der XenDesktop 7.x-Bereitstellungsgruppe werden nicht mit den Einstellungen der XenDesktop 4-Gruppe überschrieben. Wenn dieser Parameter nicht angegeben wird und eine Gruppe mit demselben Namen wie eine in der XML-Datei definierte Gruppe existiert, zeigt das Tool einen Fehler an und wird angehalten, bevor Daten importiert werden.
Desktops	Sie können keine privaten Desktops zu zufälligen Bereitstellungsgruppen hinzufügen. Zufällige Desktops können einer statischen Bereitstellungsgruppe nicht hinzugefügt werden.
Maschinen	Maschinen werden in vier Maschinenkataloge importiert. Die folgenden Maschinenkataloge werden vom Importtool in der XenDesktop 7.x-Site automatisch erstellt: • Importierte bestehende zufällige (für gepoolte VMs) • Importierte bestehende statische (für zugewiesene VMs) • Importierte physische zufällige (für gepoolte oder Blade-PC) • Importierte physische statische (für private oder Blade-PC) Alle folgenden Importe von Maschinen verwenden dieselben vier Maschinenkataloge.
Poolverwaltungspools	Umfasst aus mehreren Pools bestehende Pools und Einstellungen für betriebsbereite Pools, einschließlich Zeitplan. • PeakBuffersizePercent ist standardmäßig auf 10 % gesetzt. • OffPeakBufferSizePercent ist standardmäßig auf 10 % gesetzt. • Alle nicht ausgewählten Tage in der Einstellung Business days in XenDesktop 4 werden in dieses Release als Teil des Wochenend-Energieschemas importiert. • HostingXD4-Aktionszeiten werden auf die nächste volle Minute gerundet. • Startzeiten werden auf die nächste volle Stunde gerundet. • Endzeiten werden auf die nächste volle Stunde gerundet.
Farmeinstellungen	Die folgenden Farmeinstellungen werden als Maschinenrichtlinie importiert: • IcaKeepAlive • AutoClientReconnect

Datentyp	Hinweise
	• SessionReliability Die Einstellung zum Aktivieren von Flash Player wird nicht importiert.
Richtlinien	Bestimmte Richtliniendaten werden importiert. Filter, Einstellungen und Drucker werden als Benutzerrichtlinien importiert. Weitere Informationen zum Export und Import von Benutzerrichtlinien finden Sie in der anderen Tabelle in diesem Dokument. • Neue Regeln für Zugriffsrichtlinien werden basierend auf XenDesktop 4-Gruppeneinstellungen erstellt. • Beim Import von Richtlinien wird deren relative Prioritätsreihenfolge beibehalten. Sie werden jedoch immer mit einer höheren Priorität als alle auf der XenDesktop 7.x-Site vorhandenen Richtlinien hinzugefügt. • Das Zusammenführen von Richtlinien wird nicht unterstützt. Es gibt keine Möglichkeit, Richtlinien in Active Directory zu importieren. Sie werden immer in der Site gespeichert.
Benutzerzuweisungen	
Hypervisoreinstellungen	Dieser Parameter ist für das XdImport-Tool erforderlich. Hypervisoradressen werden exportiert, nicht aber die Anmeldeinformationen, die für den Zugriff auf diese Hypervisors erforderlich sind. Zum Erstellen von Hypervisorverbindungen in der XenDesktop 7.x-Site müssen Sie die Adressen aus der XML-Datei extrahieren und eine PowerShell-Hashtabelle anlegen, in der die Adressen den entsprechenden Anmeldeinformationen zugeordnet sind. Geben Sie dann diese Tabelle im Parameter HypervisorConnectionCredentials des Importtools an. Weitere Informationen finden Sie unter Importieren von XenDesktop 4-Daten. Das Zusammenführen oder Aktualisieren von Hypervisoreinstellungen für vorhandene Desktopgruppen und Hypervisorverbindungen wird nicht unterstützt.
Administratoren	(Wird nicht importiert.) Es werden keine Administratordaten importiert, einschließlich Daten über delegierte Administratoren. Sie müssen neue Administratoren für die XenDesktop 7.x-Site erstellen.
Lizenzierungskonfiguration	(Wird nicht importiert.) Enthält Informationen wie Lizenzservername und Edition. Lizenzdateien werden nicht exportiert.
Desktopgruppenordner	(Wird nicht importiert.) Dieses Release unterstützt keine Desktopgruppenordner. Bei doppelten Desktopgruppennamen (weil unterschiedliche Ordner in der XenDesktop 4-Farm Gruppen mit identischen Namen enthielten) wird das Importtool angehalten, wenn Sie die Namen in der XML-Datei nicht bearbeiten.
Registrierungsschlüssel	(Wird nicht importiert.) Weitere Informationen zur Implementierung von Registrierungsschlüsseln finden Sie unter Aufgaben nach der Migration.

Benutzerrichtliniendaten

In der folgenden Tabelle wird beschrieben, wie Benutzerrichtliniendaten exportiert und importiert werden.

Kategorie und Einstellung in XenDesktop 4	XML-Datei	Kategorie und Einstellung in XenDesktop 7.x
Bandbreite\Visuelle Effekte\Sitzungslimits OEM-Virtuelle Kanäle	ClientOEMVCBandwidth	Nicht importiert

Kategorie und Einstellung in XenDesktop 4	XML-Datei	Kategorie und Einstellung in XenDesktop 7.x
OEM-Virtuelle Kanäle deaktivieren		
Benutzerarbeitsbereich\Zeitzone Lokale Zeit des Clients nicht verwenden	DoNotUseClientLocalTime	Nicht importiert
Sicherheit\Verschlüsselung SecureICA-Verschlüsselung	ClientSecurityRequirement	Nicht importiert
Bandbreite\SpeedScreen Beschleunigung der Bildanzeige durch verlustreiche Komprimierung	LossyCompression settings	ICA\Visuelle Anzeige\Festbilder Grad der verlustreichen Komprimierung Schwellenwert für verlustreiche Komprimierung Heavyweight-Komprimierung ICA\Visuelle Anzeige\Bewegtbilder Grad der progressiven Komprimierung Schwellenwert für progressive Komprimierung
Bandbreite\Visuelle Effekte Desktophintergrund deaktivieren	TurnOffWallpaper	ICA\Desktopbenutzeroberfläche Desktophintergrund
Bandbreite\Visuelle Effekte Menüanimation	TurnOffMenuWindowAnimation	ICA\Desktopbenutzeroberfläche Menüanimation
Bandbreite\Visuelle Effekte Fensterinhalt beim Verschieben nicht anzeigen	DoNotShowWindowContentsWhileDragging	ICA\Desktopbenutzeroberfläche Fensterinhalt beim Verschieben anzeigen
Bandbreite\Visuelle Effekte\Sitzungslimits Audio	ClientAudioBandwidth__AllowedBandWidth	ICA\Bandbreite Bandbreitenlimit für die Audioumleitung
Bandbreite\Visuelle Effekte\Sitzungslimits Zwischenablage	ClientClipboardBandwidth__AllowedBandWidth	ICA\Bandbreite Bandbreitenlimit für Zwischenablagenumleitung

Kategorie und Einstellung in XenDesktop 4	XML-Datei	Kategorie und Einstellung in XenDesktop 7.x
Bandbreite\Visuelle Effekte\Sitzungslimits COM-Ports	ClientComBandwidth__AllowedBandWidth	Die COM-Portumleitung ist in XenDesktop 7.x veraltet.
Bandbreite\Visuelle Effekte\Sitzungslimits Laufwerke	ClientDriveBandwidth__AllowedBandWidth	ICA\Bandbreite Bandbreitenlimit für Dateiumleitung
Bandbreite\Visuelle Effekte\Sitzungslimits LPT-Ports	ClientLptBandwidth__AllowedBandWidth	Die LPT-Portumleitung ist in XenDesktop 7.x veraltet.
Bandbreite\Visuelle Effekte\Sitzungslimits Sitzung insgesamt	OverallBandwidth__AllowedBandWidth	ICA\Bandbreite Bandbreitenlimit für Sitzung insgesamt
Bandbreite\Visuelle Effekte\Sitzungslimits Drucker	LimitPrinterBandWidth__AllowedBandWidth	ICA\Bandbreite Bandbreitenlimit für Druckerumleitung
Clientgeräte\Ressourcen\Audio Mikrofone	ClientAudioMicrophone__TurnOn	ICA\Audio Clientmikrofonumleitung
Clientgeräte\Ressourcen\Audio Tonqualität	ClientAudioQuality__Quality	ICA\Audio Audioqualität
Clientgeräte\Ressourcen\Audio Lautsprecher deaktivieren	DisableClientAudioMapping	ICA\Audio Clientaudioumleitung
Clientgeräte\Ressourcen\Laufwerke Verbindung (Connection)	ConnectClientDriveAtLogon__TurnOn	ICA\Dateiumleitung Laufwerke automatisch verbinden
Clientgeräte\Ressourcen\Laufwerke Diskettenlaufwerke deaktivieren	DisableClientDriveMapping__DisableFloppyDrive	ICA\Dateiumleitung Clientdiskettenlaufwerke
Clientgeräte\Ressourcen\Laufwerke Festplatten deaktivieren	DisableClientDriveMapping__DisableHardDrive	ICA\Dateiumleitung Lokale Clientfestplattenlaufwerke
Clientgeräte\Ressourcen\Laufwerke CD-ROM-Laufwerke deaktivieren	DisableClientDriveMapping__DisableCdrom	ICA\Dateiumleitung Optische Clientlaufwerke

Kategorie und Einstellung in XenDesktop 4	XML-Datei	Kategorie und Einstellung in XenDesktop 7.x
Clientgeräte\Ressourcen\Laufwerke Remotelaufwerke deaktivieren	DisableClientDriveMapping__DisableRemote	ICA\Dateiumleitung Clientnetzlaufwerke
Clientgeräte\Ressourcen\Laufwerke USB-Laufwerke deaktivieren	DisableClientDriveMapping__DisableUSB	ICA\Dateiumleitung Clientwechsellaufwerke
Clientgeräte\Ressourcen\Laufwerke\Optimierung Asynchrones Schreiben	CDMAsyncWrites	ICA\Dateiumleitung Asynchrones Schreiben verwenden
Clientgeräte\Ressourcen\Sonstiges Zwischenablagezuordnung deaktivieren	DisableClientClipboardMapping	ICA Clientzwischenablagenumleitung
Clientgeräte\Ressourcen\Ports COM-Ports deaktivieren	DisableClientCOMPortMapping	Die COM-Portumleitung ist in XenDesktop 7.x veraltet.
Clientgeräte\Ressourcen\Ports LPT-Ports deaktivieren	DisableClientLPTPortMapping	Die LPT-Portumleitung ist in XenDesktop 7.x veraltet.
Clientgeräte\Ressourcen\USB USB	RemoteUSBDevices__DisableRemoteUSBDevices	ICA\USB-Geräte Client-USB-Geräteumleitung
Drucken\Clientdrucker Automatische Erstellung	ConnectClientPrinterAtLogon__Flag	ICA\Drucken\Clientdrucker Clientdrucker automatisch erstellen
Drucken\Clientdrucker Legacy-Clientdrucker	LegacyClientPrinters__TurnOn	ICA\Drucken\Clientdrucker Clientdruckernamen
Drucken\Clientdrucker Speicherung von Druckereigenschaften	ModifiedPrinterProperties__WriteMethod	ICA\Drucken\Clientdrucker Speicherung von Druckereigenschaften
Drucken\Clientdrucker Weiterleiten von Druckaufträgen	ClientPrintingForNetworkPrinter__TurnOn	ICA\Drucken\Clientdrucker Direkte Verbindungen zu Druckservern
Drucken\Clientdrucker Clientdruckerzuordnung deaktivieren	DisableClientPrinterMapping	ICA\Drucken Clientdruckerumleitung

Kategorie und Einstellung in XenDesktop 4	XML-Datei	Kategorie und Einstellung in XenDesktop 7.x
Drucken\Treiber Native Druckertreiber automatisch installieren	PrintDriverAutoInstall__TurnOn	ICA\Drucken\Treiber Automatische Installation von mitgelieferten Druckertreibern
Drucken\Treiber Universeller Treiber	ClientPrintDriverToUse	ICA\Drucken\Treiber Verwendung universeller Druckertreiber
Drucken\Sitzungsdrucker Sitzungsdrucker	NetworkPrinters	ICA\Drucken Sitzungsdrucker
Drucken\Sitzungsdrucker Standarddrucker des Clients wählen	DefaultToMainClientPrinter__NetworkDefault DefaultToMainClientPrinter__TurnOn	ICA\Drucken Standarddrucker

Ausgeschlossene Elemente

Nicht alle XenDesktop 4-Komponenten werden in diesem Release unterstützt. Die folgenden Elemente werden nicht migriert:

- **Virtual Delivery Agent**: Bevor Sie mit einem XenDesktop 7.x-Delivery Controller virtuelle Desktops von XenDesktop 4 verwalten können, müssen Sie ein Upgrade der VDAs auf mindestens XenDesktop 5.x durchführen. Weitere Informationen zum Upgrade der VDAs finden Sie unter Aufgaben nach der Migration.
- **Controller**: Sie müssen neue Controller-Server bereitstellen. Sie können einen XenDesktop 4-Controller nicht auf eine XenDesktop 7.x-Site aktualisieren. XenDesktop 7.x-Sites können keiner XenDesktop 4-Farm und XenDesktop 4-Controller können keiner XenDesktop 7.x-Site beitreten. Darüber hinaus gelten für jede Version andere Serveranforderungen. XenDesktop 4 erfordert Windows Server 2003 und XenDesktop 7.x neuere Windows Server-Versionen.
- **Webinterface**: Citrix empfiehlt die Verwendung von StoreFront mit XenDesktop 7.x Informationen zu Installation und Einrichtung finden Sie in der StoreFront-Dokumentation. Wenn das XenDesktop-Installationsprogramm das Webinterface erkennt, wird StoreFront zwar installiert, das Webinterface jedoch nicht entfernt.
- **Konfiguration der Organisationseinheiten in Active Directory**: Die Freigabe einer Organisationseinheit zwischen zwei Farmen oder zwei Sites oder einer Farm und einer Site wird nicht unterstützt. Wenn Sie die neue Site mit der Active Directory-basierten Controller-Discovery statt der standardmäßigen registrierungsbasierten Controller-Discovery konfigurieren, müssen Sie eine neue Organisationseinheit hierfür erstellen.
- **XML-Datei PortICAConfig**: Wenn Sie die Standardeinstellungen für diese Datei geändert haben, müssen Sie diese Einstellungen für die neue Site unter Umständen über Gruppenrichtlinienobjekte konfigurieren.
- **Über XenDesktop 4 Service Pack 1 bereitgestellte Einstellungen für die Konfigurationsprotokollierung**:
- **Daten von Provisioning Services**:
- **Anwendungen**:
- **Liste der Controller**:
- **NetScaler Gateway**:
- **Drosselungseinstellungen für das Ereignisprotokoll**:

Sicherheit

May 10, 2016

PDF Sicherheit mit Citrix XenApp und XenDesktop: Erste Schritte

XenApp und XenDesktop bieten eine auf Sicherheit ausgelegte Lösung, mit der Sie Ihre Umgebung Ihren Sicherheitsanforderungen anpassen können.

Bei mobilen Mitarbeitern steht die IT-Abteilung dem Sicherheitsrisiko durch verlorene oder gestohlene Daten gegenüber. Durch Hosten von Anwendungen und Desktops trennen XenApp und XenDesktop sicher vertrauliche Daten und geistiges Eigentum von Endpunktgeräten, da alle Daten in einem Datencenter gespeichert werden. Wenn Richtlinien für das Zulassen von Datenübertragungen aktiviert sind, werden alle Daten verschlüsselt.

Die XenDesktop- und XenApp-Datencenter vereinfachen auch die Reaktion auf Vorfälle mit einem zentralisierten Überwachungs- und Verwaltungsdienst. Mit Director überwachen und analysieren IT-Mitarbeiter Daten, auf die im Netzwerk zugegriffen wird, und mit Studio kann die IT-Abteilung im Datencenter Patches anwenden und Systemanfälligkeiten verhindern statt Probleme lokal auf jedem Endbenutzergerät zu beheben.

XenApp und XenDesktop vereinfachen auch Audits und die Einhaltung der Richtlinientreue, da Untersuchende mit einer zentralisierten Überwachungsliste ermitteln können, wer auf welche Anwendungen und Daten zugegriffen hat. Director sammelt durch Zugriff auf die Konfigurationsprotokollierung und die OData-API Verlaufsdaten über Updates des Systems und der Benutzerdatennutzung.

Mit der delegierten Administration richten Sie Administratorrollen ein, um den Zugriff auf XenDesktop und XenApp auf granulärer Ebene zu steuern. Dies ermöglicht Flexibilität in Ihrer Organisation, um bestimmten Administratoren vollständigen Zugriff auf Aufgaben, Vorgänge und Geltungsbereiche zugeben, während der Zugriff anderer Administratoren beschränkt ist.

Mit XenApp und XenDesktop wenden Administratoren Richtlinien auf verschiedenen Netzwerkebenen an, von der lokalen Ebene bis zur Organisationseinheitsebene, und steuern damit Benutzer granulär. Diese Steuerung der Richtlinien legt fest, ob ein Benutzer, ein Gerät oder eine Gruppe von Benutzern und Geräten eine Verbindung herstellen, Kopieren bzw. Einfügen oder lokale Laufwerke zuordnen können. Dies verringert Sicherheitsbedenken bei Zeitpersonal von Drittanbietern. Administratoren können auch Desktop Lock verwenden, sodass Benutzer nur den virtuellen Desktop verwenden können und der Zugriff auf das lokale Betriebssystem des Endbenutzergeräts verhindert wird.

Administratoren können die Sicherheit in XenApp oder XenDesktop erhöhen und die Site so konfigurieren, dass sie das TLS-Sicherheitsprotokoll (Transport Layer Security) des Controllers oder zwischen Endbenutzern und VDAs verwendet. Das Protokoll kann auch für eine Site aktiviert werden, um die Serverauthentifizierung, die Verschlüsselung des Datenstroms und die Prüfung der Nachrichtenintegrität für eine TCP/IP-Verbindungen bereitzustellen.

XenApp und XenDesktop unterstützen auch die mehrstufige Authentifizierung für Windows oder eine bestimmte Anwendung. Mit der mehrstufigen Authentifizierung können auch alle Ressourcen, die von XenApp und XenDesktop bereitgestellt werden, verwaltet werden. Diese Methoden sind u. a.:

- Tokens
- Smartcards
- RADIUS
- Kerberos

- Biometrie

XenDesktop kann mit vielen Sicherheitslösungen von Drittanbietern integriert werden, von der Identitätsverwaltung bis zu Antivirensoftware. Eine Liste der unterstützten Produkte finden Sie unter http://www.citrix.com/ready.

Bestimmte Releases von XenApp und XenDesktop sind für Common Criteria zertifiziert. Eine Liste dieser Standards finden Sie unter http://www.commoncriteriaportal.org/cc/.

Verwandter Inhalt

- Best Practices und Überlegungen zur Sicherheit
- Delegierte Administration
- Smartcards
- TLS

Sicherheit – Überlegungen und bewährte Methoden

Jul 22, 2016

In diesem Dokument wird Folgendes beschrieben:

- Allgemeine bewährte Methoden zur Gewährleistung der Sicherheit beim Verwenden dieses Releases sowie sicherheitsrelevante Unterschiede zwischen diesem Release und einer konventionellen Computerumgebung
- Verwalten von Benutzerkonten
- Verwalten von Benutzerprivilegien
- Verwalten von Anmelderechten
- Konfigurieren von Benutzerrechten
- Konfigurieren von Diensteinstellungen
- Bereitstellungsszenarios und ihre Auswirkungen auf die Sicherheit
- Sicherheitsüberlegungen für Remote-PC-Zugriff

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/.

Bewährte Methoden zur Gewährleistung der 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.

Schützen Sie alle Maschinen in der Umgebung mit Umkreisfirewalls, u. a. bei Bedarf auch an Grenzen von Enklaven.

Wenn Sie eine konventionelle Umgebung zu diesem Release migrieren, müssen Sie ggf. eine vorhandene Umkreisfirewall neu positionieren oder neue Umkreisfirewalls hinzufügen. Beispiel: Zwischen einem konventionellen Client und einem Datenbankserver im Datenzentrum befindet sich eine Umkreisfirewall. Bei diesem Release muss diese Umkreisfirewall so platziert werden, dass sich der virtuelle Desktop und das Benutzergerät auf der einen Seite befinden und die Datenbankserver und Controller im Datencenter auf der anderen Seite. Es empfiehlt sich daher, im Datencenter einen Netzbereich für die von XenDesktop verwendeten Datenbankserver und Controller zu erstellen. Außerdem sollten Sie die Installation eines Schutzmechanismus zwischen dem Benutzergerät und dem virtuellen Desktop in Betracht ziehen.

Alle Maschinen in der Umgebung müssen durch eine persönliche Firewall geschützt werden. Wenn Sie Kernkomponenten und Virtual Delivery Agents (VDAs) installieren, können Sie die erforderlichen Ports für Komponenten und Features so einrichten, dass sie automatisch geöffnet werden, sobald der Windows-Firewalldienst erkannt wird (auch wenn die Firewall nicht aktiviert ist). Sie können die Firewallports auch manuell konfigurieren. Wenn Sie eine andere Firewall verwenden, muss diese manuell konfiguriert werden.

Hinweis: Da die TCP-Ports 1494 und 2598 für ICA und CGP verwendet werden, sind sie normalerweise an der Firewall geöffnet, damit Benutzer außerhalb des Rechenzentrums auf sie zugreifen können. Citrix empfiehlt, dass diese Ports nicht für etwas Anderes verwendet werden, damit administrative Benutzeroberflächen nicht versehentlich gefährdet werden. Die

Ports 1494 und 2598 sind bei der Internet Assigned Numbers Authority (http://www.iana.org/) offiziell registriert.

Die gesamte Netzwerkkommunikation sollte Ihren Sicherheitsrichtlinien gemäß angemessen gesichert und verschlüsselt werden. Sie können die gesamte Kommunikation zwischen Microsoft Windows-Computern mit IPSec sichern. Weitere Informationen hierzu finden Sie in der 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 (siehe Ändern von Benutzereinstellungen).

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.

Verwalten von Benutzerkonten

Wenn Sie bei der Installation eines Virtual Delivery Agents (VDA) die Option zum Installieren von App-V-Veröffentlichungskomponenten wählen oder diese Komponenten später installieren, wird dem VDA das lokale Administratorkonto CtxAppVCOMAdmin hinzugefügt. Wenn Sie die App-V-Veröffentlichung verwenden, ändern Sie dieses Konto nicht. Wenn Sie die App-V-Veröffentlichung nicht benötigen, aktivieren Sie das Feature bei der Installation nicht. Wenn Sie sich nach der Installation der App-V-Veröffentlichung gegen eine Verwendung des Features entscheiden, können Sie das Konto deaktivieren oder löschen.

Verwalten von Benutzerprivilegien

Geben Sie Benutzern nur die Rechte, die sie benötigen. Microsoft Windows-Privilegien können weiterhin in der üblichen Weise auf Desktops angewendet werden: Konfigurieren Sie Privilegien mit "Zuweisung von Benutzerrechten" und Gruppenmitgliedschaften mit einer Gruppenrichtlinie. Der Vorteil dieses Release besteht darin, dass einem Benutzer Administratorrechte für einen Desktop eingeräumt werden können, ohne ihm auch die physische Kontrolle über den Computer, auf dem der Desktop gespeichert ist, zu gewähren.

Beachten Sie beim Planen von Desktopprivilegien Folgendes:

- Standardmäßig wird nicht berechtigten Benutzern beim Herstellen einer Verbindung mit einem Desktop die Zeitzone des Systems, auf dem der Desktop ausgeführt wird, statt der Zeitzone ihres eigenen Benutzergerätes angezeigt. Weitere Informationen dazu, wie Sie Benutzern erlauben, ihre Ortszeit beim Verwenden von Desktops anzuzeigen, finden Sie unter Ändern von Benutzereinstellungen.
- 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

Geben Sie Benutzern die erforderlichen Anmelderechte. 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, Übers Netzwerk anmelden, Anmelden als Stapelverarbeitungsauftrag und Anmelden als Dienst.

Laut Microsoft wird der Gruppe Remotedesktopbenutzer standardmäßig das Anmelderecht "Anmelden über Remotedesktopdienste" gewährt (außer für Domänencontroller).

Die Sicherheitsrichtlinie Ihres Unternehmens legt möglicherweise explizit fest, dass diese Gruppe aus dem Anmelderecht entfernt werden sollte. Erwägen Sie folgenden Ansatz:

- Der Virtual Delivery Agent (VDA) für Serverbetriebssysteme verwendet Microsoft-Remotedesktopdienste. Sie können die Gruppe der Remotedesktopbenutzer als eine eingeschränkte Gruppe konfigurieren und die Gruppenmitgliedschaft durch Active Directory-Gruppenrichtlinien steuern. Weitere Informationen finden Sie in der Dokumentation von Microsoft.
- Für andere XenApp- und XenDesktop-Komponenten, einschließlich dem VDA für Desktopbetriebssysteme, ist die Gruppe der Remotedesktopbenutzer nicht erforderlich. Für diese Komponenten benötigt die Gruppe der Remotedesktopbenutzer das Recht "Anmelden über Remotedesktopdienste" also nicht und Sie können es entfernen. Beachten Sie außerdem Folgendes:
  - Wenn Sie diese Computer mit Remotedesktopdienste verwalten, stellen Sie sicher, dass alle Administratoren Mitglieder der Administratorgruppe sind.
  - Wenn Sie diese Computer nicht mit Remotedesktopdienste verwalten, könnten Sie Remotedesktopdienste auf diesen Computern deaktivieren.

Es ist zwar möglich, dem Anmelderecht "Anmelden über Remotedesktopdienste verweigern" Benutzer und Gruppen hinzuzufügen, jedoch wird von der Verwendung von verweigernden Rechten allgemein abgeraten. Weitere Informationen finden Sie in der Dokumentation von Microsoft.

Konfigurieren von Benutzerrechten

Bei der Installation des Delivery Controllers werden die folgenden Windows-Dienste erstellt:

- Citrix AD-Identitätsdienst (NT SERVICE\CitrixADIdentityService): Verwaltet Microsoft Active Directory-Computerkonten für VMs.
- Citrix Analytics (NT SERVICE\CitrixAnalytics): Sammelt Sitekonfigurations- und Nutzungsinformationen zur Verwendung von Citrix, wenn das Sammeln vom Siteadministrator genehmigt wurde. Diese Informationen werden dann an Citrix gesendet, damit das Produkt verbessert werden kann.
- Citrix App-Bibliothek (NT SERVICE\CitrixAppLibrary): Unterstützt die Verwaltung und das Provisioning von AppDisks, AppDNA-Integration und die Verwaltung von App-V.
- Citrix Brokerdienst (NT SERVICE\CitrixBrokerService): Wählt die virtuellen Desktops oder Anwendungen aus, die den

Benutzern zur Verfügung stehen.

- Citrix Konfigurationsprotokollierungsdienst (NT SERVICE\CitrixConfigurationLogging): Erfasst alle Konfigurationsänderungen und andere Zustandsänderungen, die von den Administratoren an der Site vorgenommen werden.
- Citrix Konfigurationsdienst (NT SERVICE\CitrixConfigurationService): Repository der Site für freigegebene Konfigurationen.
- Citrix Dienst für die delegierte Administration (NT SERVICE\CitrixDelegatedAdmin): Verwaltet die Berechtigungen, die Administratoren gewährt werden.
- Citrix Umgebungstestdienst (NT SERVICE\CitrixEnvTest): Verwaltet Selbsttests der anderen Delivery Controller-Dienste.
- Citrix Hostdienst (NT SERVICE\CitrixHostService): Speichert Informationen zu den Hypervisorinfrastrukturen, die in einer XenApp- oder XenDesktop-Bereitstellung verwendet werden, und bietet der Konsole die Funktionalität zum Enumerieren von Ressourcen in einem Hypervisorpool.
- Citrix Maschinenerstellungsdienste (NT SERVICE\CitrixMachineCreationService): Orchestriert das Erstellen von Desktop-VMs.
- Citrix Überwachungsdienst (NT SERVICE\CitrixMonitor): Sammelt Metrik für XenApp oder XenDesktop, speichert historische Informationen und bietet eine Abfrageschnittstelle für Problembehandlungs- und Berichterstattungstools.
- Citrix StoreFront-Dienst (NT SERVICE\CitrixStorefront): Unterstützt die Verwaltung von StoreFront. (Der Dienst selbst gehört nicht zur StoreFront-Komponente.)
- Citrix StoreFront-Dienst für die privilegierte Administration (NT SERVICE\CitrixPrivilegedService): Unterstützt privilegierte Verwaltungsvorgänge von StoreFront. (Der Dienst selbst gehört nicht zur StoreFront-Komponente.)

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.

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 melden sich die oben im Abschnitt "Konfigurieren von Benutzerrechten" aufgeführten Windows-Dienste des Delivery Controllers als NETWORK SERVICE an. Ändern Sie diese Diensteinstellungen nicht.

Der Citrix StoreFront-Dienst für die privilegierte Administration meldet sich als lokales System an (NT AUTHORITY\SYSTEM). Dies ist für StoreFront-Vorgänge des Delivery Controllers erforderlich, die normalerweise nicht für Dienste verfügbar sind (einschließlich das 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.

Auswirkungen von Bereitstellungsszenarios auf die Sicherheit

Ihre Benutzerumgebung kann Benutzergeräte enthalten, die von Ihrer Organisation nicht verwaltet werden und dem Vollzugriff der jeweiligen Benutzer unterliegen oder solche, die von Ihrer Organisation verwaltet werden. Die Sicherheitsüberlegungen für diese beiden Umgebungen sind generell unterschiedlich.

Verwaltete Benutzergeräte

Verwaltete Benutzergeräte unterliegen einer administrativen Steuerung. Sie werden entweder von Ihnen gesteuert oder von einer anderen Organisation, der Sie vertrauen. Sie können Benutzergeräte konfigurieren und Benutzern direkt bereitstellen. Alternativ können Sie Terminals bereitstellen, auf denen ein einzelner Desktop im Vollbildmodus ausgeführt wird. Befolgen Sie die oben beschriebenen Sicherheitsanweisungen bei allen verwalteten Benutzergeräten. Dieses Release bietet den Vorteil, dass nur ganz wenig Software auf einem Benutzergerät erforderlich ist.

Ein verwaltetes Benutzergerät kann für die Verwendung im Vollbildmodus oder im Fenstermodus konfiguriert werden.

- Im Vollbildmodus können Benutzer sich über den normalen Anmeldebildschirm für Windows anmelden. Dieselben Anmeldeinformationen des Benutzers werden dann zum automatischen Anmelden für dieses Release verwendet.
- Im Fenstermodus melden sich die Benutzer zunächst beim Benutzergerät an. Anschließend melden sie sich über die in diesem Release bereitgestellte Website bei diesem Release an.

Nicht verwaltete Benutzergeräte

Wenn Benutzergeräte nicht von einer vertrauenswürdigen Organisation verwaltet werden, kann nicht von einer administrativen Steuerung ausgegangen werden. Beispiel: Sie erlauben Benutzern, sich ihre eigenen Geräte zu besorgen und sie zu konfigurieren, doch die Benutzer halten sich u. U. nicht an die oben beschriebenen generellen optimalen Sicherheitsverfahren. Dieses Release hat den Vorteil, nicht verwalteten Benutzergeräten Desktops sicher bereitstellen zu können. Diese Geräte sollten jedoch einen grundlegenden Antivirenschutz haben, um Keylogger und ähnliche Angriffe auf Benutzereingaben abzuwehren.

Überlegungen zum Datenspeicher

Mit diesem Release können Sie verhindern, dass Benutzer Daten auf Benutzergeräten speichern, die sie selbst physisch steuern können. Sie müssen dennoch bedenken, welche Auswirkungen es haben kann, wenn Benutzer Daten auf Desktops speichern. Im Allgemeinen sollten Benutzer keine Daten auf Desktops speichern. Daten sollten an einem Ort gespeichert werden, an dem sie entsprechend geschützt werden können, wie z. B. auf Dateiservern, Datenbankservern oder in anderen Repositorys.

Möglicherweise enthält Ihre Desktopumgebung verschiedene Desktoptypen, wie gepoolte und dedizierte Desktops. Benutzer sollten zu keiner Zeit Daten auf Desktops speichern, die für andere Benutzer freigegeben sind, wie z. B. gepoolte Desktops. Wenn Benutzer Daten auf dedizierten Desktops speichern, sollten diese Daten entfernt werden, wenn der Desktop zu einem späteren Zeitpunkt anderen Benutzern zugänglich gemacht wird.

Umgebungen mit mehreren Versionen

Umgebungen mit mehreren Versionen sind während einiger Upgrades unvermeidbar. Folgen Sie bewährten Methoden und minimieren Sie die Zeitdauer, während der unterschiedliche Versionen von Citrix Komponenten koexistieren. In Umgebungen mit mehreren Versionen wird beispielsweise die Sicherheitsrichtlinie nicht gleichförmig durchgesetzt.

Hinweis: Dies ist typisch für andere Softwareprodukte. Bei Verwendung einer älteren Version von Active Directory wird die Gruppenrichtlinie bei neueren Windows-Versionen nur teilweise durchgesetzt.

Nachfolgend wird eine spezifische Citrix Umgebung mit mehreren Versionen beschrieben, bei der ein Sicherheitsproblem auftreten kann. Wenn Citrix Receiver 1.7 zum Herstellen einer Verbindung mit einem virtuellen Desktop verwendet wird, auf dem der Virtual Delivery Agent in XenApp und XenDesktop 7.6 Feature Pack 2 ausgeführt wird, ist die Richtlinieneinstellung **Dateiübertragungen zwischen Desktop und Client zulassen** für die Site aktiviert, kann jedoch nicht von einem Delivery Controller deaktiviert werden, auf dem XenApp und XenDesktop 7.1 ausgeführt werden. 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.

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. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.

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

Typ: REG_DWORD

Wert: 0 = Zuweisung mehrerer Benutzer deaktivieren, 1 = (Standard) Zuweisung mehrerer Benutzer aktivieren.

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.

Delegierte Administration

Feb 29, 2016

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**: Administratoren sind Einzelpersonen oder Personengruppen, die durch ein Active Directory-Konto identifiziert werden. Jeder Administrator ist mit mindestens einem Paar aus Rolle und Geltungsbereich verknüpft.
- **Rollen**: Eine Rolle repräsentiert eine Stellenfunktion und ist mit definierten Berechtigungen ausgestattet. Beispiel: Die Rolle "Bereitstellungsgruppenadministrator" verfügt über Berechtigungen wie etwa "Bereitstellungsgruppe erstellen" und "Desktop aus Bereitstellungsgruppe entfernen". Ein Administrator kann mehrere Rollen für eine Site haben, d. h. eine Person kann sowohl Bereitstellungsgruppenadministrator als auch Maschinenkatalogadministrator sein. Rollen können integriert oder benutzerdefiniert sein.

  Integrierte Rollen:

Rolle	Berechtigungen
Volladministrator	Kann alle Aufgaben und Vorgänge ausführen. Ein Volladministrator wird immer mit dem Geltungsbereich "Alle" kombiniert.
Lesezugriffadministrator	Kann alle Objekte in den angegebenen Geltungsbereichen sowie globale Informationen anzeigen, aber nicht ändern. Beispiel: Ein Lesezugriffadministrator mit Geltungsbereich = London kann alle globalen Objekte (z. B. Konfigurationsprotokollierung) und alle London-bezogenen Geltungsbereichsobjekte (z. B. London-Bereitstellungsgruppen) sehen. Dieser Administrator kann jedoch nicht die Objekte im Geltungsbereich "New York" sehen (sofern die Geltungsbereiche "London" und "New York" einander nicht überlappen).
Helpdeskadministrator	Kann Bereitstellungsgruppen anzeigen und die diesen Gruppen zugeordneten Sitzungen und Maschinen verwalten. Kann den Maschinenkatalog und die Hostinformationen der überwachten Bereitstellungsgruppen sehen sowie Sitzungsverwaltungs- und Energieverwaltungsvorgänge für die Maschinen in diesen Bereitstellungsgruppen durchführen.
Maschinenkatalogadministrator	Kann Maschinenkataloge erstellen und verwalten sowie darin Maschinen bereitstellen. Kann Maschinenkataloge aus der Virtualisierungsinfrastruktur, Provisioning Services und von physischen Maschinen anlegen. Mit dieser Rolle können Basisimages verwaltet und Software installiert werden, aber den Benutzern können keine Anwendungen oder Desktops zugewiesen werden.
Bereitstellungsgruppenadministrator	Kann Anwendungen, Desktops und Maschinen bereitstellen sowie die mit ihnen verbundenen Sitzungen verwalten. Kann zudem Anwendungs- und Desktopkonfigurationen wie Richtlinien und die Energieverwaltungseinstellungen verwalten.
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	Alle Vertrieb

Administrator	Rollen	Geltungsbereiche
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 erwägt, Peter zum Volladministrator für den Geltungsbereich "Win7" zu machen; entscheidet sich jedoch dagegen, da ein Volladministrator ebenfalls über vollständige Administratorrechte für alle Objekte verfügt, die nicht in einen Geltungsbereich fallen, z. B. "Site" und "Administrator".

Verwenden der delegierten Administration

Im Allgemeinen hängt die Anzahl der Administratoren und die Granularität der Berechtigungen von der Größe und Komplexität der Bereitstellung ab.

- In kleinen Bereitstellungen oder Testbereitstellungen übernehmen ein oder wenige Administratoren alle Aufgaben und es findet keine Delegierung statt. Erstellen Sie in diesem Fall einen einzelnen Administrator mit der integrierten Rolle "Volladministrator", die den Geltungsbereich "Alle" hat.
- In größeren Bereitstellungen mit mehr Maschinen, Anwendungen und Desktops ist mehr Delegierung erforderlich. Mehrere Administratoren haben möglicherweise bestimmte funktionale Zuständigkeiten (Rollen). Beispiel: Es gibt zwei Volladministratoren, andere sind Helpdeskadministratoren. Weiterhin werden von einem Administrator ggf. nur bestimmte Objektgruppen (Geltungsbereiche) wie Maschinenkataloge verwaltet. Erstellen Sie in diesem Fall neue Geltungsbereiche und Administratoren mit einer der integrierten Rollen und den entsprechenden Geltungsbereichen.
- Noch größere Bereitstellungen erfordern möglicherweise weitere (oder differenziertere) Geltungsbereiche sowie andere Administratoren mit ungewöhnlichen Rollen. Bearbeiten oder erstellen Sie in diesem Fall weitere Geltungsbereiche, erstellen Sie benutzerdefinierte Rollen und erstellen Sie jeden Administrator mit einer integrierten oder benutzerdefinierten Rolle sowie vorhandenen und neuen Geltungsbereichen.

Für mehr Flexibilität und zur Vereinfachung der Konfiguration können Sie neue Geltungsbereiche erstellen, wenn Sie einen Administrator erstellen. Sie können auch beim Erstellen oder Bearbeiten von Maschinenkatalogen oder Verbindungen Geltungsbereiche festlegen.

Erstellen und Verwalten von Administratoren

Beim Erstellen einer Site als lokaler Administrator wird dieses Benutzerkonto automatisch zum Volladministrator mit Vollzugriff auf alle Objekte. Nachdem die Site erstellt wurde, verfügen lokale Administratoren über keine besonderen Rechte.

Die Volladministratorrolle hat immer den Geltungsbereich "Alle"; dies kann nicht geändert werden.

Standardmäßig wird ein Administrator aktiviert. Beim Erstellen des neuen Administrators kann das Deaktivieren eines Administrators erforderlich sein, die betroffene Person übernimmt jedoch erst zu einem späteren Zeitpunkt Verwaltungsaufgaben. Bei vorhandenen aktivierten Administratoren kann es vorkommen, dass Sie einige deaktivieren müssen, während Sie Objekte/Geltungsbereiche neu strukturieren und sie dann wieder aktivieren, wenn Sie die Aktualisierung der Konfiguration abgeschlossen haben. Der Volladministrator kann nicht deaktiviert werden, wenn dies dazu führen würde, dass kein aktivierter Volladministrator mehr vorhanden ist. Das Kontrollkästchen zum Aktivieren/Deaktivieren steht zur Verfügung, wenn Sie einen Administrator erstellen, kopieren oder bearbeiten.

Wenn Sie ein Rollen-/Geltungsbereichspaar beim Kopieren, Bearbeiten oder Löschen eines Administrators löschen, wird nur die Beziehung zwischen Rolle und Geltungsbereich für diesen Administrator gelöscht, jedoch nicht die Rolle oder der Geltungsbereich selbst. Außerdem hat dies keine Auswirkungen auf andere Administratoren, die mit diesem Rollen-/Geltungsbereichspaar konfiguriert sind.

Klicken Sie zum Verwalten von Administratoren im Studio-Navigationsbereich auf Konfiguration > Administratoren und dann im mittleren Bereich oben auf die Registerkarte Administratoren.

- Zum Erstellen eines Administrators klicken Sie im Aktionsbereich auf Administrator erstellen. Geben Sie den Namen eines Benutzerkontos ein oder navigieren zu einem Benutzerkonto, wählen oder erstellen Sie einen Geltungsbereich und wählen Sie eine Rolle. Der neue Administrator ist standardmäßig aktiviert. Sie können dies ändern.
- Zum Kopieren eines Administrators wählen Sie diesen im mittleren Bereich aus und klicken Sie im Aktionsbereich auf Administrator kopieren. Geben Sie den Namen des Benutzerkontos ein oder navigieren zu dem Benutzerkonto. Sie können die Rollen-/Geltungsbereichspaare auswählen und dann bearbeiten oder löschen und neue hinzufügen. Der neue Administrator ist standardmäßig aktiviert. Sie können dies ändern.
- Zum Bearbeiten eines Administrators wählen Sie diesen im mittleren Bereich aus und klicken Sie im Aktionsbereich auf Administrator bearbeiten. Sie können die Rollen-/Geltungsbereichspaare bearbeiten oder löschen und neue hinzufügen.
- Zum Löschen eines Administrators wählen Sie diesen im mittleren Bereich aus und klicken Sie im Aktionsbereich auf Administrator löschen. Der Volladministrator kann nicht gelöscht werden, wenn dies dazu führen würde, dass kein aktivierter Volladministrator mehr vorhanden ist.

Erstellen und Verwalten von Rollen

Rollennamen können maximal 64 Unicode-Zeichen enthalten. Die folgenden Zeichen sind nicht zulässig: \ (umgekehrter Schrägstrich), / (Schrägstrich), ; (Semikolon), : (Doppelpunkt), # (Nummernzeichen), , (Komma), * (Sternchen), ? (Fragezeichen), = (Gleichheitszeichen) , < (Pfeil nach links), > (Pfeil nach rechts), | (senkrechter Strich), [ ] (eckige Klammern), () (runde Klammern), " (Anführungszeichen) und ' (Apostroph). Beschreibungen können bis zu 256 Unicode-Zeichen enthalten.

Integrierte Rollen können nicht bearbeitet oder gelöscht werden. Benutzerdefinierte Rollen können nicht gelöscht werden, wenn sie von einem Administrator verwendet werden.

Hinweis: Nur bestimmte Produkteditionen unterstützen benutzerdefinierte Rollen. Editionen, die keine benutzerdefinierten Rollen unterstützen, verfügen nicht über verwandte Einträge im Aktionsbereich.
Klicken Sie zum Verwalten von Rollen im Studio-Navigationsbereich auf Konfiguration > Administratoren und dann im unteren mittleren Bereich auf die Registerkarte Rollen.

- Zum Anzeigen von Rollendetails wählen Sie die Rolle im mittleren Bereich aus. Im unteren Teil des mittleren Bereichs werden die Objekttypen und die zugehörigen Berechtigungen für die Rolle angezeigt. Klicken Sie auf die Registerkarte Administratoren im unteren Bereich, um eine Liste der Administratoren anzuzeigen, die derzeit diese Rolle haben.
- Zum Erstellen einer benutzerdefinierten Rolle klicken Sie im Aktionsbereich auf Rolle erstellen. Geben Sie einen Namen und eine Beschreibung ein. Wählen Sie die Objekttypen und Berechtigungen aus.
- Zum Kopieren einer Rolle wählen Sie diese im mittleren Bereich aus und klicken Sie im Aktionsbereich auf Rolle kopieren. Ändern Sie den Namen und die Beschreibung sowie die Objekttypen und Berechtigungen nach Bedarf.
- Zum Bearbeiten einer Rolle wählen Sie diese im mittleren Bereich aus und klicken Sie im Aktionsbereich auf Rolle bearbeiten. Ändern Sie den Namen und die Beschreibung sowie die Objekttypen und Berechtigungen nach Bedarf.
- Zum Löschen einer Rolle wählen Sie diese im mittleren Bereich aus und klicken Sie im Aktionsbereich auf Rolle löschen. Bestätigen Sie die Löschung.

Erstellen und Verwalten von Geltungsbereichen

Beim Erstellen einer Site steht nur der Geltungsbereich "Alle" zur Verfügung. Dieser kann nicht gelöscht werden.

Sie können Geltungsbereiche mit der unten aufgeführten Vorgehensweise erstellen. Sie können auch die Geltungsbereiche erstellen, wenn Sie einen Administrator erstellen. Jeder Administrator muss mindestens einem Rollen-/Geltungsbereichspaar zugeordnet werden. Beim Erstellen oder Bearbeiten von Desktops, Maschinenkatalogen, Anwendungen oder Hosts können Sie diese einem bestehenden Geltungsbereich hinzufügen. Wenn Sie sie keinem Geltungsbereich hinzufügen, bleiben sie Teil des Geltungsbereichs "Alle".

Die Geltungsbereichszuordnung ist bei der Erstellung von Sites und für Objekte der delegierten Administration (Geltungsbereiche und Rollen) nicht möglich. Objekte, die nicht zugeordnet werden können, gehören zum Geltungsbereich "Alle". (Volladministratoren ist immer der Geltungsbereich "Alle" zugeordnet.) Maschinen, Energieaktionen, Desktops und Sitzungen werden nicht direkt einem Geltungsbereich zugeordnet. Administratoren können Berechtigungen für diese Objekte über die zugehörigen Maschinenkataloge oder Bereitstellungsgruppen zugewiesen werden.

Geltungsbereichsnamen können maximal 64 Unicode-Zeichen enthalten. Die folgenden Zeichen sind nicht zulässig: \ (umgekehrter Schrägstrich), / (Schrägstrich), ; (Semikolon), : (Doppelpunkt), # (Nummernzeichen), , (Komma), * (Sternchen), ? (Fragezeichen), = (Gleichheitszeichen) , < (Pfeil nach links), > (Pfeil nach rechts), | (senkrechter Strich), [ ] (eckige Klammern), () (runde Klammern), " (Anführungszeichen) und ' (Apostroph). Beschreibungen können bis zu 256 Unicode-Zeichen enthalten.

Wenn Sie einen Geltungsbereich kopieren oder bearbeiten, dürfen Sie nicht vergessen, dass Objekte, die aus dem Geltungsbereich entfernt werden, für den Administrator ggf. nicht mehr zugänglich sind. Ist der bearbeitete Geltungsbereich mit einer oder mehreren Rollen gepaart, stellen Sie sicher, dass durch Änderungen an dem Bereich kein Rollen-/Geltungsbereichspaar unbrauchbar wird.

Klicken Sie zum Verwalten von Geltungsbereichen im Studio-Navigationsbereich auf Konfiguration > Administratoren und dann im mittleren Bereich oben auf die Registerkarte Geltungsbereiche.

- Zum Erstellen eines Geltungsbereichs klicken Sie im Aktionsbereich auf Geltungsbereich erstellen. Geben Sie einen Namen und eine Beschreibung ein. Zum Einschließen aller Objekte eines bestimmten Typs (z. B. Bereitstellungsgruppen), wählen Sie den Objekttyp aus. Zum Einschließen bestimmter Objekte erweitern Sie den Typ und wählen Sie die einzelnen Objekte (z. B. einzelne Bereitstellungsgruppen des Vertriebs) aus.
- Zum Kopieren eines Geltungsbereichs wählen Sie diesen im mittleren Bereich aus und klicken Sie im Aktionsbereich auf Geltungsbereich kopieren. Geben Sie einen Namen und eine Beschreibung ein. Ändern Sie die Objekttypen und Berechtigungen nach Bedarf.
- Zum Bearbeiten eines Geltungsbereichs wählen Sie diesen im mittleren Bereich aus und klicken Sie im Aktionsbereich auf Geltungsbereich bearbeiten. Ändern Sie den Namen und die Beschreibung sowie die Objekttypen und Objekte nach Bedarf.
- Zum Löschen eines Geltungsbereichs wählen Sie diesen im mittleren Bereich aus und klicken Sie im Aktionsbereich auf Geltungsbereich löschen. Bestätigen Sie die Löschung.

Erstellen von Berichten

Sie können zwei Arten delegierter Administrationsberichte erstellen:

- Einen HTML-Bericht, der die Rollen-/Geltungsbereichspaare, die einem Administrator zugeordnet sind, sowie die einzelnen Berechtigungen für jeden Objekttyp (z. B. Bereitstellungsgruppen, und Maschinenkataloge) enthält. Sie generieren diesen Bericht in Studio.
  Zum Erstellen dieses Berichts klicken Sie im Navigationsbereich auf Konfiguration > Administratoren. Wählen Sie im mittleren Bereich einen Administrator aus, und klicken Sie dann im Aktionsbereich auf Bericht erstellen.

  Sie können diesen Bericht auch beim Erstellen, Kopieren oder Bearbeiten eines Administrators anfordern.

- HTML- oder CSV Bericht, in dem alle integrierten benutzerdefinierten Rollen und Berechtigungen zugeordnet sind. Sie generieren diesen Bericht durch Ausführen des PowerShell-Skripts "OutputPermissionMapping.ps1".
  Um dieses Skript auszuführen, müssen Sie ein Volladministrator, ein Lesezugriffadministrator oder ein benutzerdefinierter Administrator mit der Berechtigung zum Lesen von Rollen sein. Das Skript befindet sich in: Programme\Citrix\DelegatedAdmin\SnapIn\Citrix.DelegatedAdmin.Admin.V1\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	Zielspeicherort für die Ausgabe. Standard = stdout
-AdminAddress	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.
	Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer und OutVariable. Weitere Informationen finden Sie in der Dokumentation von Microsoft.

Mit dem Befehl im folgenden Beispiel wird eine HTML-Tabelle in eine Datei namens Roles.html geschrieben und die Tabelle in einem Webbrowser geöffnet.
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\ Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1" -Path Roles.html –Show
Mit dem Befehl im folgenden Beispiel wird eine CSV-Tabelle in eine Datei namens Roles.csv geschrieben. Die Tabelle wird nicht angezeigt.
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\ Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1" –CSV -Path Roles.csv
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"

Smartcards

Feb 29, 2016

Die Smartcardauthentifizierung wird bei Beachtung der hier beschriebenen Richtlinien unterstützt.

Mehrere Smartcards und mehrere Leser können an dem gleichen Benutzergerät verwendet werden, wenn jedoch Passthrough-Authentifizierung verwendet wird, kann nur eine Smartcard eingesteckt werden, wenn der Benutzer einen virtuellen Desktop oder eine virtuelle Anwendung startet. Wenn eine Smartcard innerhalb einer Anwendung verwendet wird (z. B. zur digitalen Signierung oder für Verschlüsselungsfunktionen), werden Sie möglicherweise mehrmals zum Einlegen einer Smartcard oder zur Eingabe einer PIN-Nummer aufgefordert. Dieser Fall kann eintreten, wenn eine oder mehrere Smartcards gleichzeitig eingelegt wurden. Wenn Benutzer zum Einlegen einer Smartcard aufgefordert werden und diese sich bereits im Leser befindet, sollten sie auf Abbrechen klicken. Wenn sie zur Eingabe der PIN-Nummer aufgefordert werden, sollten sie diese erneut eingeben.

Wenn Sie gehostete Anwendungen unter Windows Server 2008 oder 2008 R2 und mit Smartcards verwenden, die den Microsoft-Kryptografiedienstanbieter für Basissmartcards benötigen, werden im Fall der Ausführung einer Smartcard-Transaktion alle anderen Benutzer, die eine Smartcard bei der Anmeldung verwendet haben, blockiert. Weitere Details und einen Hotfix zur Behebung dieses Problems finden Sie unter http://support.microsoft.com/kb/949538.

Ihre Organisation hat möglicherweise bestimmte Sicherheitsrichtlinien in Bezug auf die Verwendung von Smartcards. Mit diesen Richtlinien wird z. B. festgelegt, wie Smartcards ausgegeben werden und wie diese von Benutzern gesichert werden sollten. Einige Aspekte dieser Richtlinien müssen ggf. in einer XenApp- bzw. XenDesktop-Umgebung neu bewertet werden.

Sie können PINs mit einem Kartenverwaltungsprogramm oder einem Herstellerdienstprogramm zurücksetzen.

Die Unterstützung von Smartcards umfasst außerdem Komponenten, die über Citrix Partner bezogen werden können. Diese werden von den jeweiligen Partnern aktualisiert und in den vorliegenden Dokumenten nicht erläutert. Weitere Informationen finden Sie unter http://www.citrix.com/ready/.

Anforderungen

Unterstützung für Smartcardleser:

- Smartcardleser vom Typ ZKA (Zentraler Kreditausschuss) Klasse 1, die USB Chip-/CCID-konform (Smart Card Interface Devices) sind, werden unterstützt. Diese enthalten einen Schlitz, in den die Smartcard eingeführt wird. Andere Klassen, einschließlich Klasse 2 (Leser mit Tastatur für die Eingabe von PINs) und kontaktlose Leser werden nicht unterstützt.
- Virtuelle Smartcards, die auf Microsoft Windows Trusted Platform Module basieren, werden auf Benutzergeräten mit Receiver für Windows 4.3 und Windows 10 oder 8 unterstützt. XenApp- und XenDesktop-Versionen vor Version 7.6 FP3 unterstützen keine virtuellen Smartcards. Weitere Informationen über virtuelle Smartcards finden Sie unter Virtual Smart Card Overview im Microsoft Windows TechCenter.
- Installieren Sie für den Smartcardleser einen Gerätetreiber auf dem Benutzergerät. Viele Smartcardleser können mit dem von Microsoft bereitgestellten CCID-Gerätetreiber benutzt werden.
- Beziehen Sie einen Gerätetreiber und Kryptografiedienstanbietersoftware (CSP) vom Smartcard-Hersteller und installieren Sie beides auf Benutzergeräten und auf virtuellen Desktops. Der Treiber und die CSP-Software müssen mit XenApp bzw. XenDesktop kompatibel sein (Informationen zur Kompatibilität enthält die Dokumentation).

Important

Installieren von Treiber und CSP-Software vor der Installation von Citrix Software

- Citrix empfiehlt, dass Sie die Treiber vor der Installation von Citrix Software auf einem physischen Computer installieren und testen.
- Für virtuelle Desktops unter Windows 7 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.

Remote-PC-Zugriff mit Smartcards:

- Smartcards werden nur für den Remotezugriff auf physische Büro-PCs mit Windows 10, Windows 8 oder Windows 7 unterstützt; Smartcards werden nicht für Büro-PCs mit Windows XP unterstützt.
- Die folgenden Smartcards wurden mit Remote-PC-Zugriff getestet:
  - Gemalto .NET v2+ mit Gemalto .NET-Minitreiber
  - NIST PIV-Karten mit ActivIdentity ActivClient 6.2
  - NIST PIV-Karten mit dem Microsoft-Minitreiber
  - CAC-Karten mit ActivIdentity ActivClient 6.2
  - virtuelle Smartcards mit nativem Microsoft-Treiber

Auf Benutzergeräten muss Citrix Receiver, geeignete Middleware und eines der folgenden Betriebssysteme ausgeführt werden: Windows 7 oder Windows 8 (einschließlich Embedded Edition), 32 Bit und 64 Bit.

Middleware:

- Die Smartcard-Unterstützung in Receiver basiert auf dem PC/SC-Standard (Personal Computer/Smart Card) von Microsoft. Als Mindestanforderung müssen Smartcards und Smartcardleser vom zu Grunde 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.
- 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**
ActivClient 7.0 (DoD-Modus aktiviert)	DoD CAC-Karte
ActivClient 7.0 im Modus PIV	NIST PIV-Karte
Microsoft-Minitreiber	NIST PIV-Karte
GemAlto-Minitreiber für .NET-Karte	GemAlto .NET v2+
nativer Microsoft-Treiber	virtuelle Smartcards (TPM)

Führen Sie vor dem Bereitstellen von Smartcards folgende Schritte aus:

- Fügen Sie die Citrix Receiver für Web-URL der Liste der vertrauenswürdigen Sites für Benutzer hinzu, die mit Smartcards im Internet Explorer unter Windows 10 arbeiten. In Windows 10 wird Internet Explorer für vertrauenswürdige Sites nicht standardmäßig im geschützten Modus ausgeführt.
- Stellen Sie sicher, dass die Public Key-Infrastruktur entsprechend konfiguriert ist. Hierzu gehört, dass die Zertifikat-zu-Konto-Zuordnung richtig für die Active Directory-Umgebung konfiguriert ist, und dass die Validierung des Benutzerzertifikats ausgeführt werden kann.
- Konfigurieren Sie die Komponenten, die TLS 1.0 verwenden, für die Smartcard-Anmeldung.
- Stellen Sie sicher, dass die Bereitstellung die Systemanforderungen der anderen Citrix Komponenten erfüllt, die mit Smartcards verwendet werden, u. a. Receiver und StoreFront.
- Stellen Sie sicher, dass auf die folgenden Server in der Site Zugriff besteht:
  - Active Directory-Domänencontroller für das Benutzerkonto mit zugeordnetem Anmeldezertifikat auf der Smartcard
  - Delivery Controller
  - Citrix StoreFront
  - Citrix NetScaler Gateway/Citrix Access Gateway 10.x
  - Virtual Delivery Agent
  - Optional für Remotezugriff: Microsoft Exchange Server
- Sie müssen mit der Smartcard-Technik im Allgemeinen und im Besonderen mit der von Ihnen gewählten Technik und dem SDK vertraut sein. Informieren Sie sich auch über die Installation und Pflege von Zertifikaten in verteilten Umgebungen.

Aktivieren der Smartcard-Verwendung

1. Aktivieren Sie das Produkt für die Verwendung von Smartcards.
   1. Geben Sie die Smartcards an die Benutzer aus und berücksichtigen Sie dabei die Kartenausstellungsrichtlinie.
   2. Optional: Richten Sie Smartcards ein, damit Benutzer Remote-PC-Zugriff verwenden können.
   3. Installieren und konfigurieren Sie den Delivery Controller und StoreFront (falls nicht bereits für Smartcardremoting installiert).
2. Aktivieren Sie StoreFront für die Verwendung mit Smartcard. Einzelheiten finden Sie unter
   — Konfigurieren der Smartcardauthentifizierung
   in der StoreFront-Dokumentation.
3. Aktivieren Sie NetScaler Gateway/Access Gateway für die Verwendung mit Smartcard. Einzelheiten finden Sie unter
   — Configuring Authentication and Authorization
   und
   — Configuring Smart Card Access with the Web Interface
   in der NetScaler-Dokumentation.
4. Aktivieren Sie den Virtual Delivery Agent (VDA) für die Verwendung mit Smartcard.
   1. Stellen Sie sicher, dass der Virtual Delivery Agent die erforderlichen Anwendungen und Updates hat.
   2. Installieren Sie die Middleware.
   3. Richten Sie Smartcardremoting ein, damit die Kommunikation von Smartcarddaten zwischen Receiver auf einem Benutzergerät und einer virtuellen Desktopsitzung möglich ist.
5. 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.
   1. Importieren Sie das Zertifizierungsstellen-Stammzertifikat und das Zertifikat der ausstellenden Zertifizierungsstelle in den Schlüsselspeicher des Geräts.
   2. Installieren Sie die kryptografische Middleware.
   3. Installieren und konfigurieren Sie Citrix Receiver für Windows. Stellen Sie sicher, dass Sie icaclient.adm mit der Gruppenrichtlinien-Verwaltungskonsole importieren und die Smartcard-Authentifizierung aktivieren.

6. 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 Receiver).

Smartcardbereitstellungen

Feb 29, 2016

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.

Eingabe	Verbindung mit StoreFront
Lokale in Domänen eingebundene Computer	Direkte Verbindung
Remotezugriff von in Domänen eingebundenen Computern	Verbindung über NetScaler Gateway
Nicht in Domänen eingebundene Computer	Direkte Verbindung
Remotezugriff von nicht in Domänen eingebundenen Computern	Verbindung über NetScaler Gateway
Nicht in Domänen eingebundene Computer und Thin Clients mit Zugriff auf die Desktopgerätesite	Verbindung über Desktopgerätesites
In Domänen eingebundene Computer und Thin Clients mit Zugriff auf StoreFront über die XenApp Services-URL	Verbindung über XenApp Services-URLs

Die Bereitstellungstypen werden durch die Merkmale des Benutzergeräts definiert, mit dem der Smartcardleser verbunden ist:

- In Domäne eingebundenes Gerät oder nicht in Domäne eingebundenes Gerät
- Art der Verbindung zwischen Gerät und StoreFront
- Zur Anzeige der virtuellen Desktops und Anwendungen verwendete Software

Darüber hinaus können smartcardfähige Anwendungen wie Microsoft Word oder Microsoft Excel in diesen Bereitstellungen verwendet werden. In diesen Anwendungen können Benutzer Dokumente digital signieren und verschlüsseln.

Bimodale Authentifizierung

Soweit in der jeweiligen Bereitstellung möglich, unterstützt Receiver die bimodale Authentifizierung, d. h. der Benutzer hat die Wahl, sich mit einer Smartcard oder mit dem Benutzernamen und Kennwort anzumelden. Dies ist nützlich, wenn die Smartcard nicht verwendet werden kann (z. B. sie wurde vom Benutzer zu Hause vergessen oder das Zertifikat ist abgelaufen).

Da Benutzer nicht domänengebundener Geräte sich direkt an Receiver für Windows anmelden, können Sie für diese Benutzer ein Fallback auf die explizite Authentifizierung aktivieren. Wenn Sie die bimodale Authentifizierung konfigurieren, müssen sich Benutzer zuerst mit den Smartcards und PINs anmelden; sie können aber die explizite Authentifizierung auswählen, wenn sie Probleme mit den Smartcards haben.

Wenn Sie NetScaler Gateway bereitstellen, melden sich Benutzer an den Geräten an und werden von Receiver für Windows zur Authentifizierung bei NetScaler Gateway aufgefordert. Dies gilt sowohl für in Domänen eingebundene Geräte als auch

für Geräte, die nicht in Domänen eingebunden sind. Benutzer können sich bei NetScaler Gateway mit Smartcard und PIN oder mit expliziten Anmeldeinformationen anmelden. Sie können dann Benutzern die bimodale Authentifizierung für Anmeldungen an NetScaler Gateway bereitstellen. Konfigurieren Sie die Passthrough-Authentifizierung von NetScaler Gateway an StoreFront und delegieren Sie die Validierung der Anmeldeinformationen für Smartcardbenutzer an NetScaler Gateway, sodass Benutzer automatisch bei StoreFront authentifiziert werden.

Überlegungen zu mehreren Active Directory-Gesamtstrukturen

In einer Citrix Umgebung werden Smartcards in einer einzelnen Gesamtstruktur unterstützt. Strukturübergreifende Smartcard-Anmeldungen erfordern eine direkte bidirektionale Gesamtstruktur-Vertrauensstellung für alle Benutzerkonten. Komplexere Mehrfachstruktur-Bereitstellungen mit Smartcards (d. h. Vertrauensstellungen sind nur unidirektional oder sonstiger Art) werden nicht unterstützt.

Sie können Smartcards in einer Citrix Umgebung mit Remotedesktops verwenden. Dieses Feature kann lokal installiert werden (auf dem Benutzergerät, mit dem die Smartcard verbunden ist) oder remote (auf dem Remotedesktop, mit dem das Benutzergerät verbunden wird).

Richtlinie zum Entfernen der Smartcard

Die Richtlinie zum Entfernen der Smartcard legt fest, was passiert, wenn die Smartcard während einer Sitzung entfernt wird. Die Richtlinie zum Entfernen der Smartcard wird im Windows-Betriebssystem konfiguriert und verarbeitet.

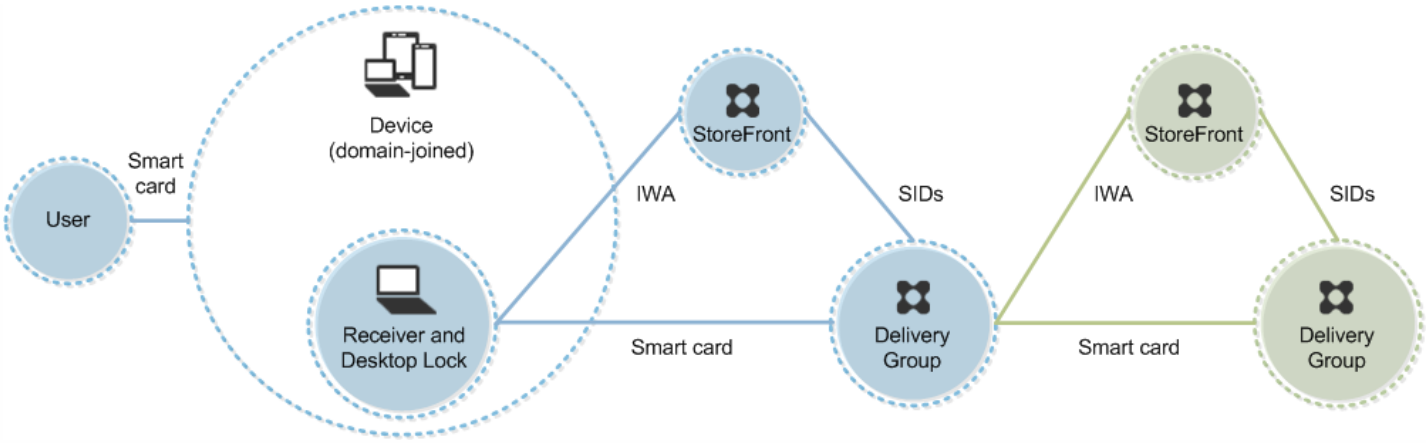
Richtlinieneinstellung	**Desktop-Verhalten**
Keine Aktion	Keine Aktion.
Arbeitsstation sperren	Die Desktopsitzung wird getrennt und der virtuelle Desktop gesperrt.
Abmeldung erzwingen	Der Benutzer wird zur Abmeldung gezwungen. Wenn die Netzwerkverbindung unterbrochen ist und diese Einstellung aktiviert wird, wird die Sitzung möglicherweise abgemeldet und der Benutzer verliert Daten.
Trennen bei einer Remotedienstesitzung	Die Sitzung wird getrennt und der virtuelle Desktop gesperrt.

Überprüfen der Zertifikatsperrlisten

Wenn die Überprüfung von Zertifikatsperrlisten aktiviert ist und ein Benutzer führt eine Smartcard mit einem ungültigen Zertifikat in einen Smartcardleser ein, kann der Benutzer nicht authentifiziert werden oder nicht auf den mit dem Zertifikat verbundenen Desktop oder die Anwendung zugreifen. Bei einem ungültigen Zertifikat für die E-Mail-Entschlüsselung bleibt die E-Mail beispielsweise verschlüsselt. Wenn andere Zertifikate auf der Smartcard, z. B. solche, die für die Authentifizierung verwendet werden, noch gültig sind, bleiben diese Funktionen weiterhin aktiv.

Bereitstellungsbeispiel: in Domänen eingebundene Computer

Diese Bereitstellung bezieht sich auf in Domänen eingebundene Benutzergeräte mit Desktop Viewer und Direktverbindung mit StoreFront.

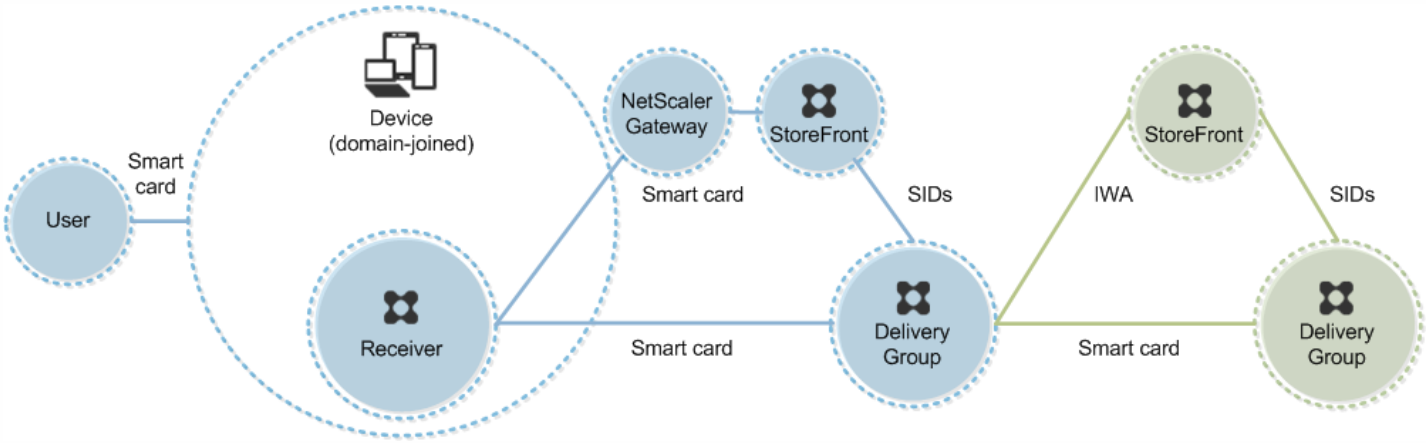


Zum Anmelden beim Gerät benötigt der Benutzer eine Smartcard und eine PIN. Der Benutzer wird dann durch Receiver beim Storefront-Server mittels integrierter Windows-Authentifizierung (IWA) authentifiziert. StoreFront übergibt die Sicherheits-IDs (SIDs) an XenApp bzw. XenDesktop. Wenn der Benutzer einen virtuellen Desktop oder eine Anwendung startet, wird er nicht aufgefordert, die PIN neu einzugeben, da in Receiver das Feature "Single Sign-On" konfiguriert ist.

Diese Bereitstellung kann um einen zweiten StoreFront-Server und einen Server mit gehosteten Anwendungen auf ein Double-Hop-System erweitert werden. Ein Receiver auf dem virtuellen Desktop übernimmt die Authentifizierung beim zweiten StoreFront-Server. Für diese zweite Verbindung kann eine beliebige Authentifizierungsmethode verwendet werden. Die für den ersten Hop dargestellte Konfiguration kann im zweiten Hop wiederverwendet oder nur für den zweiten Hop verwendet werden.

Bereitstellungsbeispiel: Remotezugriff von in Domänen eingebundenen Computern

Diese Bereitstellung bezieht sich auf in Domänen eingebundene Benutzergeräte mit Desktop Viewer und Verbindung mit StoreFront über NetScaler Gateway/Access Gateway.



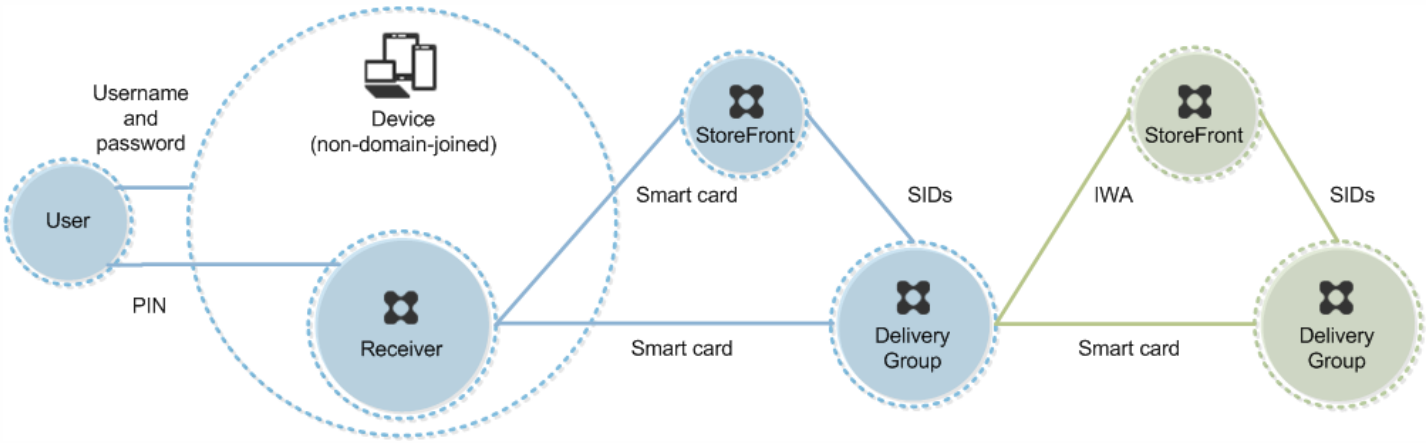
Der Benutzer meldet sich mit Smartcard und PIN beim Gerät und anschließend erneut bei NetScaler Gateway oder Access Gateway an. Die zweite Anmeldung kann entweder mit Smartcard und PIN oder einem Benutzernamen und einem Kennwort erfolgen, da Receiver in dieser Bereitstellung eine bimodale Authentifizierung zulässt.

Der Benutzer wird automatisch bei StoreFront angemeldet; StoreFront übergibt die Sicherheits-IDs (SIDs) an XenApp bzw. XenDesktop. Wenn der Benutzer einen virtuellen Desktop oder eine Anwendung startet, wird er nicht aufgefordert, die PIN neu einzugeben, da in Receiver das Feature "Single Sign-On" konfiguriert ist.

Diese Bereitstellung kann um einen zweiten StoreFront-Server und einen Server mit gehosteten Anwendungen auf ein Double-Hop-System erweitert werden. Ein Receiver auf dem virtuellen Desktop übernimmt die Authentifizierung beim zweiten StoreFront-Server. Für diese zweite Verbindung kann eine beliebige Authentifizierungsmethode verwendet werden. Die für den ersten Hop dargestellte Konfiguration kann im zweiten Hop wiederverwendet oder nur für den zweiten Hop verwendet werden.

Bereitstellungsbeispiel: nicht in Domänen eingebundene Computer

Diese Bereitstellung bezieht sich auf nicht in Domänen eingebundene Benutzergeräte mit Desktop Viewer und Direktverbindung mit StoreFront.



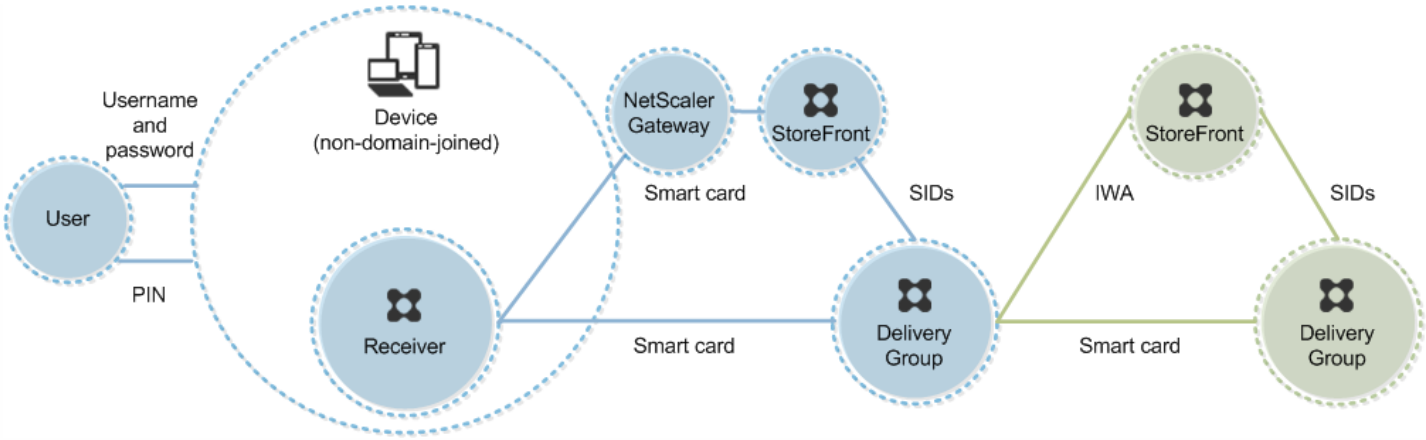
Ein Benutzer meldet sich beim Gerät an. Normalerweise muss er seinen Benutzernamen und das Kennwort eingeben, aber da das Gerät nicht Mitglied einer Domäne ist, sind die Anmeldeinformationen für diese Anmeldung optional. Da bimodale Authentifizierung in dieser Bereitstellung möglich ist, fordert Receiver den Benutzer auf, sich entweder mit Smartcard und PIN oder mit Benutzernamen und Kennwort anzumelden. Receiver authentifiziert dann bei StoreFront.

StoreFront übergibt die Sicherheits-IDs (SIDs) an XenApp bzw. XenDesktop. Wenn der Benutzer einen virtuellen Desktop oder eine Anwendung startet, wird er aufgefordert, die PIN neu einzugeben, da Single Sign-On in dieser Bereitstellung nicht verfügbar ist.

Diese Bereitstellung kann um einen zweiten StoreFront-Server und einen Server mit gehosteten Anwendungen auf ein Double-Hop-System erweitert werden. Ein Receiver auf dem virtuellen Desktop übernimmt die Authentifizierung beim zweiten StoreFront-Server. Für diese zweite Verbindung kann eine beliebige Authentifizierungsmethode verwendet werden. Die für den ersten Hop dargestellte Konfiguration kann im zweiten Hop wiederverwendet oder nur für den zweiten Hop verwendet werden.

Bereitstellungsbeispiel: Remotezugriff von nicht in Domänen eingebundenen Computern

Diese Bereitstellung bezieht sich auf nicht in Domänen eingebundene Benutzergeräte mit Desktop Viewer und Direktverbindung mit StoreFront.



Ein Benutzer meldet sich beim Gerät an. Normalerweise muss er seinen Benutzernamen und das Kennwort eingeben, aber da das Gerät nicht Mitglied einer Domäne ist, sind die Anmeldeinformationen für diese Anmeldung optional. Da bimodale Authentifizierung in dieser Bereitstellung möglich ist, fordert Receiver den Benutzer auf, sich entweder mit Smartcard und PIN oder mit Benutzernamen und Kennwort anzumelden. Receiver authentifiziert dann bei StoreFront.

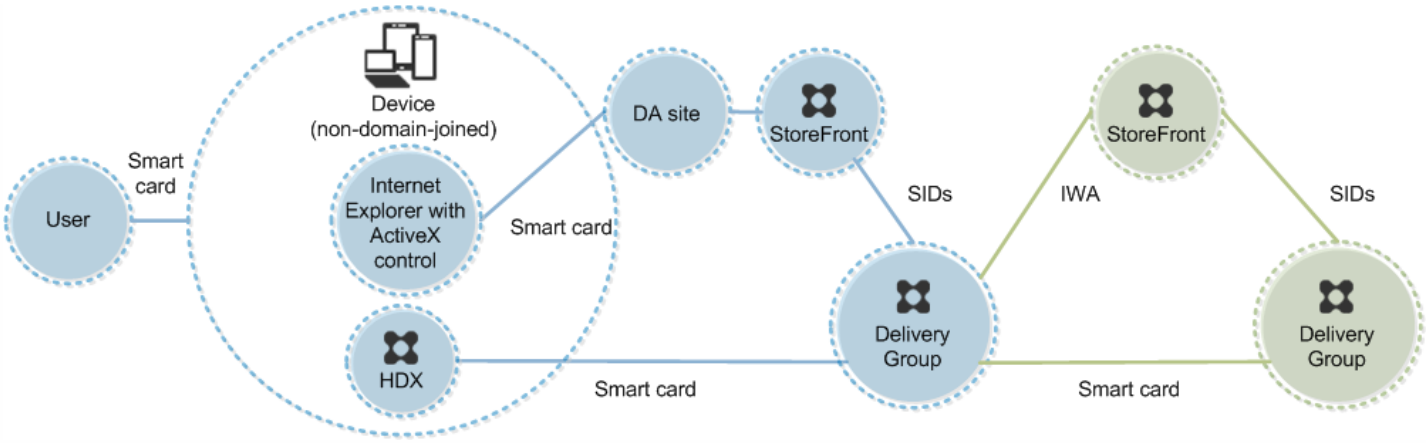
StoreFront übergibt die Sicherheits-IDs (SIDs) an XenApp bzw. XenDesktop. Wenn der Benutzer einen virtuellen Desktop oder eine Anwendung startet, wird er aufgefordert, die PIN neu einzugeben, da Single Sign-On in dieser Bereitstellung nicht verfügbar ist.

Diese Bereitstellung kann um einen zweiten StoreFront-Server und einen Server mit gehosteten Anwendungen auf ein Double-Hop-System erweitert werden. Ein Receiver auf dem virtuellen Desktop übernimmt die Authentifizierung beim zweiten StoreFront-Server. Für diese zweite Verbindung kann eine beliebige Authentifizierungsmethode verwendet werden. Die für den ersten Hop dargestellte Konfiguration kann im zweiten Hop wiederverwendet oder nur für den zweiten Hop verwendet werden.

Bereitstellungsbeispiel: nicht in Domänen eingebundene Computer und Thin Clients mit Zugriff auf die Desktopgerätesite

Diese Bereitstellung bezieht sich auf nicht in Domänen eingebundene Benutzergeräte, auf denen möglicherweise Desktop Lock ausgeführt wird und die mit StoreFront über Desktopgerätesites verbunden werden.

Desktop Lock ist eine eigenständige Komponente, die mit XenApp, XenDesktop und VDI-in-a-Box auf den Markt gebracht wurde. Das Programm ist eine Alternative zu Desktop Viewer und wird hauptsächlich für umfunktionierte Windows-Computer und Thin Clients verwendet. Desktop Lock ersetzt die Windows-Shell und Task-Manager bei diesen Benutzergeräten, wodurch der Benutzerzugriff auf die zugrunde liegenden Geräte verhindert wird. Mit Desktop Lock können Benutzer auf Desktops von Windows-Servermaschinen und Windows-Desktopmaschinen zugreifen. Die Installation von Desktop Lock ist optional.



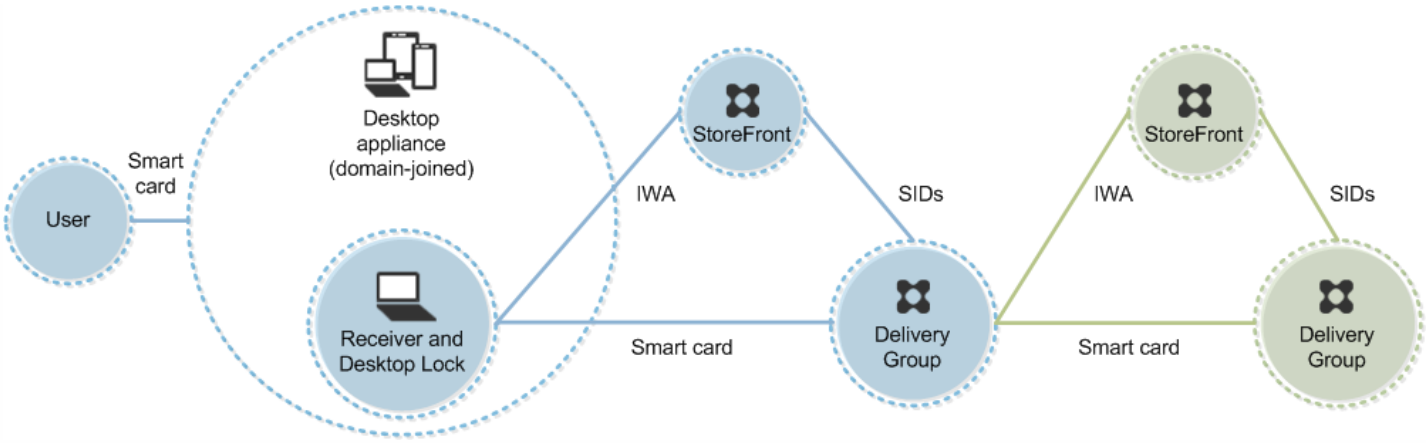
Zum Anmelden beim Gerät benötigt der Benutzer eine Smartcard. Wenn Desktop Lock auf dem Gerät ausgeführt wird, wird das Gerät so konfiguriert, dass eine Desktopgerätesite über Internet Explorer im Kioskmodus gestartet wird. Der Benutzer wird durch ein ActiveX-Steuerelement der Site aufgefordert, seine PIN einzugeben, die dann an StoreFront gesendet wird. StoreFront übergibt die Sicherheits-IDs (SIDs) an XenApp bzw. XenDesktop. Der erste verfügbare Desktop in der alphabetischen Liste einer zugewiesenen Desktopgruppe wird gestartet.

Diese Bereitstellung kann um einen zweiten StoreFront-Server und einen Server mit gehosteten Anwendungen auf ein Double-Hop-System erweitert werden. Ein Receiver auf dem virtuellen Desktop übernimmt die Authentifizierung beim zweiten StoreFront-Server. Für diese zweite Verbindung kann eine beliebige Authentifizierungsmethode verwendet werden. Die für den ersten Hop dargestellte Konfiguration kann im zweiten Hop wiederverwendet oder nur für den zweiten Hop verwendet werden.

Bereitstellungsbeispiel: in Domänen eingebundene Computer und Thin Clients mit Zugriff auf StoreFront über die XenApp Services-URL

Diese Bereitstellung bezieht sich auf in Domänen eingebundene Benutzergeräte, auf denen Desktop Lock ausgeführt wird und die mit StoreFront über XenApp Services-URLs verbunden werden.

Desktop Lock ist eine eigenständige Komponente, die mit XenApp, XenDesktop und VDI-in-a-Box auf den Markt gebracht wurde. Das Programm ist eine Alternative zu Desktop Viewer und wird hauptsächlich für umfunktionierte Windows-Computer und Thin Clients verwendet. Desktop Lock ersetzt die Windows-Shell und Task-Manager bei diesen Benutzergeräten, wodurch der Benutzerzugriff auf die zugrunde liegenden Geräte verhindert wird. Mit Desktop Lock können Benutzer auf Desktops von Windows-Servermaschinen und Windows-Desktopmaschinen zugreifen. Die Installation von Desktop Lock ist optional.



Zum Anmelden beim Gerät benötigt der Benutzer eine Smartcard und eine PIN. Wenn Desktop Lock auf dem Gerät ausgeführt wird, wird der Benutzer beim Storefront-Server über die integrierte Windows-Authentifizierung (IWA) authentifiziert. StoreFront übergibt die Sicherheits-IDs (SIDs) an XenApp bzw. XenDesktop. Wenn der Benutzer einen virtuellen Desktop startet, wird er nicht aufgefordert, die PIN neu einzugeben, da in Receiver Single Sign-On konfiguriert ist.

Diese Bereitstellung kann um einen zweiten StoreFront-Server und einen Server mit gehosteten Anwendungen auf ein Double-Hop-System erweitert werden. Ein Receiver auf dem virtuellen Desktop übernimmt die Authentifizierung beim zweiten StoreFront-Server. Für diese zweite Verbindung kann eine beliebige Authentifizierungsmethode verwendet werden. Die für den ersten Hop dargestellte Konfiguration kann im zweiten Hop wiederverwendet oder nur für den zweiten Hop verwendet werden.

Passthrough-Authentifizierung und Single Sign-On mit Smartcards

Feb 29, 2016

Passthrough-Authentifizierung

Die Passthrough-Authentifizierung mit Smartcards bei virtuellen Desktops wird auf Benutzergeräten unterstützt, auf denen Windows 10, Windows 8 und Windows 7 SP1, Enterprise und Professional Editionen ausgeführt werden.

Die Passthrough-Authentifizierung mit Smartcards bei gehosteten Anwendungen wird auf Servern unterstützt, auf denen Windows Server 2008 und Windows Server 2012 ausgeführt werden.

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 unter
— Konfigurieren des Authentifizierungsdiensts
in der StoreFront-Dokumentation.

Single Sign-On

Single Sign-On ist ein Citrix Feature, mit dem die Passthrough-Authentifizierung in Starts von virtuellen Desktops und Anwendungen implementiert wird. Sie können dieses Feature bei Smartcardbereitstellungen verwenden, die in Domänen eingebunden und direkt mit StoreFront verbunden sind, sowie bei in Domänen eingebundenen und über NetScaler mit StoreFront verbundenen Bereitstellungen. So müssen Benutzer ihre PIN weniger häufig eingeben. Zur die Verwendung von Single Sign-On in diesen Bereitstellungstypen bearbeiten Sie die folgenden Parameter in der Datei default.ica, die sich auf dem StoreFront-Server befindet:

- In Domänen eingebundene, direkt mit StoreFront verbundene Smartcardbereitstellungen: Einstellung für DisableCtrlAltDel auf Off
- In Domänen eingebundene, über NetScaler mit StoreFront verbundene Smartcardbereitstellungen: Einstellung für UseLocalUserAndPassword auf On

Weitere Anweisungen zum Einrichten dieser Parameter finden Sie in der Dokumentation für StoreFront oder NetScaler Gateway.

Die Verfügbarkeit der Single Sign-On-Funktion hängt von vielen Faktoren ab, u. a.:

- Sicherheitsrichtlinien für Single Sign-On der jeweiligen Organisation
- Typ und Konfiguration der Middleware
- Typen der Smartcardleser
- Richtlinie für das Zwischenspeichern von Middleware-PINs

Hinweis: Wenn Benutzer sich beim Virtual Delivery Agent (VDA) mit einer Maschine anmelden, an die ein Smartcardleser angeschlossen ist, wird möglicherweise eine Windows-Kachel angezeigt, die die letzte erfolgreiche Authentifizierungsmethode repräsentiert, z. B. Smartcard oder Kennwort. Daher wird bei aktiviertem Single Sign-On ggf. eine entsprechende Kachel angezeigt. Zum Anmelden müssen Benutzer Benutzer wechseln auswählen, um eine andere Kachel auszuwählen, da die Single Sign-On-Kachel nicht funktioniert.

Transport Layer Security (TLS)

Jul 22, 2016

Das Konfigurieren einer XenApp- oder XenDesktop-Site zur Verwendung des TLS-Sicherheitsprotokolls (Transport Layer Security) umfasst folgende Schritte:

- Rufen Sie ein Serverzertifikat ab und installieren und registrieren Sie es auf allen Delivery Controllern. Konfigurieren Sie zudem einen Port mit dem SSL-Zertifikat. Einzelheiten finden Sie unter Installieren von TLS-Serverzertifikaten auf Controllern.
  Sie können die Ports ändern, die der Controller zum Abhören von HTTP- und HTTPS-Datenverkehr verwendet.

- Aktivieren Sie TLS-Verbindungen zwischen Benutzern und Virtual Delivery Agents (VDAs) mit den folgenden Schritten:
  - Konfigurieren Sie TLS auf den Maschinen, auf denen die VDAs installiert sind. (Der Einfachheit halber werden nachfolgend Maschinen, auf denen VDAs installiert sind, als "VDAs" bezeichnet.) Sie können ein PowerShell-Skript von Citrix verwenden oder eine manuelle Konfiguration vornehmen. Allgemeine Informationen finden Sie unter TLS-Einstellungen auf VDAs. Detaillierte Informationen finden Sie unter Konfigurieren von auf einem VDA mit dem PowerShell-Skript und Manuelle Konfiguration von TLS auf einem VDA.
  - Konfigurieren Sie SSL in den Bereitstellungsgruppen, die die VDAs enthalten, indem Sie eine Reihe von PowerShell-Cmdlets in Studio ausführen. Einzelheiten finden Sie unter Konfigurieren von TLS auf Bereitstellungsgruppen.

  Anforderungen und Überlegungen:
  - Das Aktivieren von TLS-Verbindungen zwischen Benutzern und VDAs gilt nur für XenApp 7.6- und XenDesktop 7.6-Sites sowie für unterstützte höhere Releases.
  - Konfigurieren Sie TLS in den Bereitstellungsgruppen und auf den VDAs nach der Installation von Komponenten sowie nach dem Erstellen von Sites, Maschinenkatalogen und Bereitstellungsgruppen.
  - Zum Konfigurieren von TLS in den Bereitstellungsgruppen müssen Sie die Berechtigung zum Ändern der Zugriffsregeln für Controller haben; ein Volladministrator hat diese Berechtigung.
  - Zum Konfigurieren von TLS auf den VDAs müssen Sie ein Windows-Administrator auf der Maschine sein, auf der der VDA installiert ist.
  - Wenn Sie TLS auf VDAs konfigurieren möchten, für die ein Upgrade von einer früheren Version durchgeführt wurde, deinstallieren Sie die SSL-Relay-Software vor dem Upgrade von den Maschinen.
  - Das PowerShell-Skript konfiguriert TLS auf statischen VDAs, jedoch nicht auf gepoolten VDAs, die von Maschinenerstellungsdienste oder Provisioning Services bereitgestellt wurden und deren Maschinenimage bei jedem Neustart zurückgesetzt wird.

Beachten Sie Folgendes beim Arbeiten in der Windows-Registrierung:
Achtung: Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.
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. Nachfolgend finden Sie Anleitungen zum Abrufen eines Zertifikats und zur Installation und Registrierung auf einem Controller sowie zum Konfigurieren eines Ports mit dem SSL-Zertifikat:

- Wenn IIS auf dem Controller installiert ist, folgen Sie den Anleitungen unter https://technet.microsoft.com/en-us/library/cc771438%28v=ws.10%29.aspx.
- Wenn der Controller nicht über IIS verfügt, können Sie das Zertifikat mit folgender Methode konfigurieren:
  1. Rufen Sie ein SSL-Serverzertifikat ab und installieren Sie es auf dem Controller, wie unter http://blogs.technet.com/b/pki/archive/2009/08/05/how-to-create-a-web-server-ssl-certificate-manually.aspx beschrieben. Weitere Informationen zum certreq-Tool finden Sie unter http://technet.microsoft.com/en-us/library/cc736326(WS.10).aspx.
     Wenn Sie TLS auf VDAs mit dem PowerShell-Skript konfigurieren und dabei den Fingerabdruck des SSL-Zertifikats nicht angeben, stellen Sie sicher, dass das Zertifikat im Zertifikatspeicher unter "Lokaler Computer > Eigene Zertifikate > Zertifikate" gespeichert ist. Wenn mehrere Zertifikate in dem Speicherort sind, wird das zuerst gefundene verwendet.
  2. Konfigurieren Sie einen Port mit dem Zertifikat. Weitere Informationen finden Sie unter http://msdn.microsoft.com/en-us/library/ms733791%28v=vs.110%29.aspx.

Ändern von HTTP- oder HTTPS-Ports

Der XML-Dienst hört standardmäßig Port 80 auf HTTP-Datenverkehr und Port 443 auf HTTPS-Datenverkehr ab. Zwar können auch andere Ports verwendet werden, jedoch wird der Controller dabei nicht vertrauenswürdigen Netzwerken ausgeliefert, und es entsteht ein Sicherheitsrisiko. Das Bereitstellen eines eigenständigen StoreFront-Servers ist dem Ändern der Standardwerte vorzuziehen.
Zum Ändern der vom Controller verwendeten standardmäßigen HTTP- oder HTTPS-Ports führen Sie den folgenden Befehl in Studio aus: BrokerService.exe -WIPORT <http-port> -WISSLPORT <https-port>

<http-port> ist die Portnummer für HTTP-Datenverkehr und <https-port> ist die Portnummer für HTTPS-Datenverkehr.

Hinweis: Nachdem Sie einen Port geändert haben, zeigt Studio möglicherweise eine Meldung zu Lizenzkompatibilität und Upgrades an. Sie lösen das Problem, indem Sie Dienstinstanzen mit den folgenden PowerShell-Cmdlets neu registrieren:
Get-ConfigRegisteredServiceInstance -ServiceType Broker -Binding XML_HTTPS | Unregister-ConfigRegisteredServiceInstance Get-BrokerServiceInstance | where Binding -eq "XML_HTTPS" | Regist

Erzwingen von HTTPS-Datenverkehr

Wenn der XML-Dienst den HTTP-Datenverkehr ignorieren soll, legen Sie den folgenden Registrierungswert unter HKLM\Software\Citrix\DesktopServer\ auf dem Controller fest und starten Sie den Brokerdienst neu.

Um den HTTP-Datenverkehr zu ignorieren, legen Sie für XmlServicesEnableNonSsl 0 fest.

Es gibt einen entsprechenden Registrierungswert, damit der HTTPS-Datenverkehr ignoriert wird: XmlServicesEnableSsl. Stellen Sie sicher, dass er nicht auf 0 festgelegt ist.

TLS-Einstellungen auf VDAs

Wenn Sie TLS auf VDAs konfigurieren, werden Berechtigungen auf dem installierten SSL-Zertifikat geändert. Der ICA-Dienst erhält Lesezugriff für den privaten Schlüssel des Zertifikats und informiert den ICA-Dienst über Folgendes:

- **Das für TLS zu verwendende Zertifikat im Zertifikatspeicher**
- **Die für TLS-Verbindungen zu verwendende TCP-Portnummer**
  Die Windows-Firewall (wenn sie aktiviert ist) muss so konfiguriert sein, dass eingehende Verbindungen auf diesem TCP-Port zugelassen sind. Diese Konfiguration wird für Sie ausgeführt, wenn Sie das PowerShell-Skript verwenden.

- **Die zulässigen Versionen des TLS-Protokolls**

> Important

Citrix empfiehlt seinen Kunden 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. Weitere Informationen finden Sie unter CTX200238.

Die unterstützten SSL-Protokollversionen unterliegen einer Hierarchie (von der niedrigsten zur höchsten Version): TLS 3.0, TLS 1.0, TLS 1.1 und TLS 1.2. Wenn Sie die zulässige Mindestversion angeben, sind alle Protokollverbindungen, die diese Version oder eine höhere Version verwenden, zulässig.

Wenn Sie beispielsweise TLS 1.1 als Mindestversion angeben, werden auch TLS 1.1- und TLS 1.2-Protokollverbindungen zugelassen. Wenn Sie SSL 3.0 als Mindestversion angeben, sind Verbindungen für alle unterstützten Versionen zulässig. Wenn Sie TLS 1.2 als Mindestversion angeben, werden nur TLS 1.2-Verbindungen zugelassen.

- **Die zulässigen TLS-Verschlüsselungsverfahren**
  Eine Verschlüsselungssammlung ist eine Liste gebräuchlicher TLS-Verschlüsselungsverfahren. Wenn ein Client eine Verbindung herstellt und eine Liste unterstützter TLS-Verschlüsselungsverfahren übermittelt, ordnet der VDA ein Verschlüsselungsverfahren des Clients einem Verschlüsselungsverfahren in der konfigurierten Verschlüsselungssammlung zu und akzeptiert die Verbindung. Wenn der Client ein Verschlüsselungsverfahren übermittelt, das nicht in der Verschlüsselungssammlung des VDAs ist, lehnt der VDA die Verbindung ab.

  Drei Verschlüsselungssammlungen werden unterstützt: GOV (Government), COM (Commercial) und ALL. Die Verschlüsselungsverfahren in diesen Verschlüsselungssammlungen hängen vom Windows FIPS-Modus ab. Weitere Informationen zum Windows FIPS-Modus finden Sie unter http://support.microsoft.com/kb/811833. In der folgenden Tabelle finden Sie die für die jeweilige Verschlüsselungssammlung unterstützten Verschlüsselungsverfahren.

TLS-Verschlüsselungssammlung	GOV	COM	ALL	GOV	COM	ALL
FIPS-Modus	Off	Off	Off	On	On	On
RSA_KEYX	x	x	x	x	x	x
RSA_SIGN	x	x	x	x	x	x
3DES	x		x	x		x
RC4		x	x			
MD5	x	x	x			
SHA	x	x	x	x	x	x
SHA_256	x	x	x	x	x	x
SHA_384	x	x	x	x	x	x
SHA_512	x	x	x	x	x	x
AES	x	x	x	x	x	x

Eine Bereitstellungsgruppe darf nicht eine Mischung von VDAs mit und ohne konfiguriertem TLS enthalten. Wenn Sie TLS für eine Bereitstellungsgruppe konfigurieren, sollten Sie TLS bereits für alle VDAs in dieser Bereitstellungsgruppe konfiguriert haben.

Konfigurieren von TLS auf einem VDA mit dem PowerShell-Skript

Das Skript Enable-VdaSSL.ps1 aktiviert oder deaktiviert den TLS-Listener auf einem VDA. Dieses Skript ist im Ordner Support > Tools > SslSupport auf dem Installationsmedium verfügbar.

Wenn Sie TLS aktivieren, deaktiviert das Skript alle vorhandenen Windows-Firewallregeln für den angegebenen TCP-Port. Dann wird eine Regel hinzugefügt, die dem ICA-Dienst die Annahme eingehender Verbindungen nur auf dem TLS-TCP-Port gewährt. Außerdem werden die Windows-Firewallregeln für Folgendes deaktiviert:

- Citrix ICA (Standard: 1494)
- Citrix CGP (Standard: 2598)
- Citrix WebSocket (Standard: 8008)

Als Folge können Benutzer Verbindungen nur über TLS herstellen und nicht über unformatiertes ICA, CGP oder WebSocket.

Das Skript enthält die folgenden Syntax-Beschreibungen sowie zusätzliche Beispiele. Sie können diese Informationen mit einem Tool wie Notepad++ überprüfen.

Sie müssen einen der Parameter –Enable oder –Disable angeben, alle anderen Parameter sind optional.

Syntax

Enable-VdaSSL {-Enable | -Disable} [–SSLPort <port>] [-SSLMinVersion "<min-ssl-version>"] [-SSLCipherSuite"<suite>"] [-CertificateThumbPrint "<thumbprint>"]

Parameter	**Beschreibung**
-Enable	Installiert und aktiviert den TLS-Listener auf dem VDA. Dieser Parameter oder der Parameter –Disable ist erforderlich.
-Disable	Deaktiviert den TLS-Listener auf dem VDA. Dieser Parameter oder der Parameter –Enable ist erforderlich. Wenn Sie diesen Parameter festlegen, sind keine anderen Parameter gültig.
–SSLPort <port>	TLS port: Standard: 443

Parameter	Beschreibung
-SSLMinVersion "<min-ssl-version>"	Mindestversion des TLS-Protokolls zwischen Anführungszeichen. Gültige Werte: "SSL_3.0", "TLS_1.0", "TLS_1.1" und "TLS_1.2". Standard: "TLS_1.0" **Wichtig:** Citrix empfiehlt seinen Kunden 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. Weitere Informationen finden Sie unter CTX200238.
-SSLCipherSuite "<suite>"	TLS-Verschlüsselungssammlung zwischen Anführungszeichen. Gültige Werte: "GOV", "COM" und "ALL". Standard: "ALL"
-CertificateThumbPrint "<thumbprint>"	Fingerabdruck des SSL-Zertifikats im Zertifikatspeicher, zwischen Anführungszeichen. Dieser Parameter wird normalerweise verwendet, wenn der Zertifikatspeicher über mehrere Zertifikate verfügt. Das Skript verwendet den Fingerabdruck, um das gewünschte Zertifikat auszuwählen. Standard: das erste verfügbare Zertifikat im Bereich "Lokaler Computer > Eigene Zertifikate > Zertifikate" des Zertifikatspeicher.

Beispiele

Das folgende Skript installiert und aktiviert den TLS 1.2-Versionswert.

```
Enable-VdaSSL –Enable
```

Das folgende Skript installiert und aktiviert den TLS-Listener und gibt den TLS-Port 400 an sowie die Verschlüsselungssammlung GOV und als Mindestprotokollversion "TLS 1.2 TLS".

```
Enable-VdaSSL – Enable –SSLPort 400 'SSLMinVersion "TLS_1.2"  –SSLCipherSuite "GOV"
```

Das folgende Skript deaktiviert den TLS-Listener auf dem VDA.

```
Enable-VdaSSL –Disable
```

Manuelle Konfiguration von TLS auf einem VDA

Bei der manuellen Konfiguration von TLS auf einem VDA gewähren Sie dem privaten Schlüssel des TLS-Zertifikats allgemeinen Lesezugriff für den entsprechenden Dienst auf jedem VDA: NT SERVICE\PorticaService für einen VDA für Windows-Desktopbetriebssysteme oder NT SERVICE\TermService für einen VDA für Windows-Serverbetriebssysteme. Führen Sie auf der Maschine, auf der der VDA installiert ist, folgende Schritte aus:

1. Starten Sie die Microsoft Management Console (MMC): Start > Ausführen > mmc.exe.
2. Fügen Sie dem MMC das Zertifikat-Snap-In hinzu:
   1. Wählen Sie Datei > Snap-In hinzufügen/entfernen.
   2. Wählen Sie Zertifikate aus und klicken Sie 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.
3. Klicken Sie unter "Zertifikate (Lokaler Computer) > Eigene Zertifikate > Zertifikate" mit der rechten Maustaste auf das Zertifikat und wählen Sie Alle Aufgaben > Private Schlüssel verwalten.
4. Im Zugriffssteuerungslisten-Editor wird "Permissions for <Anzeigename> private keys" angezeigt, wobei <Anzeigename> der Name des SSL-Zertifikats ist. Fügen Sie einen der folgenden Dienste hinzu und geben Sie ihm Lesezugriff:
   - Für einen VDA für Windows-Desktopbetriebssysteme "PORTICASERVICE"
   - Für einen VDA für Windows-Serverbetriebssysteme "TERMSERVICE"
5. Doppelklicken Sie auf das installierte SSL-Zertifikat. Wählen Sie im Dialogfeld des Zertifikats die Registerkarte "Details" aus und führen Sie einen Bildlauf nach unten durch. Klicken Sie auf Fingerabdruck.
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 SSL-Zertifikats in den binären Wert. Sie können unbekannte Elemente im Dialogfeld Binärwert bearbeiten ignorieren (z. B. "0000" und Sonderzeichen).
   2. Bearbeiten Sie den Schlüssel "SSLEnabled" und ändern Sie den Wert für DWORD in "1". (Um SSL zu einem späteren Zeitpunkt zu deaktivieren, ändern Sie den Wert für DWORD in "0&".)
   3. Wenn Sie die Standardeinstellungen ändern möchten (optional), verwenden Sie Folgendes im gleichen Registrierungspfad:
      - SSLPort DWORD – SSL-Portnummer. Standard: 443.
      - SSLMinVersion DWORD – 1 = SSL 3.0, 2 = TLS 1.0, 3 = TLS 1.1, 4 = TLS 1.2. Standard: 2 (TLS 1.0).
      - SSLCipherSuite DWORD – 1 = GOV, 2 = COM, 3 = ALL. Standard: 3 (ALL).
7. Stellen Sie sicher, dass der TLS-TCP-Port in der Windows-Firewall geöffnet ist, wenn Sie nicht den Standardport 443 verwenden. (Wenn Sie die eingehende Regel für die Windows-Firewall erstellen, wählen Sie in den Eigenschaften die Optionen "Verbindung zulassen" und "Aktiviert" aus.)
8. Stellen Sie sicher, dass keine anderen Anwendungen oder Dienste (z. B. IIS) den TLS-TCP-Port verwenden.
9. Damit die Änderungen auf VDAs für Windows-Serverbetriebssysteme wirksam werden, starten Sie die Maschine neu. (Sie brauchen Maschinen mit VDAs für Windows-Desktopbetriebssysteme nicht neu starten.)

Konfigurieren von TLS auf Bereitstellungsgruppen

Führen Sie diese Schritte für jede Bereitstellungsgruppe aus, die VDAs enthält, die Sie für TLS-Verbindungen konfiguriert haben.

1. Öffnen Sie in Studio die PowerShell-Konsole.
2. Führen Sie asnp Citrix.* aus, um die Citrix Produkt-Cmdlets zu laden.
3. Führen Sie Get-BrokerAccessPolicyRule –DesktopGroupName '<delivery-group-name>' | Set-BrokerAccessPolicyRule –HdxSslEnabled $true aus.
   <delivery-group-name> ist der Name der Bereitstellungsgruppe mit den VDAs.
4. Führen Sie Set-BrokerSite –DnsResolutionEnabled $true aus.

Problembehandlung

Wenn ein Verbindungsfehler auftritt, überprüfen Sie Systemereignisprotokoll des VDAs.

Wenn Sie Citrix Receiver für Windows verwenden und ein Verbindungsfehler auftritt (z. B. 1030), der auf einen TLS-Fehler hinweist, deaktivieren Sie Desktop Viewer und versuchen Sie erneut, die Verbindung herzustellen. Der Verbindungsfehler tritt zwar immer noch auf, aber u. U. wird eine Erklärung zu dem zugrunde liegenden TLS-Fehler angegeben (z. B. dass Sie beim Anfordern eines Zertifikats von der Zertifizierungsstelle die falsche Vorlage angegeben haben).

Drucken

Feb 29, 2016

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.

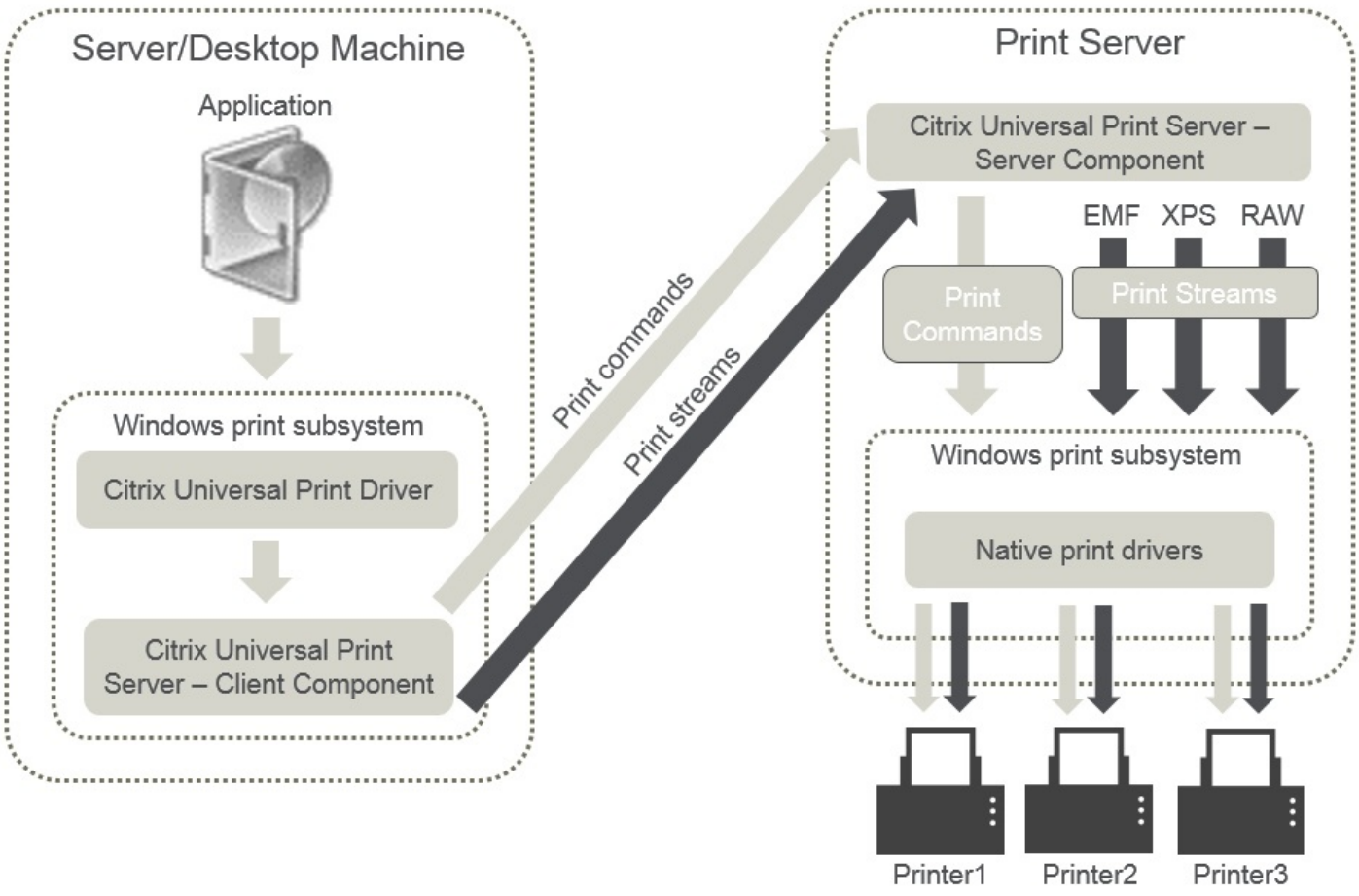
Die gängigsten Methoden der Druckerbereitstellung sind folgende:

- **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 Serverbetriebssystemmaschine und damit den Netzwerkdruck von jedem Gerät aus.
  Citrix empfiehlt den Einsatz des universellen Druckservers für Szenarios mit Remote-Druckerservern. Der universelle Druckserver überträgt den Druckauftrag über das Netzwerk in einem optimierten und komprimierten Format, wodurch der Netzwerkverkehr reduziert und die Benutzererfahrung verbessert wird.

  Der universelle Druckserver umfasst als Feature die folgenden Komponenten:
  - Clientkomponente "UPClient": Aktivieren Sie UPClient auf jeder Serverbetriebssystemmaschine, die Netzwerksitzungsdrucker bereitstellt und den universellen Druckertreiber verwendet.
  - Serverkomponente "UPServer": Installieren Sie UPServer auf jedem Druckserver, der Netzwerksitzungsdrucker bereitstellt und den universellen Druckertreiber für die Sitzungsdrucker verwendet (unabhängig davon, ob die Sitzungsdrucker zentral bereitgestellt werden).

  Informationen zu den Anforderungen und zum Setup des universellen Druckservers finden Sie in den Artikeln Systemanforderungen und Installation.

  Die folgende Abbildung zeigt den typischen Workflow eines Netzwerkdruckers in einer Umgebung mit universellem Druckserver.



Wenn Sie das Citrix Feature "Universeller Druckserver" aktivieren, wird es von allen verbundenen Netzwerkdruckern automatisch über Autodiscovery genutzt.

Hinweis: Der universelle Druckserver wird auch für VDI-in-a-Box 5.3 unterstützt. Informationen zur Installation des universellen Druckservers mit VDI-in-a-Box finden Sie in der Dokumentation zu VDI-in-a-Box.

- **Automatische Erstellung**: Dies bezieht sich auf Drucker, die automatisch zu Beginn jeder Sitzung erstellt werden. Sowohl Remotedrucker als auch lokal angeschlossene Drucker können automatisch erstellt werden. Bei Umgebungen mit einer großen Anzahl von Druckern pro Benutzer ist es u. U. besser, nur den Standarddrucker automatisch zu erstellen. Wenn weniger Drucker automatisch erstellt werden, entsteht auf den Serverbetriebssystemmaschinen weniger Mehraufwand (Arbeitsspeicher und CPU). Eine reduzierte Anzahl an automatisch erstellten Druckern kann auch die Anmeldedauer der Benutzer verkürzen.
  Automatisch erstellte Drucker basieren auf:

  - Den auf dem Benutzergerät installierten Druckern.
  - Den auf die Sitzung angewendeten Richtlinien.
    Durch Richtlinieneinstellungen für die automatische Erstellung können Sie Anzahl oder Art der automatisch erstellten Drucker beschränken. Standardmäßig sind die Drucker in Sitzungen verfügbar, wenn alle Drucker auf dem Benutzergerät automatisch konfiguriert werden, einschließlich der lokal angeschlossenen und der Netzwerkdrucker.

  Nachdem der Benutzer die Sitzung beendet, werden die Drucker für diese Sitzung gelöscht.

Mit der automatischen Erstellung von Client- und Netzwerkdruckern sind Wartungsarbeiten verbunden. Bei Hinzufügen eines Druckers muss beispielsweise auch Folgendes durchgeführt werden:

- Aktualisieren der Richtlinieneinstellung "Sitzungsdrucker"
- Hinzufügen des Treibers zu allen Serverbetriebssystemmaschinen über die Richtlinieneinstellung "Druckertreiberzuordnung und -kompatibilität"

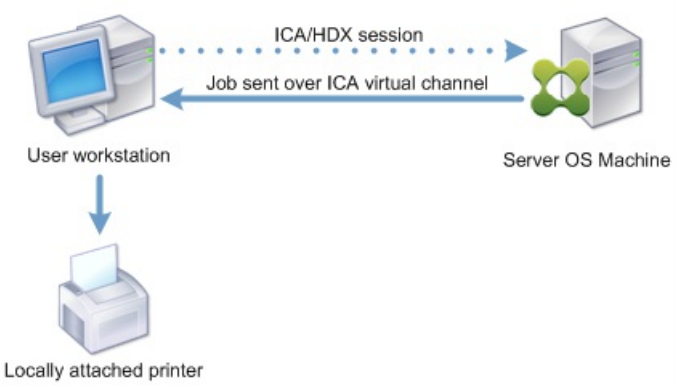
Weiterleiten von Druckaufträgen

Der Begriff Druckpfad umfasst den Pfad, über den Druckaufträge weitergeleitet werden, und den Speicherort, an dem Druckaufträge gespoolt werden. Beide Aspekte dieses Konzepts sind wichtig. Die Weiterleitung wirkt sich auf den Netzwerk-Datenverkehr aus. Das Spooling wirkt sich auf die Auslastung der lokalen Ressourcen an dem Gerät, das den Auftrag verarbeitet, aus.

In dieser Umgebung können Druckaufträge auf zwei Wegen zu einem Druckgerät gelangen: über den Client oder über einen Netzwerkdruckserver. Dafür werden die Bezeichnungen Clientdruckpfad und Netzwerkdruckpfad verwendet. Welcher Pfad standardmäßig ausgewählt wird, hängt vom verwendeten Drucker ab.

Lokal angeschlossene Drucker

Das System leitet Aufträge von der Serverbetriebssystemmaschine über den Client an den Drucker. Der Druckdatenverkehr wird über das ICA-Protokoll optimiert und komprimiert. Wenn ein Druckgerät lokal an das Benutzergerät angeschlossen ist, werden Druckaufträge über den virtuellen ICA-Kanal weitergeleitet.



Netzwerkdrucker

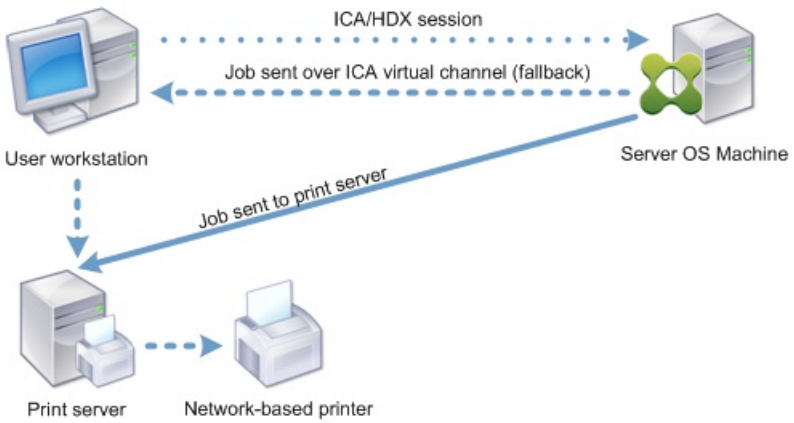
Standardmäßig werden alle für Netzwerkdrucker bestimmten Druckaufträge von der Serverbetriebssystemmaschine über das Netzwerk direkt an den Druckserver weitergeleitet. In folgenden Situationen werden jedoch Druckaufträge automatisch über die ICA-Verbindung geleitet:

- Wenn der virtuelle Desktop oder die Anwendung keine Verbindung mit dem Druckserver herstellen kann.
- Wenn der systemeigene Druckertreiber auf der Serverbetriebssystemmaschine nicht verfügbar ist.

Wenn der universelle Druckserver nicht aktiviert ist, empfiehlt sich die Konfiguration des Clientdruckpfads für den Netzwerkdruck bei Verbindungen mit geringer Bandbreite, z. B. WANs, die von der Optimierung und Komprimierung des Datenverkehrs beim Senden von Aufträgen über die ICA-Verbindung profitieren.

Der Clientdruckpfad ermöglicht auch die Begrenzung des Datenverkehrs oder der für Druckaufträge zugeordneten Bandbreite. Wenn die Auftragsleitung über das Benutzergerät nicht möglich ist, z. B. bei Thin Clients ohne Druckerfunktionen, muss die Servicequalität so konfiguriert werden, dass ICA/HDX-Verkehr Vorrang hat und eine gute

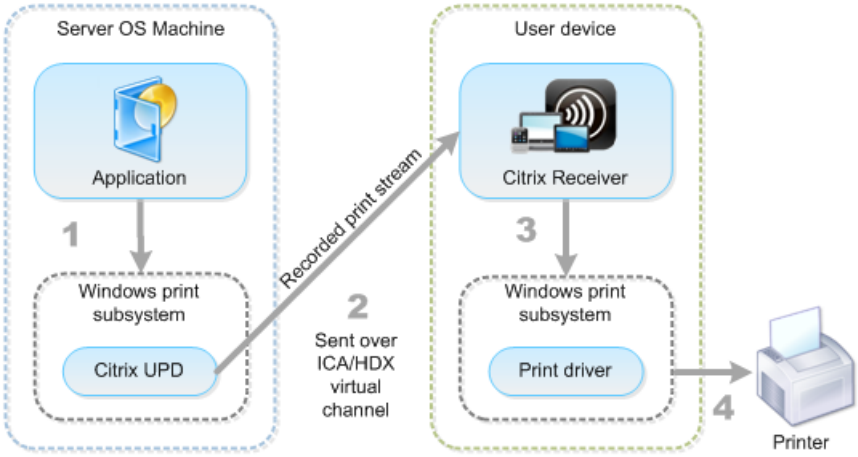
Benutzererfahrung bei der Sitzung gewährleistet ist.



Druckertreiberverwaltung

Zur Vereinfachung der Druckprozesse in dieser Umgebung empfiehlt Citrix die Verwendung des universellen Citrix Druckertreibers. Der universelle Druckertreiber ist ein geräteunabhängiger, für jedes Druckgerät geeigneter Treiber. Durch die so erzielte Reduzierung der Treiberanzahl wird die Verwaltung erheblich vereinfacht. Der universelle Druckertreiber unterstützt die erweiterten Druckerfunktionen, wie z. B. Heftung und Sortierung und beschränkt nicht die Farbtiefe.

Die folgende Abbildung zeigt die universellen Druckertreiberkomponenten und einen typischen Workflow für ein lokal angeschlossenes Druckgerät.

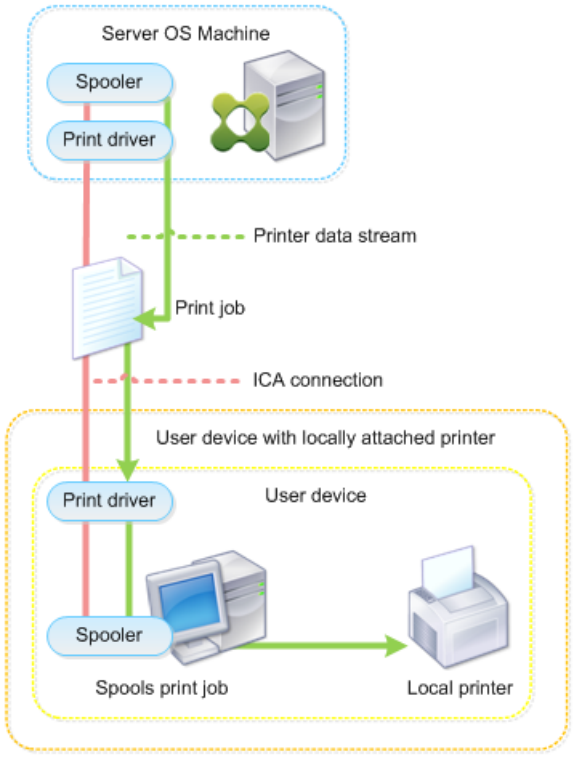


Legen Sie bei der Planung der Strategie zur Treiberverwaltung fest, ob Sie gerätespezifische Treiber, den universellen Druckertreiber oder beides unterstützen wollen. Wenn Sie Standardtreiber unterstützen, müssen Sie außerdem Folgendes festlegen:

- Zu unterstützende Treibertypen
- Aktivieren oder Deaktivieren der automatischen Installation der Druckertreiber (falls auf Serverbetriebssystemmaschinen nicht vorhanden)
- Erstellen der Treiberkompatibilitätslisten

Wenn das System während der automatischen Druckererstellung erkennt, dass ein neuer lokaler Drucker an einem Benutzergerät angeschlossen ist, wird die Serverbetriebssystemmaschine auf den erforderlichen Druckertreiber hin überprüft. Ist kein Windows-systemeigener Treiber verfügbar, wird vom System standardmäßig der universelle Druckertreiber verwendet.

Der Druckvorgang kann nur dann erfolgreich ausgeführt werden, wenn der Druckertreiber auf der Serverbetriebssystemmaschine und der Treiber auf dem Benutzergerät übereinstimmen. In der folgenden Abbildung wird dargestellt, wie der Druckertreiber an zwei Orten für den Clientdruck verwendet wird.



Verwandter Inhalt

- Beispiel einer Druckkonfiguration
- Bewährte Methoden, Sicherheitsüberlegungen und Standardvorgänge
- Druckrichtlinien und Einstellungen
- Bereitstellen von Druckern
- Pflege der Druckumgebung

Beispiel einer Druckkonfiguration

Feb 29, 2016

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:

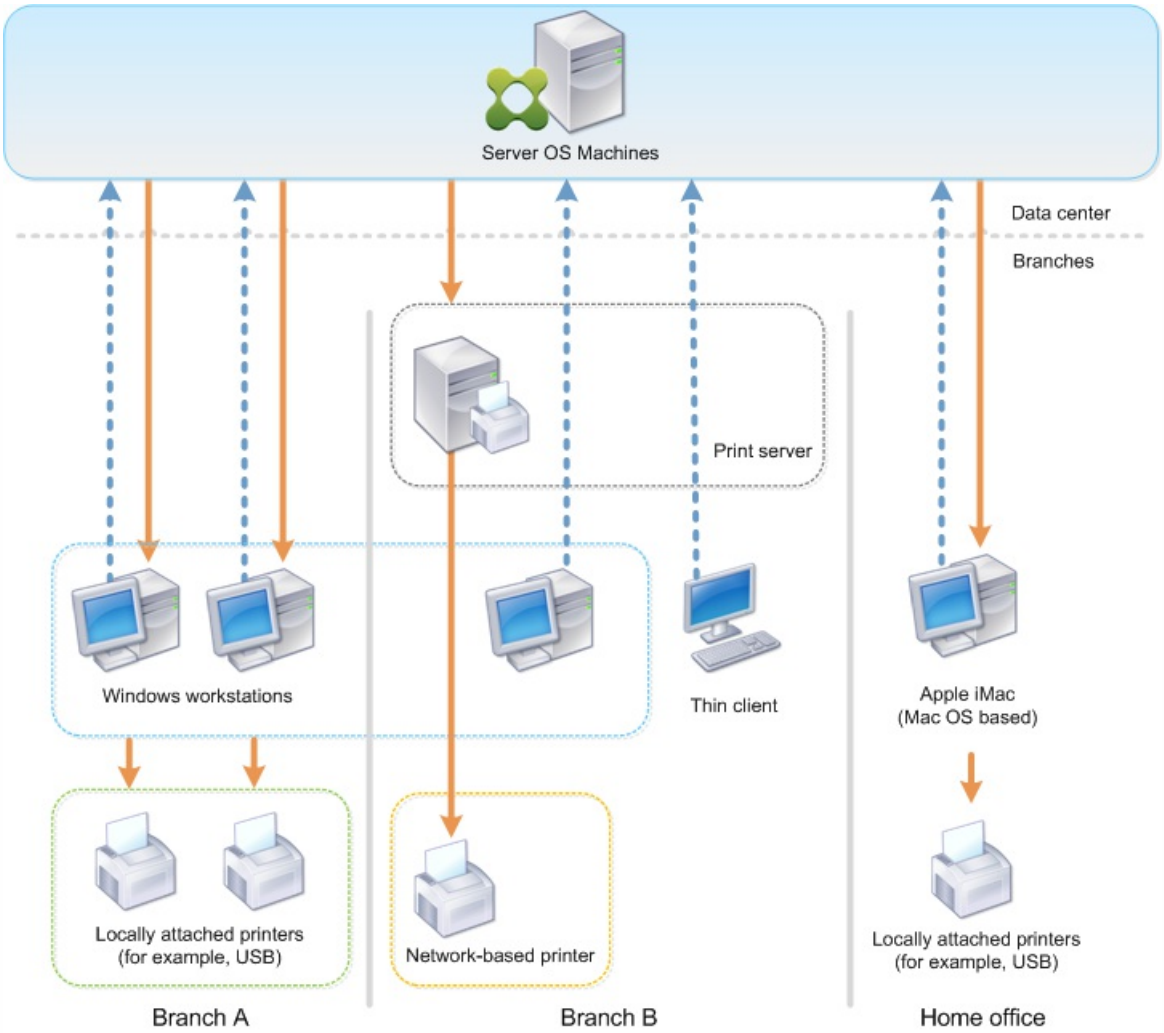
- Den Unternehmensanforderungen und der vorhandenen Druckinfrastruktur.
  Berücksichtigen Sie bei der Druckkonfiguration die Anforderungen der Organisation. Die vorhandene Druckimplementierung (ob Benutzer Drucker hinzufügen können, welche Benutzer Zugriff auf welche Drucker haben usw.) kann bei der 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:

- **Zweigstelle A**: Kleine Auslandsniederlassung mit einigen Windows-Arbeitsstationen. Jede Benutzerarbeitsstation hat einen lokal angeschlossenen, privaten Drucker.
- **Zweigstelle B**: Großes Zweigstellenbüro mit Thin Clients und auf Windows basierenden 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-basierten Benutzergerät, über das auf die Citrix Infrastruktur des Unternehmens zugegriffen wird. Das Benutzergerät hat einen lokal angeschlossenen Drucker.



In den folgenden Abschnitten werden Konfigurationen beschrieben, die die Komplexität der Umgebung minimieren und die Verwaltung vereinfachen.

Automatisch erstellte Clientdrucker und der universelle Citrix Druckertreiber

In Branch A arbeiten alle Benutzer auf Arbeitsstationen unter Windows und verwenden daher automatisch erstellte Clientdrucker und den universellen Druckertreiber. Dies bietet folgende Vorteile:

- Leistung: Druckaufträge werden über den ICA-Druckkanal geleitet, sodass die Druckdaten komprimiert werden können und Bandbreite eingespart wird.
  Um sicherzustellen, dass ein einzelner Benutzer durch den Druck eines großen Dokuments nicht die Sitzungsleistung anderer Benutzer beeinträchtigt, wird eine Citrix Richtlinie für die maximale Druckbandbreite konfiguriert.

  Eine andere Lösung wäre die Multistream-ICA-Verbindung, bei der der Druckverkehr innerhalb einer separaten TCP-Verbindung mit niedriger Priorität übertragen wird. Multistream-ICA kann verwendet werden, wenn Quality of Service (QoS) über die WAN-Verbindung nicht implementiert ist.

- Flexibilität: Der universelle Citrix Druckertreiber gewährleistet, dass alle mit dem Client verbundenen Drucker auch von virtuellen Desktop- oder Anwendungssitzungen verwendet werden können, ohne dass ein neuer Druckertreiber im Datencenter integriert werden muss.

Universeller Citrix Druckserver

In Branch B werden alle Netzwerkdrucker und ihre Warteschlangen auf einem Windows-Druckerserver verwaltet. Somit

erweist sich der universelle Citrix Druckserver als die effizienteste Konfiguration.

Alle erforderlichen Druckertreiber werden von lokalen Administratoren auf dem Druckserver installiert und verwaltet. Das Zuordnen von Druckern in virtuellen Desktop- oder Anwendungssitzungen funktioniert wie folgt:

- Arbeitsstationen unter Windows: Das IT-Team vor Ort hilft den Benutzern beim Herstellen der Verbindung mit dem geeigneten Netzwerkdrucker auf ihren Windows-Arbeitsstationen. Dies ermöglicht Benutzern, über lokal installierte Anwendungen zu drucken.
  Bei virtuellen Desktop- oder Anwendungssitzungen werden die lokal konfigurierten Drucker über die automatische Erstellung aufgelistet. Der virtuelle Desktop oder die virtuelle Anwendung stellt dann eine Verbindung mit dem Druckserver her, falls möglich, als Direktnetzwerkverbindung.

  Die Komponenten des universellen Citrix Druckservers werden installiert und aktiviert, systemeigene Druckertreiber sind nicht erforderlich. Falls ein Treiber aktualisiert oder eine Druckerwarteschlange geändert wird, ist im Datencenter keine weitere Konfiguration nötig.

- Thin Clients: Für Thin Clients-Benutzer müssen die Drucker in den virtuellen Desktop- oder Anwendungssitzungen angeschlossen werden. Um den Benutzern das Drucken so einfach wie möglich zu machen, konfigurieren die Administratoren eine einzige Citrix Sitzungsdruckerrichtlinie pro Stockwerk, damit der jeweilige Drucker als Standarddrucker festgelegt wird.
  Damit sichergestellt ist, dass die Benutzer stets mit dem richtigen Drucker verbunden sind, auch wenn sie in einem anderen Stockwerk sind, werden die Richtlinien nach Subnetz oder Thin Client-Namen gefiltert. Diese Konfiguration, die auch als "Proximitydrucken" bezeichnet wird, lässt die Wartung lokaler Druckertreiber zu (gemäß der delegierten Administration).

  Wenn eine Druckerwarteschlange geändert oder hinzugefügt werden muss, müssen Citrix Administratoren die entsprechende Richtlinie für Sitzungsdrucker in der Umgebung ändern.

Da der Netzwerkdruckdatenverkehr außerhalb des virtuellen ICA-Kanals gesendet wird, wird QoS implementiert. Eingehende und ausgehende Netzwerkdaten an Ports für ICA/HDX-Datenverkehr haben Vorrang vor sonstigem Netzwerkdatenverkehr. Diese Konfiguration gewährleistet, dass Benutzersitzungen von großen Druckaufträgen nicht beeinträchtigt werden.

Automatisch erstellte Clientdrucker und der universelle Citrix Druckertreiber

Bei Heimbüros mit nicht standardmäßigen Arbeitsstationen und nicht verwalteten Druckgeräten ist es am einfachsten, automatisch erstellte Drucker und den universellen Druckertreiber zu verwenden.

Zusammenfassung der Bereitstellung

Zusammenfassend lässt sich die Konfiguration dieses Bereitstellungsbeispiels wie folgt beschreiben:

- Auf Serverbetriebssystemmaschinen werden keine Druckertreiber installiert. Es wird nur der universelle Citrix Druckertreiber verwendet. Fallback auf systemeigene Druckertreiber und die automatische Installation von Druckertreibern sind deaktiviert.
- Die automatische Erstellung von Clientdruckern für alle Benutzer wird über eine Richtlinie konfiguriert. Serverbetriebssystemmaschinen werden standardmäßig direkt mit dem Druckserver verbunden. Zur Konfiguration müssen lediglich die Komponenten des universellen Druckservers aktiviert werden.
- Eine Sitzungsdruckerrichtlinie wird für jedes Stockwerk von Branch B konfiguriert und gilt für alle Thin Clients des jeweiligen Stockwerks.
- Die Implementierung von QoS für Branch B gewährleistet eine hervorragende Benutzererfahrung.

Bewährte Methoden, Sicherheitsüberlegungen und Standardvorgänge

Feb 29, 2016

Bewährte Methoden

Viele Faktoren bestimmen die beste Drucklösung für eine bestimmte Umgebung. Einige dieser bewährten Methoden sind möglicherweise für Ihre Site nicht geeignet.

- Verwenden Sie das Citrix Feature "universeller Druckserver".
- Verwenden Sie den universellen Druckertreiber oder Windows-systemeigene Treiber.
- Reduzieren Sie die Anzahl der installierten Druckertreiber auf den Serverbetriebssystemmaschinen auf das Minimum.
- Verwenden Sie Treiberzuordnung zu systemeigenen Treibern.
- Installieren Sie nie ungetestete Druckertreiber in einer Produktionssite.
- Vermeiden Sie Updates von Treibern. Versuchen Sie stets, einen Treiber zu deinstallieren, den Server neu zu starten und dann einen Ersatztreiber zu installieren.
- Deinstallieren Sie nicht verwendete Treiber oder verwenden Sie die Richtlinie Druckertreiberzuordnung und -kompatibilität, um zu verhindern, dass Drucker mit dem Treiber erstellt werden.
- Vermeiden Sie möglichst Kernelmodustreiber der Version 2.
- Wenden Sie sich an den Hersteller oder sehen Sie in der Citrix Ready-Produktdokumentation www.citrix.com/ready nach, ob ein Druckermodell unterstützt wird.
  Im Allgemeinen werden alle von Microsoft zur Verfügung gestellten Druckertreiber mit Terminaldiensten getestet und ihre Funktion unter Citrix gewährleistet. Vergewissern Sie sich jedoch vor Einsatz eines Druckertreibers eines Drittanbieters, dass der Treiber von Windows Hardware Quality Labs (WHQL) für Terminaldienste zertifiziert wurde. Citrix vergibt keine Zertifizierung für Druckertreiber.

Sicherheitsüberlegungen

Citrix Drucklösungen sind inhärent sicher.

- Der Citrix Druckmanagerdienst überwacht und reagiert fortlaufend auf Sitzungsereignisse wie An- und Abmeldung, Trennen, Wiederverbinden und Beenden der Sitzung. Er behandelt Anforderungen, indem er die Identität des Benutzers der aktuellen Sitzung übernimmt.
- Beim Citrix Drucken wird jedem Drucker ein eindeutiger Namespace in einer Sitzung zugewiesen.
- Die Standardsicherheitsbeschreibung für automatisch erstellte Drucker wird eingerichtet, 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 Richtlinieneinstellung Clientdrucker automatisch erstellen mit der Option Alle Clientdrucker automatisch erstellen.

- Das System leitet alle Druckaufträge, die in Warteschlangen für an Benutzergeräte lokal angeschlossene Drucker gestellt wurden, als Clientdruckaufträge weiter (d. h. über den ICA-Kanal und durch das Benutzergerät).

- Das System leitet alle Druckaufträge, die in Warteschlangen von Netzwerkdruckern gestellt wurden, direkt über Serverbetriebssystemmaschinen. Falls die Aufträge vom System nicht über das Netzwerk weitergeleitet werden können, werden sie als umgeleiteter Clientdruckauftrag über das Benutzergerät weitergeleitet.
  Dieses Verhalten entspricht dem Deaktivieren der Citrix Richtlinieneinstellung Direkte Verbindungen zu Druckservern.

- Standardmäßig versucht das System, die Druckeigenschaften (eine Kombination aus den Druckeinstellungen des Benutzers und den gerätespezifischen Druckeinstellungen) auf dem Benutzergerät zu speichern. Wenn der Client diesen Vorgang nicht unterstützt, werden die Druckeigenschaften vom System in Benutzerprofilen auf der Serverbetriebssystemmaschine gespeichert.
  Dieses Verhalten entspricht der Citrix Richtlinieneinstellung Speicherung von Druckereigenschaften mit der Option Nur im Profil speichern, wenn sie nicht auf dem Client gespeichert sind.

- Das System verwendet die Windows-Version des Druckertreibers, falls sie auf der Serverbetriebssystemmaschine verfügbar ist. Ist der Druckertreiber nicht verfügbar, versucht das System, den Treiber vom Windows-Betriebssystem zu installieren. Ist der Treiber in Windows nicht verfügbar, wird ein universeller Citrix Druckertreiber verwendet.
  Dieses Verhalten entspricht dem Aktivieren der Citrix Richtlinieneinstellung Automatische Installation von mitgelieferten Druckertreibern und Konfigurieren der Einstellung Universal Printing mit der Option 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 das PowerShell-Cmdlet **Start-TelemetryUpload**.

Druckrichtlinien und -einstellungen

Feb 29, 2016

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 Druckrichtlinien konfiguriert. Druckeinstellungen folgen dem Standardverhalten für Citrix Richtlinien:

Druckereinstellungen können vom System am Ende einer Sitzung in das Druckerobjekt oder das Clientdruckgerät geschrieben werden, sofern das Netzwerkkonto des Benutzers ausreichende Berechtigungen hat. Standardmäßig verwendet Citrix Receiver die Einstellungen, die im Druckerobjekt in der Sitzung gespeichert wurden, bevor an anderen Orten nach Einstellungen gesucht wird.

Standardmäßig werden die Druckereigenschaften auf dem Benutzergerät (falls vom Gerät unterstützt) oder im Benutzerprofil auf der Serverbetriebssystemmaschine gespeichert oder beibehalten. Wenn die Druckereigenschaften während einer Sitzung vom Benutzer geändert werden, werden diese Änderungen im Benutzerprofil auf der Maschine aktualisiert. Wenn sich der Benutzer das nächste Mal anmeldet oder eine neue Verbindung herstellt, übernimmt das Benutzergerät die beibehaltenen Einstellungen. Das heißt, auf dem Benutzergerät geänderte Druckereigenschaften wirken sich nicht auf die aktuelle Sitzung aus bis zum Ab- und erneuten Anmelden 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 vorgenommen wurden, also auf der Serverbetriebssystemmaschine.
- **Auf der Serverbetriebssystemmaschine**: Dies sind die Standardeinstellungen, die einem bestimmten Druckertreiber auf der Maschine zugeordnet sind.

Die in einer Windows-Umgebung gespeicherten Einstellungen sind abhängig von der Stelle, an der die Einstellungen vom

Benutzer vorgenommen wurden. Das bedeutet außerdem, dass die an einer Stelle wie einer Tabellenkalkulation angezeigten Druckeinstellungen sich von den Einstellungen an anderen Stellen, beispielsweise in Dokumenten, unterscheiden können. Die auf einen bestimmten Drucker angewendeten Druckeinstellungen variieren daher innerhalb einer Sitzung.

Hierarchie der Benutzerdruckeinstellungen

Da die Druckeinstellungen an verschiedenen Stellen gespeichert werden können, verarbeitet das System sie gemäß einer bestimmten Priorität. Sie dürfen auch nicht vergessen, dass Geräteeinstellungen anders behandelt werden als Dokumenteinstellungen und normalerweise Vorrang vor diesen haben.

Standardmäßig wendet das System immer alle Druckeinstellungen an, die ein Benutzer während einer Sitzung geändert hat, d. h. alle beibehaltenen Einstellungen, bevor andere Einstellungen berücksichtigt werden. Wenn der Benutzer druckt, führt das System die auf der Serverbetriebssystemmaschine gespeicherten Standarddruckereinstellungen mit allen beibehaltenen Einstellungen oder Clientdruckeinstellungen zusammen und wendet sie an.

Speichern der Druckeinstellungen des Benutzers

Citrix empfiehlt, dass Sie den Speicherort der Druckereigenschaften nicht ändern. Am einfachsten können Sie konsistente Druckereigenschaften sicherstellen, indem Sie die Standardeinstellung beibehalten, wonach die Druckereigenschaften auf dem Benutzergerät gespeichert werden. Wenn das System die Eigenschaften auf dem Benutzergerät nicht speichern kann, wird automatisch auf das Benutzerprofil auf der Serverbetriebssystemmaschine zurückgegriffen.

Überprüfen Sie die Richtlinieneinstellung Speicherung von Druckereigenschaften, wenn diese Szenarios zutreffen:

- Verwendung von älteren Plug-Ins, durch die das Speichern der Druckereigenschaften durch die Benutzer auf einem Benutzergerät unterbunden wird
- Verwendung verbindlicher Profile im Windows-Netzwerk, wobei die Druckereigenschaften der Benutzer beibehalten werden sollen

Bereitstellen von Druckern

Feb 29, 2016

Es gibt drei Methoden der Druckerbereitstellung:

- Universeller Citrix Druckserver
- Automatisch erstellte Clientdrucker
- Vom Administrator zugewiesene Sitzungsdrucker

Universeller Citrix Druckserver

Bei der Wahl der besten Drucklösung für Ihre Umgebung sollten Sie Folgendes berücksichtigen:

- Der universelle Druckserver bietet Features, die beim Windows-Druckanbieter nicht verfügbar sind: Zwischenspeichern von Bildern und Schriftarten, erweiterte Komprimierung, Optimierung und Unterstützung für QoS.
- Der universelle Druckertreiber unterstützt die von Microsoft definierten, öffentlichen geräteunabhängigen Einstellungen. Wenn Benutzer Zugriff auf die Geräteeinstellungen des Druckertreibers eines bestimmten Herstellers benötigen, stellt der universelle Druckserver gepaart mit einem Windows-systemeigenen Treiber die beste Lösung dar. In dieser Konfiguration bleiben die Vorteile des universellen Druckservers erhalten und die Benutzer können zugleich auf bestimmte Druckerfunktionen zugreifen. Allerdings ist zu bedenken, dass Windows-systemeigene Treiber wartungsbedürftig sind.
- Der universelle Druckserver von Citrix bietet universelle Druckunterstützung für Netzwerkdrucker. Der universelle Druckserver verwendet den universellen Druckertreiber, einen einzelnen Treiber auf der Serverbetriebssystemmaschine, mit dem von jedem Gerät aus, einschließlich Thin Clients und Tablets, auf lokalen oder Netzwerkdruckern gedruckt werden kann.

Um den universellen Druckserver mit einem Windows-systemeigenen Treiber zu verwenden, aktivieren Sie den universellen Druckserver. Wenn der Windows-systemeigene Treiber verfügbar ist, wird er standardmäßig verwendet. Andernfalls wird der universelle Druckertreiber verwendet. Um dieses Verhalten zu ändern, beispielsweise zur ausschließlichen Verwendung des Windows-systemeigenen Treibers oder des universellen Druckertreibers, müssen Sie die Richtlinieneinstellung Verwendung universeller Druckertreiber aktualisieren.

Installieren des universellen Druckservers

Zum Verwenden des universellen Druckservers installieren Sie die UPsServer-Komponente, wie in den Dokumenten zur Installation beschrieben, auf den Druckservern und konfigurieren Sie sie. Weitere Informationen finden Sie unter Installieren über die grafische Oberfläche und Installieren über die Befehlszeile.

In Umgebungen, in denen Sie die UPClient-Komponente separat bereitstellen, z. B. mit **XenApp 6.5**:

1. Laden Sie das eigenständige Paket für den XenApp und XenDesktop Virtual Delivery Agent (VDA) für Windows-Desktopbetriebssysteme oder Windows-Serverbetriebssysteme herunter.
2. Extrahieren Sie den VDA gemäß den Anweisungen für die Befehlszeile unter Verwenden des dedizierten VDA-Installationsprogramms finden.
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.

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 ist **8080**.

  Zum Ändern des HTTP-Standardports 8080 für die Kommunikation zwischen universellem Druckserver und XenApp- bzw. XenDesktop-VDAs müssen Sie außerdem auf Computern mit dem universeller Druckserver den folgenden Registrierungsschlüssel erstellen und die Portnummer ändern:

  HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\PrintingPolicies
  "UpsHttpPort"=DWORD:

  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).

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

Richtlinieneinstellung	Interaktion
	Druckens konfiguriert ist, kann mit dem universellen Druckertreiber ein direkter Netzwerkdrucker zum Druckserver erstellt werden.
UPD-Präferenz	Unterstützt EMF- und XPS-Treiber.

Auswirkungen auf Benutzeroberflächen: Der vom universellen Druckserver verwendete universelle Citrix Druckertreiber deaktiviert die folgenden Benutzeroberflächensteuerelemente:

- Schaltfläche für die lokalen Druckereinstellungen im Druckereigenschaften-Dialogfeld
- Schaltflächen für die lokalen Druckereinstellungen und die Vorschau im Dokumenteigenschaften-Dialogfeld

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 Richtlinie "Verwendung universeller Druckertreiber" festgelegt ist, dass universelles Drucken verwendet werden muss, wird der Name des universellen Druckertreibers bei der Auswahl des Druckers angezeigt. Der Windows-Druckanbieter kann den universellen Druckertreiber nicht verwenden.

Der Citrix Druckanbieter unterstützt kein clientseitiges Rendering.

Weitere Informationen zum universellen Druckserver finden Sie unter CTX200328.

Automatisch erstellte Clientdrucker

Die folgenden universellen Drucklösungen sind für Clientdrucker verfügbar:

- **Citrix Universeller Drucker**: ein generischer Drucker, der zu Beginn einer Sitzung erstellt wird und nicht an ein Druckgerät gebunden ist. Der Citrix Universelle Drucker muss die verfügbaren Clientdrucker bei der Anmeldung nicht auflisten, wodurch sich der Ressourceneinsatz erheblich reduziert und die Anmeldedauer für die Benutzer verringert wird. Mit dem Citrix Universellen Drucker kann auf jedem clientseitigen Druckgerät gedruckt werden.
  Der Citrix Universelle Drucker funktioniert allerdings möglicherweise nicht für alle Benutzergeräte oder Citrix Receiver in Ihrer Umgebung. Der Citrix Universelle Drucker erfordert eine Windows-Umgebung und unterstützt nicht das Citrix Offline Plug-In oder Anwendungen, die an Clients gestreamt werden. Verwenden Sie für solche Umgebungen automatisch erstellte Drucker und den universellen Druckertreiber.

  Wenn Sie eine universelle Drucklösung für Nicht-Windows-Citrix Receiver benötigen, verwenden Sie einen der anderen universellen Postscript/PCL-Druckertreiber, die automatisch installiert werden.

- **Universeller Citrix Druckertreiber**: ein geräteunabhängiger Druckertreiber, der erweiterte Druckerfunktionen unterstützt, z. B. Heftung und Sortierung. 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 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 Administratoren zugewiesener Drucker 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 nach Objekten, z. B. 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.

Pflege der Druckumgebung

Feb 29, 2016

Zur Pflege der Druckumgebung gehört Folgendes:

- Verwalten von Druckertreibern
- Optimieren der Druckleistung
- Anzeigen von Druckern und Verwalten von Druckwarteschlangen

Verwalten von Druckertreibern

Citrix empfiehlt die Verwendung des universellen Citrix Druckertreibers, um den Verwaltungsaufwand und mögliche Probleme mit Druckertreibern gering zu halten.

Wenn die automatische Erstellung fehlschlägt, installiert das System standardmäßig einen bei Windows integrierten systemeigenen Druckertreiber. Falls kein Treiber verfügbar ist, greift das System automatisch auf den universellen Druckertreiber zurück. Weitere Informationen über Druckertreiber-Standardwerte finden Sie unter Bewährte Methoden, Sicherheitsüberlegungen und Standardvorgänge.

Wenn der universelle Druckertreiber von Citrix nicht für alle Szenarios geeignet ist, reduzieren Sie die Anzahl installierter Treiber auf Serverbetriebssystemmaschinen mit von Druckertreiberzuordnungen. Außerdem bietet die Zuordnung von Druckertreibern folgende Optionen:

- Beschränken bestimmter Drucker auf die ausschließliche Verwendung des universellen Citrix Druckertreibers
- Zulassen oder Verhindern der Erstellung von Druckern mit einem bestimmten Treiber
- Ersetzen veralteter oder beschädigter Treiber durch gewünschte Druckertreiber
- Ersetzen von Clienttreibernamen durch einen unter Windows Server verfügbaren Treiber

Automatische Installation von Druckertreibern verhindern: Die automatische Installation von Druckertreibern muss deaktiviert sein, damit Konsistenz zwischen Serverbetriebssystemmaschinen gewährleistet ist. Dies kann über Citrix Richtlinien und/oder Microsoft-Richtlinien erreicht werden. Zum Verhindern der automatischen Installation Windows-systemeigener Druckertreiber deaktivieren Sie die Citrix Richtlinieneinstellung Automatische Installation von mitgelieferten Druckertreibern.

Zuordnen von Clientdruckertreibern: Jeder Client liefert bei der Anmeldung Informationen zu den clientseitigen Druckern, einschließlich dem Namen des Druckermodells. Bei der automatischen Erstellung der Clientdrucker werden die Namen der Druckertreiber auf dem Windows-Server ausgewählt, die den Namen der Druckermodelle entsprechen, die der Client bereitgestellt hat. Beim automatischen Erstellen werden mit diesen identifizierten verfügbaren Druckertreibern umgeleitete Clientdruckwarteschlangen erstellt.

Gehen Sie bei der Erstellung von Regeln für die Treiberersetzung und der Bearbeitung der Druckeinstellungen für zugeordnete Clientdruckertreiber grundsätzlich folgendermaßen vor:

1. Legen Sie die Regeln für die Treiberersetzung für automatisch erstellte Drucker fest, indem Sie die Citrix Richtlinieneinstellung Druckertreiberzuordnung und -kompatibilität konfigurieren. Fügen Sie dabei den Namen des Clientdruckertreibers hinzu und wählen Sie über das Menü Druckertreiber suchen den Servertreiber aus, durch den Sie den Clientdruckertreiber ersetzen möchten. Sie können in dieser Einstellung Platzhalter verwenden. Damit beispielsweise alle HP-Drucker einen bestimmten Treiber verwenden, geben Sie in der Richtlinieneinstellung HP* an.
2. Zum Ausschließen eines Druckertreibers wählen Sie den Namen des Treibers aus und aktivieren Sie die Einstellung Nicht erstellen.
3. Sie können bei Bedarf eine Treiberzuordnung bearbeiten, eine Zuordnung löschen oder die Reihenfolge der

Treibereinträge in der Liste ändern.

4. Zum Bearbeiten der Druckeinstellungen für zugeordnete Clientdruckertreiber wählen Sie den Druckertreiber aus, klicken Sie auf Einstellungen und geben Sie die Einstellungen wie Druckqualität, Ausrichtung und Farbe an. Wenn Sie eine Druckoption angeben, die der Druckertreiber nicht unterstützt, hat die Option keine Auswirkung. Mit dieser Einstellung werden die gespeicherten Druckereinstellungen überschrieben, die der Benutzer in einer vorherigen Sitzung festgelegt hat.
5. Citrix empfiehlt, das Verhalten der Drucker nach der Zuordnung von Treibern ausführlich zu testen, da einige Druckfunktionen möglicherweise nur über einen bestimmten Treiber zur Verfügung stehen.

Bei der Benutzeranmeldung wird die Clientdruckerkompatibilitätsliste vom System überprüft, bevor die Clientdrucker eingerichtet werden.

Optimieren der Druckleistung

Verwenden Sie den universellen Druckserver und den universellen Druckertreiber, um die Leistung zu optimieren. Die folgenden Richtlinien steuern die Druckoptimierung und Komprimierung:

- Universelles Drucken - Optimierungsstandards. Gibt die Standardeinstellungen für den universellen Drucker an, wenn er für eine Sitzung erstellt wird:
  - Mit Gewünschte Bildqualität geben Sie das standardmäßige Bildkomprimierungslimit an, das auf universelles Drucken angewendet wird. In der Standardeinstellung ist Standardqualität aktiviert, d. h. Benutzer können Bilder nur mit der Standardqualitäts- oder geringeren Qualitätskomprimierung drucken.
  - Mit Heavyweight-Komprimierung aktivieren aktivieren oder deaktivieren Sie das Verringern der Bandbreite unter den Komprimierungsgrad, der von "Gewünschte Bildqualität" festgelegt ist; Bildqualität geht nicht verloren. Standardmäßig ist die Heavyweight-Komprimierung deaktiviert.
  - Mit den Einstellungen Zwischenspeichern von Bildern und Schriftarten legen Sie fest, ob Bilder und Schriftarten, die mehrmals im Druckdatenstrom vorhanden sind, zwischengespeichert werden. Sie stellen damit sicher, dass jedes eindeutige Bild oder jede Schriftart nur einmal zum Drucker gesendet wird. Standardmäßig werden eingebettete Bilder und Schriftarten zwischengespeichert.
  - Mit Nicht-Administratoren können diese Einstellungen ändern legen Sie fest, ob Benutzer die Standardeinstellungen für die Druckoptimierung in einer Sitzung ändern können. Standardmäßig können Benutzer die Standardeinstellungen für die Druckoptimierung nicht ändern.
- Universelles Drucken - Bildkomprimierungslimit. Definiert die maximale Qualität und die minimale Komprimierung für Bilder, die mit dem universellen Druckertreiber gedruckt werden. Das Limit für Bildkomprimierung ist standardmäßig auf Beste Qualität (verlustfreie Komprimierung) gesetzt.
- Universelles Drucken - Druckqualitätslimit. Der Höchstwert für Punkte pro Zoll (dpi) zum Erstellen von Ausdrucken in einer Sitzung. In der Standardeinstellung ist kein Limit angegeben.

Standardmäßig werden alle für Netzwerkdrucker bestimmten Druckaufträge von der Serverbetriebssystemmaschine über das Netzwerk direkt an den Druckserver weitergeleitet. Erwägen Sie, Druckaufträge über die ICA-Verbindung zu leiten, wenn das Netzwerk hohe Latenz oder beschränkte Bandbreite aufweist. Deaktivieren Sie hierzu die Citrix Richtlinieneinstellung Direkte Verbindungen zu Druckservern. Bei einer ICA-Verbindung werden die Daten komprimiert gesendet, es wird somit weniger Bandbreite bei der Übertragung der Daten über das WAN gebraucht.

Verbessern der Sitzungsleistung durch Limitierung der Druckbandbreite: Beim Drucken von Dateien von Serverbetriebssystemmaschinen auf Benutzerdruckern, können bei anderen virtuellen Kanälen (z. B. Video) aufgrund des Wettbewerbs um die Bandbreite Leistungsverringerungen entstehen, insbesondere dann, wenn Benutzer über langsamere Netze auf Server zugreifen. Um dies zu verhindern, können Sie die für das Drucken verwendete Bandbreite beschränken. Indem Sie die Datenübertragungsrate für den Druck einschränken, stellen Sie im HDX-Datenstrom eine größere Bandbreite

für die Übertragung von Video, Tastatureingaben und Mausdaten zur Verfügung.

Wichtig: Das Druckerbandbreitenlimit wird immer eingehalten, auch wenn keine anderen Kanäle verwendet werden. Verwenden Sie die nachfolgenden Einstellungen der Citrix Richtlinie Bandbreite, um die Druckerbandbreitenlimits für die Sitzung zu beschränken. Führen Sie diese Aufgabe mit Studio aus, um die Limits für die Site festzulegen. Wenn Sie Limits für einzelne Server festlegen möchten, führen Sie diese Aufgabe über die Gruppenrichtlinien-Verwaltungskonsole in Windows lokal auf jeder Serverbetriebssystemmaschine aus.

- Die Einstellung Bandbreitenlimit für Druckerumleitung dient zur Angabe der zum Drucken verfügbaren Bandbreite in Kilobits pro Sekunde (KBit/s).
- Die Einstellung Bandbreitenlimit für Druckerumleitung (Prozent) begrenzt die zum Drucken verfügbare Bandbreite auf einen Prozentanteil der insgesamt verfügbaren Bandbreite.
  Hinweis: Zur Verwendung der Einstellung Bandbreitenlimit für Druckerumleitung (Prozent) müssen Sie auch die Einstellung Bandbreitenlimit für Sitzung insgesamt aktivieren.
  Wenn Sie Werte für beide Einstellungen eingeben, wird die strengste Einstellung (mit dem niedrigeren Wert) angewendet.

Zum Abrufen von Echtzeitinformationen zur Druckbandbreite verwenden Sie Citrix Director.

Anzeigen von Druckern und Verwalten der Druckwarteschlangen

In der folgenden Tabelle wird aufgeführt, wo Sie in Ihrer Umgebung Drucker anzeigen und die Druckwarteschlangen verwalten können.

	Druckmodell	**UAC aktiviert?**	**Speicherort**
Clientdrucker (an das Benutzergerät angeschlossene Drucker)	Clientdruckmodell	On	Druckverwaltung: Snap-in der Microsoft Management Console
		Off	Vor Windows 8: Systemsteuerung Windows 8: Snap-In Druckverwaltung
Netzwerkdrucker (Drucker auf einem Netzwerkdruckserver)	Netzwerkdruckmodell	On	Druckserver > Druckverwaltung Snap-In der Microsoft Management Console
		Off	Druckserver > Systemsteuerung
Netzwerkdrucker (Drucker auf einem Netzwerkdruckserver)	Clientdruckmodell	On	Druckserver > Druckverwaltung Snap-In der

	Druckmodell	UAC aktiviert?	Speicherort
			Microsoft Management Console
		Off	Vor Windows 8: Systemsteuerung Windows 8: Snap-In Druckverwaltung
Lokale Netzwerkserverdrucker (Drucker von einem Netzwerkdruckserver, die einer Serverbetriebssystemmaschine hinzugefügt werden)	Netzwerkdruckmodell	On	Druckserver > Systemsteuerung
		Off	Druckserver > Systemsteuerung

Hinweis: Druckwarteschlangen für Netzwerkdrucker, die das Netzwerkdruckmodell verwenden, sind privat und können nicht über das System verwaltet werden.

HDX

Feb 29, 2016

Citrix HDX enthält eine breite Palette an Technologien für eine High-Definition-Benutzererfahrung.

Auf dem Gerät	HDX nutzt die Computingfähigkeiten der Benutzergeräte und verbessert und optimiert die Benutzererfahrung. Die HDX MediaStream-Technologie liefert eine gleichmäßigen, nahtlosen Multimediainhalt in den virtuellen Desktops oder Anwendungen der Benutzer. 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 und stimmen Lastausgleich und Bandbreite anhand optimaler Technologien für die jeweiligen Benutzerszenarios aufeinander ab, 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. Komprimierte Multimediainformationen werden direkt im ursprünglichen Format an das Benutzergerät gesendet. Die in Citrix Director bereitgestellte HDX-Kanalüberwachung zeigt den Status der verbundenen HDX-Kanäle auf Benutzergeräten an. HDX Insight, die Integration von EdgeSight-Netzwerkinspektion und EdgeSight-Leistungsverwaltung mit Director, erfasst Daten zum ICA-Datenverkehr und bietet eine Dashboardansicht von Echtzeit- und historische Daten, wie die clientseitige und serverseitige ICA-Sitzungslatenz, die Bandbreitennutzung der ICA-Kanäle und die ICA-Roundtrip-Zeit für jede Sitzung.

Erleben von HDX-Funktionen mit Ihrem virtuellen Desktop:

- Sehen Sie selbst, wie hochwertige Videoinhalte auf virtuellen Desktops mit HDX wiedergegeben werden: Zeigen Sie ein Video auf einer Website mit HD-Videos an, z. B. http://www.microsoft.com/silverlight/iis-smooth-streaming/demo/.
- Erleben Sie, wie die Flash-Umleitung die Bereitstellung von Flash-Multimediainhalten beschleunigt:
  1. Laden Sie Adobe Flash Player herunter (http://get.adobe.com/flashplayer/) und installieren Sie ihn auf dem virtuellen Desktop und dem Benutzergerät.
  2. Klicken Sie auf der Desktop Viewer-Symbolleiste auf Einstellungen. Klicken Sie im Dialogfeld Desktop Viewer-Einstellungen auf die Registerkarte Flash und wählen Sie Inhalt optimieren.
  3. Erleben Sie, wie die Flash-Umleitung die Bereitstellung von Flash-Multimediainhalten auf virtuellen Desktops beschleunigt und zeigen Sie auf dem Desktop ein Video von einer Website mit Flash-Videos an, z. B. YouTube. Die Flash-Umleitung wird nahtlos integriert, sodass Benutzer nicht wissen, wann die Software ausgeführt wird. Sie können überprüfen, ob die Flash-Umleitung ausgeführt wird, indem Sie nach einem Farbblock Ausschau halten, der vorübergehend vor dem Start von Flash Player angezeigt wird.

- So stellt HDX HD-Audio bereit:
  1. Konfigurieren Sie den Citrix Client für maximale Audioqualität; weitere Informationen hierzu finden Sie in der Citrix Receiver-Dokumentation.
  2. Geben Sie Musikdateien mit einem digitalen Audioplayer (z. B. iTunes) auf dem Desktop wieder.

HDX bietet standardmäßig qualitativ hochwertige Grafiken und Videos, sodass für die meisten Benutzer keine Konfiguration erforderlich ist. Die standardmäßig aktivierten Citrix Richtlinieneinstellungen liefern die beste Sofortlösung 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 liefert den Windows-Desktopbenutzern eine Windows Aero-Oberfläche auf jedem Client.
- 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 diesen clientseitigen Inhaltsabruf nicht erfüllt sind, erfolgt die Medienbereitstellung automatisch über Windows Media-Umleitung zur Wiedergabe von Medieninhalten auf dem Benutzergerät statt auf dem Hostserver. In den meisten Fällen ist keine Änderung der Richtlinien für Windows Media erforderlich.

Gut zu wissen:

- Informationen zum Support und zu Systemanforderungen für HDX-Features finden Sie im Artikel Systemanforderungen Sofern nicht anders angegeben, stehen HDX-Features für unterstützte Windows-Serverbetriebssystemmaschinen, Windows-Desktopbetriebssystemmaschinen und Remote-PC-Zugriff-Desktops zur Verfügung.
- Nachfolgend wird beschrieben, wie Sie die Benutzererfahrung weiter optimieren, die Skalierbarkeit verbessern oder die Bandbreitenanforderungen reduzieren können. Weitere Informationen zum Arbeiten mit 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. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.

Reduzieren der Bandbreite für Windows-Desktops

HDX bietet standardmäßig eine hochgradig dynamische Windows Aero- oder Windows 8-Desktopdarstellung auf virtuellen Desktops von unterstützten Windows-Benutzergeräten. Um dies zu gewährleisten, nutzt HDX den Grafikprozessor (GPU) oder den integrierten Grafikprozessor (IGP) auf den Benutzergeräten für lokale DirectX Grafikwiedergabe. Dieses Feature wird als Desktopgestaltungsumleitung bezeichnet und gewährleistet hohe Skalierbarkeit auf dem Server. Weitere Informationen finden Sie unter "What to do with all these choices" unter http://blogs.citrix.com/2013/11/06/go-supersonic-with-xendesktop-7-x-bandwidth-supercodecs/.

Um die für Benutzersitzungen erforderliche Bandbreite zu reduzieren, sollten Sie die folgenden Richtlinieneinstellungen ändern. Beachten Sie, dass sich die Änderung der Einstellungen auf die Qualität der Benutzererfahrung auswirken kann.

- **Desktopgestaltungsumleitung**: gilt nur für Windows-Desktopbetriebssystemmaschinen, auf die über Windows-Benutzergeräte zugegriffen wird und nur für die Komposition des Windows-Desktops. Anwendungsfenster werden auf dem Server wiedergegeben, es sei denn, die Citrix Richtlinieneinstellung Zugriff auf lokale Anwendungen zulassen ist zugelassen.

- **Grafikqualität Desktopgestaltung**: verwendet hochwertige Grafiken für die Desktopgestaltung, es sei denn, Seamless-Anwendungen oder Zugriff auf lokale Anwendungen ist aktiviert. Reduzieren Sie die Grafikqualität, um die Bandbreite zu reduzieren.
- **Dynamische Fenstervorschau**: steuert die Anzeige von Seamlessfenstern in Flip, Flip 3D, Taskleistenvorschau und Peek-Fenstervorschau. Zum Reduzieren der Bandbreite deaktivieren Sie diese Richtlinieneinstellung.

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).
- Frameratesollwert: gibt die maximale Anzahl von Frames pro Sekunde an, die vom virtuellen Desktop zum Benutzergerät gesendet werden (Standardwert = 30). In vielen Fällen können Sie die Benutzererfahrung verbessern, indem Sie einen höheren Wert festlegen. Bei Geräten mit langsamen CPUs erzielen Sie durch Festlegen eines niedrigeren Werts eine bessere Benutzererfahrung.
- 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. Andere Farbtiefen als 32 Bit sind nur verfügbar, wenn die Richtlinieneinstellung Legacygrafikmodus aktiviert ist.

Verbessern der Videokonferenzleistung

Die HDX-Webcam-Videokomprimierung verbessert die Bandbreiteneffizienz und Latenztoleranz für Webcams während Videokonferenzen in einer Sitzung. Mit dieser Technologie werden die Webcamdaten über einen dedizierten virtuellen Multimediakanal gestreamt. Dies beansprucht erheblich weniger Bandbreite im Vergleich zum isochronen HDX-Plug-n-Play und funktioniert gut über WAN-Verbindungen.

Citrix Receiver-Benutzer können das Standardverhalten außer Kraft setzen, wenn sie in Desktop Viewer unter Mikrofon & Webcam die Einstellung Mikrofon und Webcam nicht verwenden auswählen. Um zu verhindern, dass Benutzer die HDX-Webcam-Videokomprimierung ändern, deaktivieren Sie die Umleitung von USB-Geräten über die Richtlinieneinstellungen unter "ICA > USB-Geräte".

Die HDX-Videokomprimierung ist bei Citrix Receiver unter Windows standardmäßig aktiviert, muss jedoch für Citrix Receiver unter Linux konfiguriert werden. Weitere Informationen finden Sie in der Citrix Receiver-Dokumentation. HDX-Webcam-Videokomprimierung erfordert, dass die folgenden Richtlinieneinstellungen aktiviert sind (alle sind standardmäßig aktiviert).

- Clientaudioumleitung
- Clientmikrofonumleitung
- Multimediakonferenzen
- Windows Media-Umleitung

Bei Webcams, die H.264-Hardwarecodierung unterstützen, verwendet HDX-Videokomprimierung die Hardwarecodierung standardmäßig. Die Hardware-Codierung beansprucht zusätzliche Bandbreite und ist nicht für Netzwerke mit geringer Bandbreite geeignet. Zum Erzwingen der Softwarekomprimierung bei Netzwerken mit geringer Bandbreite fügen Sie den folgenden DWORD-Schlüsselwert dem Registrierungsschlüssel hinzu: HKCU\Software\Citrix\HdxRealTime: DeepCompress_ForceSWEncode=1.

Bevorzugen der Skalierbarkeit des Servers vor der Benutzererfahrung

Bei Bereitstellungen, bei denen die Skalierbarkeit des Servers wichtiger ist als die Benutzererfahrung, können Sie das

Legacygrafiksystem verwenden, indem Sie die Richtlinieneinstellung Legacygrafikmodus hinzufügen und die einzelnen Richtlinieneinstellungen für Legacygrafiken konfigurieren. Ältere Grafiksysteme wirken sich auf die Benutzererfahrung über WAN- und mobile Verbindungen aus.

Flash-Umleitung

Feb 29, 2016

Bei der Flash-Umleitung wird die Verarbeitung der meisten Adobe Flash-Inhalte (einschließlich Animationen, Videos und Anwendungen) an über LAN- und WAN-angeschlossene Windows-Benutzergeräte übertragen, wodurch Server- und Netzwerklast verringert werden. Dies führt zu größerer Skalierbarkeit, während gleichzeitig eine High Definition-Benutzererfahrung sichergestellt wird. Das Konfigurieren der Flash-Umleitung erfordert sowohl server- als auch clientseitige Einstellungen.

Achtung: Bei der Flash-Umleitung findet eine erhebliche Anzahl von Interaktionen zwischen dem Benutzergerät und den Serverkomponenten statt. Verwenden Sie dieses Feature nur in Umgebungen, in denen eine sicherheitsbedingte Trennung zwischen dem Benutzergerät und dem Server nicht erforderlich ist. Zudem müssen Benutzergeräte so konfiguriert werden, dass sie dieses Feature nur mit vertrauenswürdigen Servern verwenden. Da für die Flash-Umleitung der Flash Player auf dem Benutzergerät installiert sein muss, aktivieren Sie diese Funktion nur, wenn der Flash Player gesichert ist.

Die zweite Generation und Legacyversionen der Flash-Umleitung sind unabhängige Lösungen und werden in separaten virtuellen Kanälen ausgeführt.

- Legacy-Flash-Umleitungsfeatures werden nur auf dem Client unterstützt. Wenn eine ältere Version oder gar keine Version des Flash Players auf dem Benutzergerät installiert ist, werden Flash-Inhalte auf dem Server wiedergegeben.
- Die zweite Generation der Flash-Umleitung wird sowohl auf Clients als auch auf Servern unterstützt. Wenn der Client die Flash-Umleitung der zweiten Generation unterstützt, werden Flash-Inhalte auf dem Client wiedergegeben. Flash-Umleitungsfeatures der zweiten Generation bieten Unterstützung für Benutzerverbindungen über das WAN, intelligentes Fallback und eine URL-Kompatibilitätsliste. Weitere Details finden Sie weiter unten.

Flash-Umleitung verwendet die Windows-Ereignisprotokollierung auf dem Server, um Flash-Ereignisse zu protokollieren. Das Ereignisprotokoll gibt an, ob Flash-Umleitung verwendet wird und ob Probleme vorliegen. Folgendes gilt für alle Ereignisse, die von der Flash-Umleitung protokolliert werden:

- Die Flash-Umleitung meldet Ereignisse an das Anwendungsprotokoll.
- Unter Windows 8 und Windows 7 wird ein spezifisches Protokoll für die Flash-Umleitung im Knoten "Anwendungs- und Dienstprotokolle" angezeigt.
- Der Quellwert ist Flash.
- Es wird keine Kategorie angegeben.

Aktuelle Updates für HDX Flash-Kompatibilität finden Sie unter CTX136588.

Konfigurieren der Flash-Umleitung auf dem Server

Zum Konfigurieren der Flash-Umleitung auf dem Server verwenden Sie die folgenden Citrix Richtlinieneinstellungen: Weitere Informationen finden Sie unter Einstellungen der Richtlinie "Flash-Umleitung".

- Flash-Standardverhalten: Legt das Standardverhalten der Flash-Beschleunigung fest. Standardmäßig ist die Flash-Umleitung aktiviert. Zum Überschreiben dieses Standardverhaltens für einzelne Webseiten und Flash-Instanzen verwenden Sie die Einstellung Flash-URL-Kompatibilitätsliste.
- Flash - intelligentes Fallback:Erkennt kleinere Flash-Filme (z. B. Werbefilme) und gibt sie auf dem Server wieder statt sie zur Wiedergabe auf das Benutzergerät umzuleiten. Dies verursacht keine Unterbrechung oder Fehler beim Laden der Webseite oder der Flash-Anwendung. Standardmäßig ist "Flash - intelligentes Fallback" aktiviert. Zum Umleiten aller Flash-Inhalte für die Wiedergabe auf dem Benutzergerät deaktivieren Sie diese Richtlinieneinstellung.
- URL-Liste für serverseitigen Flash-Inhaltsabruf: Mit dieser Liste können Sie die Websites angeben, deren Flash-Inhalte zum Server heruntergeladen und dann zur Wiedergabe zum Benutzergerät gesendet werden. (Bei der standardmäßigen Flash-

Umleitung werden Flash-Inhalte auf das Benutzergerät heruntergeladen und dort wiedergegeben.) Diese Einstellung ist zwingend mit der Einstellung Serverseitigen Inhaltsabruf aktivieren auf dem Benutzergerät verknüpft und ist hauptsächlich für Intranetsites und interne Flash-Anwendungen vorgesehen. Weitere Informationen finden Sie weiter unten. Sie funktioniert auch mit den meisten Websites und kann verwendet werden, wenn das Benutzergerät keinen direkten Internetzugang hat (z. B. wenn der XenApp- oder XenDesktop-Server die Verbindung herstellt).
Hinweis: Beim serverseitigen Inhaltsabruf werden keine Flash-Anwendungen unterstützt, die Real Time Messaging Protocol (RTMP) verwenden; stattdessen wird serverseitiges Rendering verwendet, bei dem HTTP und HTTPS unterstützt werden.

- Flash-URL-Kompatibilitätsliste: Gibt an, wo Flash-Inhalte von aufgelisteten Websites wiedergegeben werden: auf dem Benutzergerät, auf dem Server oder ob die Wiedergabe blockiert wird.
- Flash-Hintergrundfarbenliste: Hiermit können Sie die Farben von Webseiten und Flash-Instanzen aufeinander abstimmen, wodurch die Darstellung der Webseite bei Flash-Umleitung verbessert wird.

Konfigurieren der Flash-Umleitung auf dem Benutzergerät

Installieren Sie Citrix Receiver und Adobe Flash Player auf dem Benutzergerät. Es ist keine weitere Konfiguration auf dem Benutzergerät erforderlich.

Sie können die Standardeinstellungen mit Active Directory-Gruppenrichtlinienobjekten ändern. Importieren und fügen Sie die administrative Vorlage für HDX MediaStream Flash-Umleitung - Client (HdxFlashClient.adm) hinzu, die im folgenden Verzeichnis verfügbar ist:

- 32-Bit-Computer: %Programme%\Citrix\ICA Client\Configuration\Sprache
- 64-Bit-Computer: %Programme (x86)%\Citrix\ICA Client\Configuration\Sprache

Die Einstellungen werden unter Administrative Vorlagen > Klassische administrative Vorlage (ADM) > HDX MediaStream Flash-Umleitung - Client aufgeführt. Weitere Informationen über Gruppenrichtlinienobjekten und Vorlagen finden Sie in der Dokumentation zu Microsoft Active Directory.

Ändern der Verwendung der Flash-Umleitung

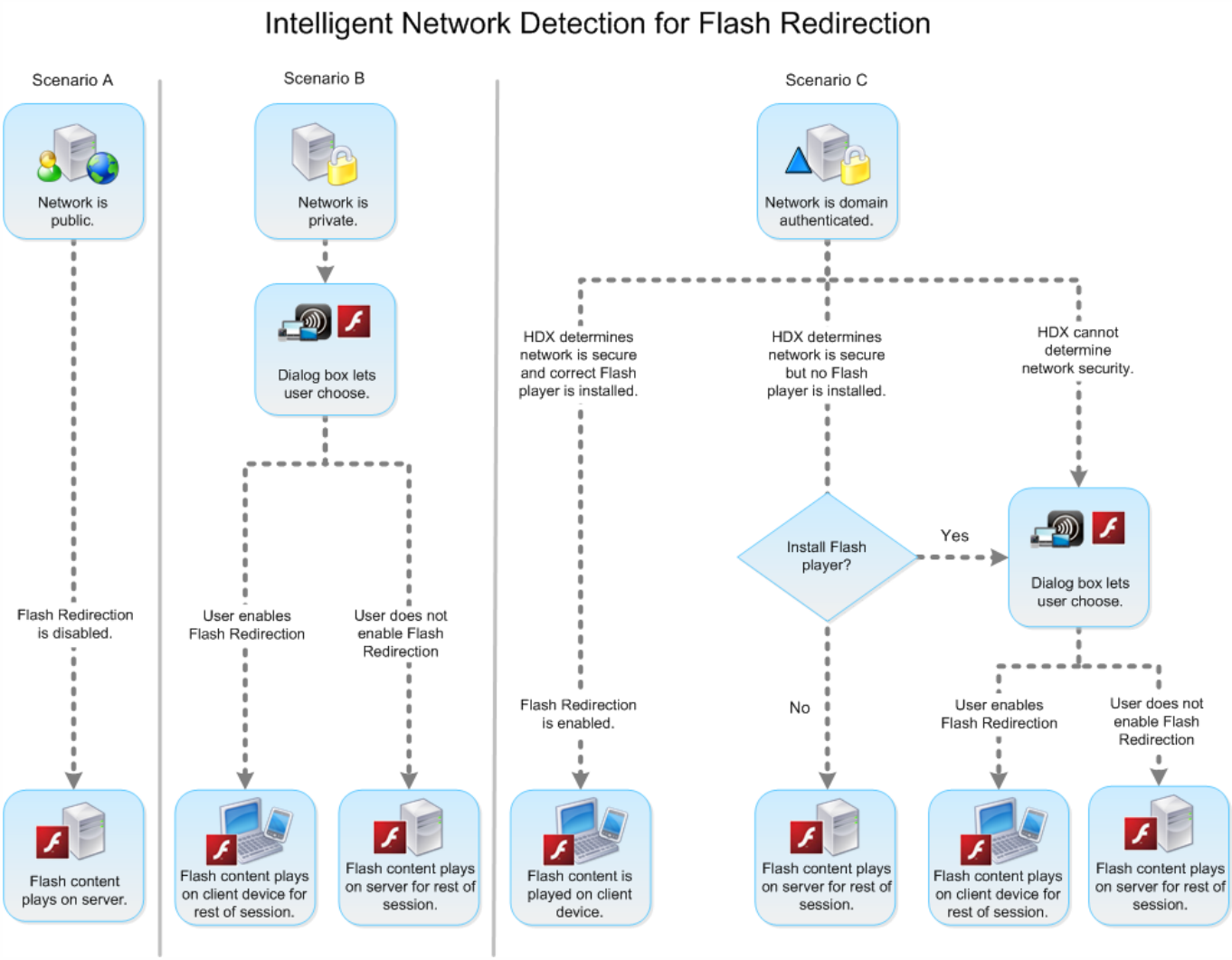
Zusammen mit serverseitigen Einstellungen steuert die Richtlinie HDX MediaStream-Flash-Umleitung auf dem Benutzergerät, ob Adobe Flash-Inhalte für die lokale Wiedergabe auf dem Benutzergerät umgeleitet werden. Standardmäßig ist die Flash-Umleitung aktiviert und ermittelt mit der intelligenten Netzwerkerkennung, wann Flash-Inhalte auf dem Benutzergerät wiedergegeben werden.

Wenn keine Konfiguration festgelegt ist und Desktop Lock verwendet wird, wird die Flash-Umleitung auf dem Benutzergerät standardmäßig aktiviert.

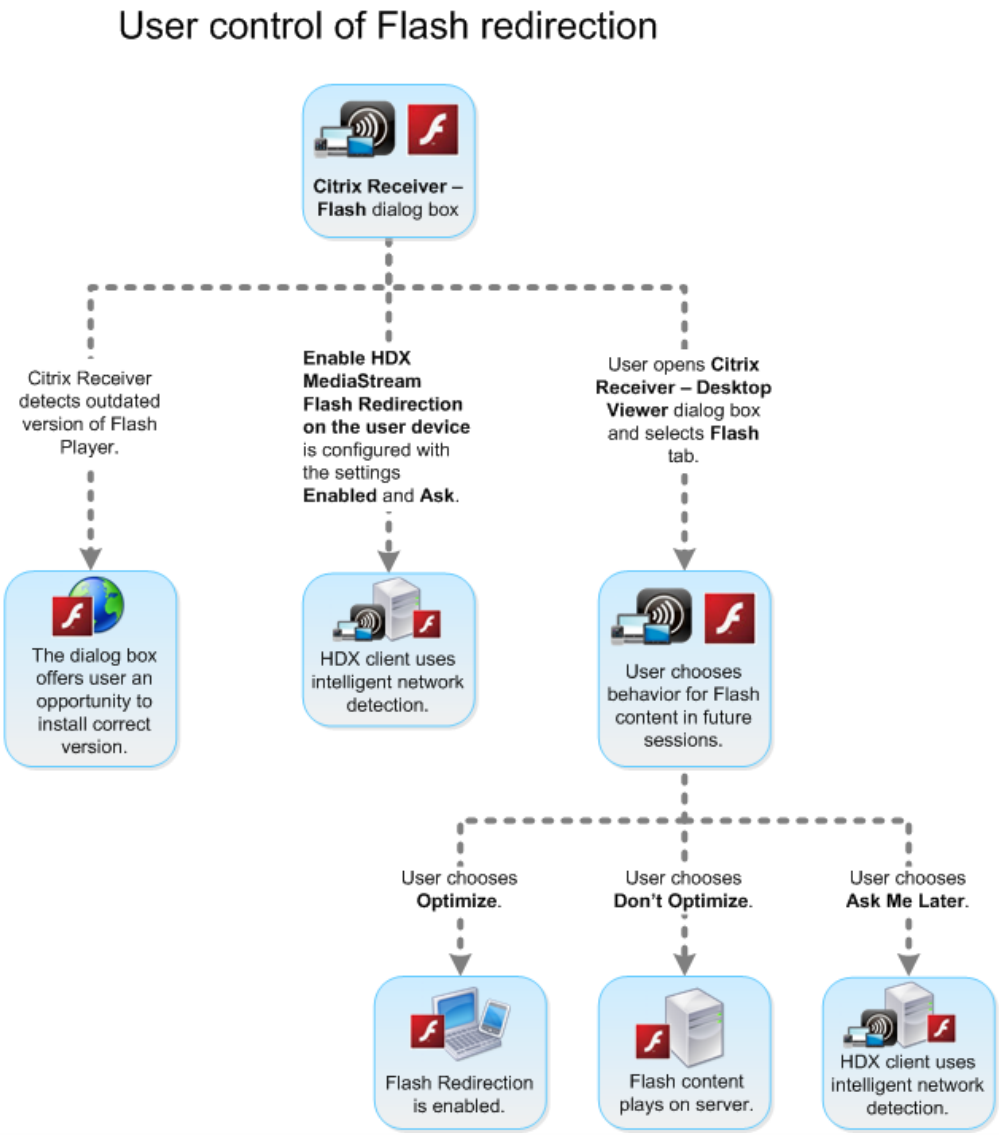
Gehen Sie zum Ändern der Verwendung von Flash-Umleitung bzw. zum Deaktivieren der Flash-Umleitung auf dem Benutzergerät wie folgt vor:

1. Wählen Sie aus der Einstellungsliste den Eintrag HDX MediaStream Flash-Umleitung auf dem Benutzergerät aktivieren und klicken Sie auf Richtlinieneinstellung.
2. Wählen Sie Nicht konfiguriert, Aktiviert (Standardeinstellung) oder Deaktiviert.
3. Wenn Sie Aktiviert eingestellt haben, wählen Sie eine Option unter HDX MediaStream Flash-Umleitung verwenden aus:
   - Die Einstellung Nur zweite Generation dient dazu, die aktuelle Flash-Umleitung zu verwenden, wenn die erforderliche Konfiguration vorhanden ist bzw. auf serverseitige Wiedergabe umzuschalten, wenn dies nicht der Fall ist.
   - Bei Wahl von Immer wird die Flash-Umleitung immer verwendet. Flash-Inhalte werden auf dem Benutzergerät wiedergegeben.
   - Bei Wahl von Nie wird die Flash-Umleitung nie verwendet. Flash-Inhalte werden auf dem Server wiedergegeben.
   - Mit Fragen (Standardeinstellung) wird festgelegt, dass die Entscheidung, ob Flash-Umleitung verwendet wird, durch

intelligente Netzwerkerkennung zur Beurteilung der Sicherheitsstufe des clientseitigen Netzwerks erfolgt. Wenn die Sicherheit des Netzwerks nicht bestimmt werden kann, erhält der Benutzer die Entscheidung über die Flash-Umleitung. Es erscheint eine Aufforderung, die Flash-Umleitung zu aktivieren bzw. zu deaktivieren.
Die folgende Abbildung zeigt, wie die Flash-Umleitung für verschiedene Netzwerktypen verarbeitet wird.



Benutzer können die intelligente Netzwerkerkennung über das Dialogfeld Citrix Receiver - Desktop Viewer-Einstellungen mit der Option Optimieren überschreiben oder über die Option Nicht optimieren auf der Registerkarte Flash. Welche Optionen zur Auswahl stehen, hängt davon ab, wie die Flash-Umleitung auf dem Benutzergerät konfiguriert ist (siehe folgende Abbildung).



Synchronisieren der clientseitigen HTTP-Cookies mit den serverseitigen HTTP-Cookies

Die Option zur serverseitigen HTTP-Cookie-Synchronisierung ist standardmäßig deaktiviert. Aktivieren Sie die Synchronisierung, um HTTP-Cookies vom Server herunterzuladen. Diese HTTP-Cookies werden dann für den clientseitigen Inhaltsabruf verwendet und können bei Bedarf von Sites mit Flash-Inhalten gelesen werden. Hinweis: Clientseitige Cookies werden bei der Synchronisierung nicht ersetzt; sie sind weiterhin verfügbar, wenn die Synchronisierungsrichtlinie zu einem späteren Zeitpunkt deaktiviert wird.

1. Wählen Sie aus der Einstellungsliste die Option Synchronisierung der clientseitigen HTTP-Cookies mit den serverseitigen HTTP-Cookies aktivieren und klicken Sie auf Richtlinieneinstellung.
2. Wählen Sie Nicht konfiguriert, Aktiviert oder Deaktiviert (Standardeinstellung).

Aktivieren Sie den serverseitigen Inhaltsabruf.

Bei der standardmäßigen Flash-Umleitung werden Flash-Inhalte auf das Benutzergerät heruntergeladen und dort wiedergegeben. Bei Aktivierung des serverseitigen Inhaltsabrufs werden die Flash-Inhalte zum Server heruntergeladen und dann an das Benutzergerät gesendet. Die Inhalte werden auf dem Benutzergerät wiedergegeben, sofern keine Richtlinie mit höherer Priorität dies verhindert, z. B. wenn eine Site durch die Richtlinieneinstellung Flash-URL-Kompatibilitätsliste blockiert wird.

Serverseitiger Inhaltsabruf wird häufig verwendet, wenn das Benutzergerät eine Verbindung zu internen Sites über

NetScaler Gateway herstellt und wenn das Benutzergerät keinen direkten Internetzugang hat.

Hinweis: Der serverseitige Inhaltsabruf unterstützt keine Flash-Anwendungen, die Real Time Messaging Protocol (RTMP) verwenden. Stattdessen wird die serverseitige Wiedergabe für solche Sites verwendet.
Die zweite Generation der Flash-Umleitung unterstützt drei Aktivierungsoptionen für den serverseitigen Inhaltsabruf. Zwei dieser Optionen umfassen das Zwischenspeichern serverseitiger Inhalte auf dem Benutzergerät, wodurch die Leistung verbessert wird, da wiederverwendeter Inhalt bereits wiedergabebereit auf dem Benutzergerät verfügbar ist. Der Inhalt dieses Caches wird separat von anderen HTTP-Inhalten auf dem Benutzergerät gespeichert.

Bei der Flash-Umleitung der zweiten Generation wird der Fallback auf serverseitigen Inhaltsabruf automatisch gestartet, wenn eine der Aktivierungsoptionen ausgewählt ist und der clientseitige Abruf von SWF-Dateien fehlschlägt.

Zum Aktivieren des serverseitigen Inhaltsabrufs müssen auf dem Clientgerät und dem Server Einstellungen festgelegt sein.

1. Wählen Sie in der Einstellungsliste den Eintrag Serverseitigen Inhaltsabruf aktivieren und klicken Sie auf Richtlinieneinstellung.
2. Wählen Sie Nicht konfiguriert, Aktiviert oder Deaktiviert (Standardeinstellung). Wenn Sie diese Einstellung aktivieren, wählen Sie eine der Optionen aus der Liste Serverseitiger Inhaltsabrufstatus:

Option	Beschreibung
Deaktiviert	Deaktiviert serverseitigen Inhaltsabruf und überschreibt die Einstellung URL-Liste für serverseitigen Flash-Inhaltsabruf auf dem Server. Fallback auf serverseitigen Inhaltsabruf ist auch deaktiviert.
Aktiviert	Aktiviert serverseitigen Inhaltsabruf für Webseiten und Flash-Anwendungen, die in der URL-Liste für serverseitigen Flash-Inhaltsabruf angegeben sind. Fallback auf serverseitigen Inhaltsabruf ist verfügbar, aber der Inhalt wird nicht zwischengespeichert.
Aktiviert (permanentes Caching)	Aktiviert serverseitigen Inhaltsabruf für Webseiten und Flash-Anwendungen, die in der URL-Liste für serverseitigen Flash-Inhaltsabruf angegeben sind. Fallback auf serverseitigen Inhaltsabruf ist verfügbar. Über serverseitigen Inhaltsabruf erhaltener Inhalt wird auf dem Benutzergerät zwischengespeichert und von Sitzung zu Sitzung gespeichert.
Aktiviert (temporäres Caching)	Aktiviert serverseitigen Inhaltsabruf für Webseiten und Flash-Anwendungen, die in der URL-Liste für serverseitigen Flash-Inhaltsabruf angegeben sind. Fallback auf serverseitigen Inhaltsabruf ist verfügbar. Über serverseitigen Inhaltsabruf erhaltener Inhalt wird auf dem Benutzergerät zwischengespeichert und am Ende der Sitzung gelöscht.

3. Aktivieren Sie auf dem Server die Richtlinieneinstellung URL-Liste für serverseitigen Flash-Inhaltsabruf und füllen Sie sie mit Ziel-URLs.

Umleiten der Benutzergeräte für clientseitigen Inhaltsabruf an andere Server

Sie können einen Versuch, Flash-Inhalte abzurufen, mit der Einstellung URL-Neuschreibregeln für clientseitigen Inhaltsabruf umleiten. Hierbei handelt es sich um ein Feature der Flash-Umleitung der zweiten Generation. Bei der Konfiguration dieses Features geben Sie zwei URL-Schemas an. Wenn das Benutzergerät versucht, Inhalte von einer Webseite abzurufen, die dem ersten Schema (dem URL-Übereinstimmungsschema) entspricht, werden sie an eine Webseite weitergeleitet, die mit dem zweiten Schema festgelegt wurde (dem Ersetzungsschema).

Mit dieser Einstellung können Sie die Auswirkungen von Inhaltsübermittlungsnetzwerken (Content Delivery Networks,

CDN) kompensieren. Manche Webseiten, die Flash-Inhalte bereitstellen, verwenden CDN-Umleitung, damit Benutzer den Inhalt vom nächstgelegenen Server in einer Gruppe von Servern, auf denen derselbe Inhalt zur Verfügung steht, abrufen können. Bei der Verwendung des clientseitigen Inhaltsabrufs der Flash-Umleitung wird der Flash-Inhalt vom Benutzergerät abgerufen, während der Rest der Webseite, auf der sich der Flash-Inhalt befindet, vom Server abgerufen wird. Wenn CDN verwendet wird, wird die Serveranfrage an den am nächsten gelegenen Server geleitet und die Benutzergerätanfrage geht an denselben Standort. Dies möglicherweise nicht der Speicherort ist, der dem Benutzergerät am nächsten liegt; je nach Entfernung, kann eine sichtbare Verzögerung zwischen dem Laden der Webseite und die Wiedergabe von Flash-Inhalten entstehen.

1. Wählen Sie in der Einstellungsliste den Eintrag URL-Neuschreibregeln für clientseitigen Inhaltsabruf und klicken Sie auf Richtlinieneinstellung.
2. Wählen Sie Nicht konfiguriert, Aktiviert oder Deaktiviert. Nicht konfiguriert ist der Standardwert; Deaktiviert bewirkt, dass alle URL-Neuschreibregeln des nächsten Schrittes ignoriert werden.
3. Wenn Sie die Einstellung aktivieren, klicken Sie auf Anzeigen. Verwenden Sie die Perl-Syntax für reguläre Ausdrücke und geben Sie das URL-Schema im Feld Wert und das neu geschriebene URL-Format im Feld Wert ein.

Angabe erforderlicher Mindestversionen für Flash-Umleitung

Sie können Registrierungseinstellungen hinzufügen, um die erforderliche Mindestversion für die Flash-Umleitung für Clientgeräte festzulegen, die auf VDAs mit Citrix Receiver für Windows oder Citrix Receiver für Linux zugreifen.

> **Warnung**
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und ein erneutes Installieren 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. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.

ServerFlashPlayerVersionMinimum ist ein Zeichenfolgenwert, der die erforderliche Mindestversion des Flash Players auf dem ICA-Server (VDA) angibt.

ClientFlashPlayerVersionMinimum ist ein Zeichenfolgenwert, der die erforderliche Mindestversion des Flash Players auf dem ICA-Client (Citrix Receiver) angibt.

Diese Versionszeichenfolgen können als "10", "10.2" oder "10.2.140" angegeben werden. Zurzeit werden nur die Hauptversions-, Nebenversions- und Buildnummern verglichen. Die Revisionsnummer wird ignoriert. Bei der Angabe von "10" als Versionszeichenfolge mit ausschließlicher Angabe der Hauptversionsnummer wird für die Nebenversions- und Buildnummer von 0 ausgegangen.

FlashPlayerVersionComparisonMask ist ein DWORD-Wert, der, wenn auf 0 festgelegt wird, den Vergleich der Flash Player-Version auf dem ICA-Client mit der auf dem ICA-Server deaktiviert. Die Vergleichsmaske hat auch andere Werte, die jedoch nicht verwendet werden sollten, da sich die Bedeutung jeder Maske mit einem Wert ungleich 0 ändern kann. Es wird empfohlen, die Vergleichsmaske für die gewünschten Clients nur auf 0 festzulegen. Es ist nicht empfehlenswert, die Vergleichsmaske unter den clientagnostischen Einstellungen festzulegen. Wenn keine Vergleichsmaske festgelegt ist, erfordert die Flash-Umleitung auf dem ICA-Client dieselbe Flash Player-Version wie auf dem ICA-Server oder eine höhere Version. Hierfür wird nur die Hauptversionsnummer verglichen.

Für die Umleitung müssen neben der Prüfung anhand der Vergleichsmaske die Prüfungen auf Mindestversion auf Client und Server bestanden werden.

Der Unterschlüssel "ClientID0x51" gibt den Linux-ICA-Client an. Der Unterschlüssel "ClientID0x1" gibt den Windows-ICA-Client an. Der Name des Unterschlüssels entsteht durch Anfügen der hexadezimalen Clientprodukt-ID (ohne führende Nullen) an die Zeichenfolge "ClientID". Eine vollständige Liste der Client-IDs enthält die Dokumentation zum Mobilen SDK für Windows Apps unter http://www.citrix.com/mobilitysdk/docs/clientdetection.html.

Beispiel für eine 32-Bit-VDA-Registrierungskonfiguration

[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer] clientagnostische Einstellungen

"ClientFlashPlayerVersionMinimum"="13.0" Mindestversion für ICA-Client "ServerFlashPlayerVersionMinimum"="13.0" Mindestversion für ICA-Server
[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer\ClientID0x1] Windows-ICA-Client-Einstellungen

"ClientFlashPlayerVersionMinimum"="16.0.0" Gibt die Flash-Player-Mindestversion für den Windows-Client an
[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer\ClientID0x51] Linux-ICA-Clienteinstellungen

"FlashPlayerVersionComparisonMask"=dword:00000000 Deaktiviert den Versionsvergleich für den Linux-Client (Prüfung, um festzustellen, ob die Flash Player-Version auf dem Client neuer ist als auf dem Server)
"ClientFlashPlayerVersionMinimum"="11.2.0" Flash Player-Mindestversion für Linux-Client.

Beispiel für eine 64-Bit-VDA-Registrierungskonfiguration

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer]

"ClientFlashPlayerVersionMinimum"="13.0" "ServerFlashPlayerVersionMinimum"="13.0"
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer\ClientID0x1]

"ClientFlashPlayerVersionMinimum"="16.0.0"
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer\ClientID0x51]

"FlashPlayerVersionComparisonMask"=dword:00000000 "ClientFlashPlayerVersionMinimum"="11.2.0"

HDX 3D Pro

Feb 29, 2016

Mit HDX 3D Pro können Sie Desktops und Anwendungen bereitstellen, die am besten mit einem Grafikprozessor (GPU) für die Hardware-Beschleunigung arbeiten, einschließlich professioneller auf OpenGL und DirectX basierender 3D-Grafikanwendungen. (Der Standard-VDA unterstützt die GPU-Beschleunigung nur für DirectX.)

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 und OpenCL verwenden
- Rechenintensive Nichtgrafik-Anwendungen, die NVIDIA CUDA-GPUs (Compute Unified Device Architecture)für paralleles Computing verwenden

HDX 3D Pro bietet die beste bandbreitenunabhängige Benutzererfahrung:

- Für WAN-Verbindungen: Stellen Sie eine interaktive Benutzererfahrung über WAN-Verbindungen mit geringen Bandbreiten bis zu 1,5 MBit/s bereit.
- LAN-Verbindungen: Stellen Sie eine Benutzererfahrung wie bei einem lokalen Desktop bei LAN-Verbindungen mit Bandbreiten von 100 MBit/s bereit.
  Sie können komplexe und teure Arbeitsstationen durch einfache Benutzergeräte ersetzen, da die Grafikverarbeitung in das Datencenter für eine zentralisierte Verwaltung verschoben wird.

HDX 3D Pro stellt Windows-Desktopbetriebssystemmaschinen und Windows-Serverbetriebssystemmaschinen die GPU-Beschleunigung bereit. HDX 3D Pro bietet vGPU-Beschleunigung für Windows-Desktopbetriebssystemmaschinen bei Verwendung mit Citrix XenServer und NVIDIA GRID-GPUs. Informationen zu den unterstützten XenServer-Versionen finden Sie unter Citrix Virtual GPU Solution.

Mit dem HDX Monitor-Tool, dass das Tool für die Systemdiagnose ersetzt, können Sie den Betrieb und die Konfiguration von HDX-Visualisierungstechnologien überprüfen und HDX-Probleme diagnostizieren und beheben. Das Tool und weitere Informationen stehen unter https://taas.citrix.com/hdx/download zur Verfügung.

GPU-Beschleunigung für Windows Desktopbetriebssysteme

Feb 29, 2016

Mit HDX 3D Pro können Sie grafikintensive Anwendungen als Teil gehosteter Desktops oder Anwendungen auf Desktopbetriebssystemmaschinen bereitstellen. HDX 3D Pro unterstützt physische Hostcomputer (einschließlich Desktop-, Blade- und Rack-Arbeitsstationen), XenServer-VMs mit GPU-Passthrough und XenServer-VMs mit virtuellem GPU (vGPU).

Mit XenServer 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 XenServer vGPU können mehrere virtuelle Maschinen die Grafikverarbeitungsleistung eines einzelnen physischen GPU direkt nutzen. Die echte gemeinsame Hardware-GPU-Nutzung bietet vollständige Windows 7- oder Windows 2008 R2 SP1-Desktops, die für Benutzer mit komplexen und anspruchsvollen Designanforderungen geeignet sind. Die gemeinsame GPU-Nutzung wird für NVIDIA GRID K1- und K2-Karten unterstützt und verwendet die gleichen NVIDIA-Grafiktreiber, die auf nicht-virtualisierten Betriebssystemen bereitgestellt werden.

HDX 3D Pro bietet die folgenden Features:

- Adaptive, auf dem H.264-Standard basierende Tiefenkomprimierung für optimale Leistung bei WAN-Verbindungen und drahtlosen Verbindungen. HDX 3D Pro verwendet die auf CPU basierende Tiefenkomprimierung als Standardkomprimierungsverfahren zur Verschlüsselung. Dadurch wird eine optimale Komprimierung gewährleistet, die sich dynamisch an die Netzwerkbedingungen anpasst.
  Der auf dem H.264-Standard basierende Tiefenkomprimierungscodec konkurriert nicht mehr mit der Grafikwiedergabe um CUDA-Kerne auf der NVIDIA-GPU. Der Tiefenkomprimierungscodec wird auf der CPU ausgeführt und bietet Bandbreiteneffizienz.

- 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. Verlustfreie Komprimierung wird nur für besondere Anwendungsfälle empfohlen, da sie wesentlich mehr Netzwerk- und Verarbeitungsressourcen benötigt.
  Bei Verwendung von verlustfreier Komprimierung:
  - Die Anzeige für Verlustfreiheit, ein Symbol in der Taskleiste, zeigt an, ob es sich bei der Bildschirmanzeige um einen verlustreichen oder verlustfreien Frame handelt. Dies ist hilfreich, wenn die Richtlinieneinstellung Bildqualität auf Zu verlustfrei verbessern festgelegt ist. Die Anzeige für Verlustfreiheit wird grün, wenn die gesendeten Frames verlustfrei sind.
  - Über die Umschaltung für Verlustfreiheit können die Benutzer jederzeit innerhalb der Sitzung in den immer verlustfreien Modus wechseln. Zum Aktivieren oder Deaktivieren des verlustfreien Modus in einer Sitzung können Sie jederzeit mit der rechten Maustaste auf das Symbol klicken oder verwenden Sie die Tastenkombination ALT + UMSCHALT + 1.
    Für verlustfreie Komprimierung: HDX 3D Pro verwendet den verlustfreien Codec für die Komprimierung unabhängig von dem durch die Richtlinie ausgewählten Codec.

    Für die verlustreiche Komprimierung: HDX 3D Pro verwendet den ursprünglichen Codec, entweder den Standard oder den über die Richtlinie ausgewählten Codec.

    Einstellungen für die Umschaltung für Verlustfreiheit werden nicht für zukünftige Sitzungen gespeichert. Wenn Sie für alle Verbindungen den verlustfreien Codec verwenden möchten, legen Sie für die Richtlinie Bildqualität die Einstellung

Immer verlustfrei fest.

- Sie können die Standardtastenkombination ALT + UMSCHALT + 1 zum Aktivieren oder Deaktivieren der Option "Verlustfrei" in einer Sitzung außer Kraft setzen. Konfigurieren Sie eine neue Registrierungseinstellung unter HKLM\SOFTWARE\Citrix\HDX3D\LLIndicator.
  - Name: HKLM_HotKey, Typ: String
  - Das Format beim Konfigurieren einer Tastenkombination ist C=0|1, A=0|1, S=0|1, W=0|1, K=val. Schlüssel müssen durch Kommata (,) getrennt werden. Die Reihenfolge der Tasten ist egal.
  - A, C, S, W und K sind Tasten, wobei Folgendes gilt: C=STRG, A=ALT, S=UMSCHALT, W=Win und K=eine gültige Taste. Zulässige Werte für K sind a-z, 0-9 und jeder virtuelle Tastencode. Weitere Informationen zu virtuellen Tastencodes finden Sie auf MSDN unter Virtual-Key Codes.
  - Beispiel:
    - Taste F10 entspricht K=0x79
    - Taste STRG + F10 entspricht C=1, K=0x79
    - ALT + A entspricht A=1, K=a oder A=1, K=A oder K=A, A=1
    - STRG + ALT + 5 entspricht C=1, A=1, K=5 oder A=1, K=5, C=1
    - STRG + UMSCHALT + F5 entspricht A=1, S=1, K=0x74

  Achtung: Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.

- Unterstützung für mehrere Monitore und hochauflösende Monitore: Für Windows 7- und Windows 8-Desktops unterstützt HDX 3D Pro Benutzergeräte mit bis zu vier Monitoren. Benutzer können ihre Monitore beliebig konfigurieren sowie Monitore mit unterschiedlichen Auflösungen und Ausrichtungen kombinieren. Die Anzahl der Monitore wird nur durch die Leistungsfähigkeit des GPU auf dem Hostcomputer, des Benutzergeräts und der verfügbaren Bandbreite begrenzt. HDX 3D Pro unterstützt alle Monitorauflösungen. Einschränkungen bestehen nur hinsichtlich der Leistungsfähigkeit der GPU auf dem Hostcomputer.
  Auf Windows XP-Desktops bietet HDX 3D Pro eingeschränkte Unterstützung für Dual-Monitor-Zugriff. Weitere Informationen hierzu finden Sie unter VDAs auf Maschinen mit Windows XP oder Windows Vista.

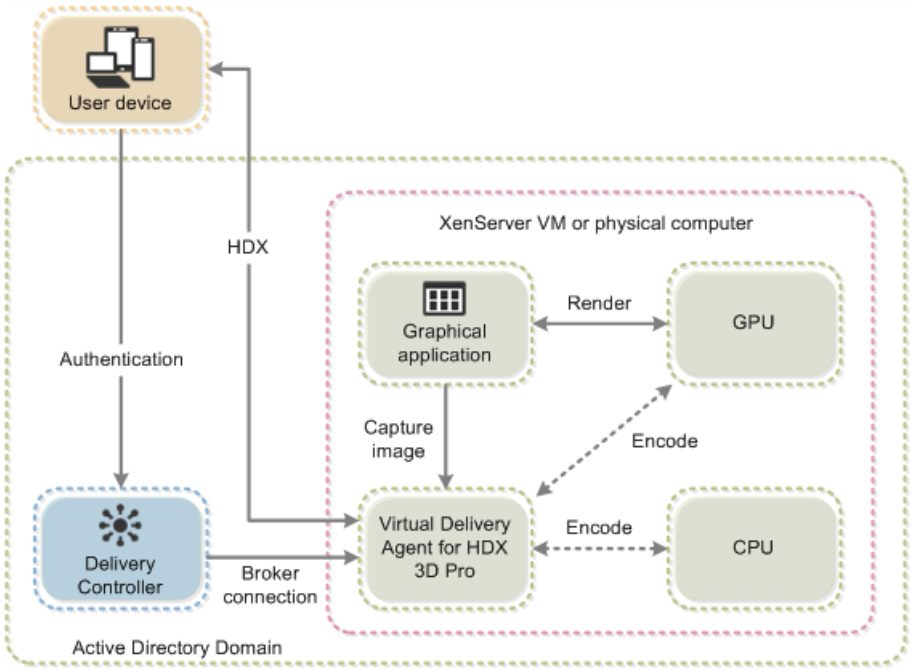
- Dynamische Auflösung: Sie können das Fenster des virtuellen Desktops oder der Anwendung auf eine beliebige Auflösung einstellen.
- Unterstützung für die NVIDIA-Kepler-Architektur. HDX 3D Pro unterstützt die NVIDIA GRID K1- und K2-Karten für GPU-Passthrough und die gemeinsame GPU-Verwendung. Der NVIDIA GRID-vGPU ermöglicht mehreren VMs den gleichzeitigen direkten Zugriff auf einen physischen GPU und die Verwendung derselben NVIDIA-Grafiktreiber, die auf nicht-virtualisierten Betriebssystemen bereitgestellt werden.
- Unterstützung für VMware vSphere und VMware ESX mit Virtual Direct Graphics Acceleration (vDGA): Sie können HDX 3D Pro mit vDGA sowohl für Remotedesktopdienste- als auch für VDI-Arbeitslasten verwenden. Wenn Sie HDX 3D Pro mit Virtual Shared Graphics Acceleration (vSGA) verwenden, wird nur ein Monitor unterstützt. Aufgrund der API-Abfangtechnologie von vSGA können bei der Verwendung mit großen 3D-Modellen Leistungsprobleme auftreten. Weitere Informationen finden Sie unter VMware vSphere 5.1 - Citrix Known Issues.

Wie in der folgenden Abbildung dargestellt:

- Der Hostcomputer muss sich in derselben Active Directory-Domäne wie der Delivery Controller befinden.
- Wenn sich ein Benutzer bei Citrix Receiver anmeldet und auf die virtuelle Anwendung oder den Desktop zugreift,

authentifiziert der Controller den Benutzer und kontaktiert den VDA für HDX 3D Pro, um eine Verbindung zum Computer, der die grafische Anwendung hostet, zu vermitteln.
Der VDA für HDX 3D Pro komprimiert mit der entsprechenden Hardware auf dem Host die Ansicht des gesamten Desktops oder nur der grafischen Anwendung.

- Die Desktop- oder Anwendungsansichten und die dazugehörigen Interaktionen der Benutzer werden zwischen dem Hostcomputer und dem Benutzergerät über eine direkte HDX-Verbindung zwischen Citrix Receiver und VDA für HDX 3D Pro übertragen.



Installieren des VDA für HDX 3D Pro

Wenn Sie mit der grafischen Benutzeroberfläche des Installationsprogramms einen VDA für Windows-Desktopbetriebssysteme installieren, wählen Sie Ja auf der Seite "HDX 3D Pro". Wenn Sie die Befehlszeilenschnittstelle verwenden, schließen Sie die Option /enable_hdx_3d_pro in den Befehl XenDesktop VdaSetup.exe ein.

Für das Upgrade von HDX 3D Pro müssen Sie die separate Komponente HDX 3D für professionelle Grafiken und den VDA deinstallieren, bevor Sie den VDA für HDX 3D Pro installieren. Ebenso müssen Sie zum Wechsel vom standardmäßigen VDA zum VDA für HDX 3D Pro vor der Installation von VDA für HDX 3D Pro den standardmäßigen VDA deinstallieren.

Installieren und Aktualisieren von NVIDIA-Treibern

Die NVIDIA GRID-API bietet direkten Zugriff auf den Framepuffer des Grafikprozessors und bietet die schnellste Framerate für eine gleichmäßige und interaktive Benutzererfahrung. Wenn Sie NVIDIA-Treiber vor einem VDA mit HDX 3D Pro installieren, ist NVIDIA GRID standardmäßig aktiviert.

Zum Aktivieren von NVIDIA GRID auf einer virtuellen Maschine müssen Sie den Microsoft Basic Display Adapter im Geräte-Manager deaktivieren. Führen Sie den folgenden Befehl aus und starten Sie dann den VDA neu: Montereyenable.exe –enable –noreset

Wenn Sie NVIDIA-Treiber nach einem VDA mit HDX 3D Pro installieren, ist NVIDIA GRID deaktiviert. Aktivieren Sie NVIDIA GRID mit dem von NVIDIA bereitgestellten Tool Montereryenable.

Führen Sie den folgenden Befehl aus, um NVIDIA GRID zu deaktivieren, und starten Sie dann den VDA neu:
Montereyenable.exe –disable –noreset

Optimierung der HDX 3D Pro-Benutzererfahrung

Stellen Sie bei der Verwendung von HDX 3D Pro mit mehreren Monitoren sicher, dass der Hostcomputer mit mindestens so vielen Monitoren konfiguriert ist, wie an den Geräten der Benutzer angeschlossen sind. Die an den Hostcomputer angeschlossenen Monitore können physikalische oder virtuelle Monitore sein.

Schließen Sie Monitore (physikalische oder virtuelle) nicht an Hostcomputer an, während Benutzer mit dem virtuellen Desktop oder der virtuellen Anwendung, die die grafische Anwendung bereitstellen, verbunden sind. Dies kann für die Dauer der Benutzersitzung zu Instabilität führen.

Teilen Sie den Benutzern mit, dass das Ausführen von Änderungen (von ihnen oder einer Anwendung) an der Desktopauflösung, während eine grafische Anwendungssitzung ausgeführt wird, nicht unterstützt wird. Nach dem Beenden der Anwendungssitzung können Benutzer die Auflösung des Desktop Viewer-Fensters in "Citrix Receiver - Desktop Viewer-Einstellungen" ändern.

Wenn mehrere Benutzer eine Verbindung mit beschränkter Bandbreite gemeinsam verwenden, z. B. in einer Zweigstelle, empfiehlt Citrix die Verwendung der Richtlinieneinstellung Bandbreitenlimit für Sitzung insgesamt, um die für die einzelnen Benutzer verfügbare Bandbreite zu beschränken. Damit wird sichergestellt, dass die verfügbare Bandbreite beim Anmelden und Abmelden der Benutzer keinen großen Schwankungen unterworfen ist. Da HDX 3D Pro automatische Anpassungen durchführt, um die gesamte Bandbreite auszuschöpfen, kann sich die stark variierende verfügbare Bandbreite während der Benutzersitzungen negativ auf die Leistung auswirken.

Wenn beispielsweise 20 Benutzer eine Verbindung mit 60 MBit/s gemeinsam verwenden, kann die Bandbreite, die den einzelnen Benutzern zur Verfügung steht, abhängig von der Anzahl der gleichzeitigen Benutzer zwischen 3 MBit/s und 60 MBit/s variieren. Um die Benutzererfahrung in diesem Szenario zu optimieren, legen Sie die Bandbreite fest, die zu Spitzenzeiten pro Benutzer erforderlich ist, und stellen Sie sicher, dass die Benutzer diesen Wert nicht überschreiten können.

Citrix empfiehlt Benutzern einer 3D-Maus, die Priorität des virtuellen Kanals für die generische USB-Umleitung auf 0 zu erhöhen. Weitere Informationen dazu, wie Sie die Priorität virtueller Kanäle ändern können, finden Sie unter CTX128190.

GPU-Beschleunigung für Windows-Serverbetriebssystem

Feb 29, 2016

Mit HDX 3D Pro können grafikintensive Anwendungen, die in Windows-Serverbetriebssystemsitzungen ausgeführt werden, auf der GPU des Servers wiedergegeben werden. Beim Verlagern der Wiedergabe von OpenGL, DirectX, Direct3D und Windows Presentation Foundation auf den GPU des Servers wird die CPU des Servers nicht durch die Grafikwiedergabe verlangsamt. Zusätzlich kann der Server so mehr Grafiken verarbeiten, weil die Arbeitslast zwischen Prozessor und Grafikprozessor aufgeteilt wird.

Bei Verwendung von HDX 3D Pro können mehrere Benutzer eine Grafikkarte gemeinsam verwenden. Wenn HDX 3D Pro mit XenServer GPU-Passthrough verwendet wird, hostet ein Server mehrere Grafikkarten, d. h. eine pro virtuelle Maschine.

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. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.

GPU Sharing

GPU Sharing ermöglicht die GPU-Hardwarewiedergabe von OpenGL- und DirectX-Anwendungen in Remotedesktopsitzungen und hat die folgenden Merkmale:

- Verwenden auf Bare-Metal- oder virtuellen Maschinen, um die Anwendungsskalierbarkeit und -leistung zu steigern.
- Mehrere gleichzeitige Sitzungen können GPU-Ressourcen gemeinsam verwenden. (Die meisten Benutzer benötigen nicht die Wiedergabeleistung eines dedizierten GPU).
- Erfordert keine besonderen Einstellungen.

Für DirectX-Anwendungen wird standardmäßig nur ein GPU verwendet. Dieser GPU wird von mehreren Benutzern gemeinsam genutzt. Die Zuordnung von Sitzungen auf mehreren GPUs mit DirectX- ist noch im Versuchsstadium und erfordert Registrierungsänderungen. Weitere Informationen erhalten Sie vom Citrix Support.

Sie können mehrere GPUs auf einem Hypervisor installieren und jedem GPU eine VM zuordnen: entweder durch Installation einer Grafikkarte mit mehreren GPUs oder durch Installation mehrerer Grafikkarten mit einem oder mehreren GPUs. Eine Mischung heterogener Grafikkarten auf einem Server wird nicht empfohlen.

Virtuelle Maschinen benötigen einen direkten Passthrough-Zugriff auf einen GPU; dies ist mit Citrix XenServer oder VMware vSphere verfügbar. Wenn HDX 3D mit GPU-Passthrough verwendet wird, unterstützt jeder GPU des Servers eine virtuelle Maschine mit mehreren Benutzern.

GPU Sharing hängt nicht von einer bestimmten Grafikkarte ab.

- Wählen Sie bei Ausführung auf einem Hypervisor eine Hardwareplattform und Grafikkarten aus, die mit der Implementierung von GPU-Passthrough des Hypervisors kompatibel sind. Die Liste der Hardware, die Zertifizierungstests mit XenServer GPU-Passthrough bestanden hat, finden Sie unter GPU-Passthroughgeräte.
- Bei Ausführung auf Bare-Metal verteilt das System die Benutzersitzungen auf alle geeigneten Grafikprozessoren. Um sicherzustellen, dass alle installierten Grafikprozessoren geeignet sind, verwenden Sie identische Grafikprozessoren.

Die Skalierbarkeit mit GPU Sharing hängt von folgenden Faktoren ab:

- Ausgeführte Anwendungen
- Verbrauchter Videospeicher
- Verarbeitungsleistung der Grafikkarte

Beispiel: Skalierbarkeitswerte im Bereich von 8 bis 10 Benutzern wurden für NVIDIA Q6000- und M2070Q-Karten berichtet, die Anwendungen wie ESRI ArcGIS ausführen. Diese Karten haben 6 GB Videospeicher. Neuere NVIDIA GRID-Karten haben 8 GB Videospeicher und eine wesentlich höhere Verarbeitungsleistung (mehr CUDA-Kerne). Bei NVIDIA GRID K2-Karten wurde bei bis zu 20 Benutzern pro GRID K2-Karte eine gute Leistung beobachtet. Bei anderen Anwendungen kann die Skalierbarkeit wesentlich höher liegen; sie können 32 gleichzeitige Benutzer bei einem Profi-GPU erreichen.

Einige Anwendungen handhaben fehlenden Videospeicher besser als andere. Wenn die Hardware stark überlastet wird, kann der Grafikkartentreiber instabil werden oder abstürzen. Schränken Sie die Anzahl der gleichzeitigen Benutzer ein, um diese Probleme zu vermeiden.

Sie können die GPU-Beschleunigung mit einem Tool von Drittanbietern bestätigen, z. B. GPU-Z. GPU-Z finden Sie unter http://www.techpowerup.com/gpuz/.

Wiedergabe von DirectX, Direct3D und WPF

Die Wiedergabe von DirectX, Direct3D und WPF steht nur auf Servern zur Verfügung, die einen Grafikprozessor haben, der eine Anzeigetreiberschnittstelle der Version 9ex, 10 oder 11 unterstützt.

- Unter Windows Server 2008 R2 sind für DirectX und Direct3D keine Sondereinstellungen erforderlich, um einen einzelnen GPU zu verwenden.
- Unter Windows Server 2012 verwenden Remotedesktopdienste-Sitzungen auf dem RD-Sitzungshostserver als Standardadapter den Microsoft Basic Render-Treiber. Um den GPU in RDS-Sitzungen unter Windows Server 2012 zu verwenden, aktivieren Sie die Einstellung Use the hardware default graphics adapter for all Remote Desktop Services sessions in der Gruppenrichtlinie "Lokale Computerrichtlinie > Computerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Remotedesktopdienste > Remotedesktop-Sitzungshost > Remotesitzungsumgebung".
- Unter Windows Server 2008 R2 und Windows Server 2012 verwenden alle DirectX- und Direct3D-Anwendungen in allen Sitzungen standardmäßig den gleichen einzelnen GPU. Um die Unterstützung für ein experimentelles Feature zu aktivieren, das die Benutzersitzungen für DirectX- und Direct3D-Anwendungen auf alle geeigneten GPUs verteilt, erstellen Sie die folgenden Einstellungen in der Registrierung des Servers, auf dem die Windows-Serverbetriebssystemsitzungen ausgeführt werden:
  - [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_Dlls\Graphics Helper] "DirectX"=dword:00000001
  - [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper] "DirectX"=dword:00000001
- Um die Wiedergabe von WPF-Anwendungen mit der GPU des Servers zu aktivieren, müssen Sie in der Registrierung des Servers, der die Windows-Serverbetriebssystemsitzungen ausführt, die folgenden Einstellungen erstellen:
  - [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_Dlls\Multiple Monitor Hook] "EnableWPFHook"=dword:00000001
  - [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\ Multiple Monitor Hook] "EnableWPFHook"=dword:00000001

Experimentelle GPU-Beschleunigungsfunktion für CUDA- oder OpenCL-Anwendungen

Experimentelle Unterstützung wird bereitgestellt für GPU-Beschleunigung von CUDA- und OpenCL-Anwendungen, die in einer Benutzersitzung ausgeführt werden. Diese Unterstützung ist in der Standardeinstellung deaktiviert, Sie können sie jedoch für Test- und Evaluierungszwecke aktivieren.

Aktivieren Sie die folgenden Registrierungseinstellungen, um die experimentellen CUDA-Beschleunigungsfeatures zu verwenden:

- [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_Dlls\Graphics Helper] "CUDA"=dword:00000001
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper] "CUDA"=dword:00000001

Aktivieren Sie die folgenden Registrierungseinstellungen, um die experimentellen OpenCL-Beschleunigungsfeatures zu verwenden:

- [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_Dlls\Graphics Helper] "OpenCL"=dword:00000001
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper] "OpenCL"=dword:00000001

OpenGL Software Accelerator

Feb 29, 2016

OpenGL Software Accelerator ist ein Softwarerasterizer für OpenGL-Anwendungen wie ArcGIS, Google Earth, Nehe, Maya, Blender, Voxler, CAD und CAM. In einigen Fällen bietet OpenGL Software Accelerator auch ohne die Verwendung einer Grafikkarte eine gute Benutzererfahrung mit OpenGL-Anwendungen.

Wichtig: OpenGL Software Accelerator wird ohne Modifikation bereitgestellt und muss für alle Anwendungen getestet werden. Er funktioniert möglicherweise mit einigen Anwendungen nicht, kann aber als Lösung dienen, wenn der Windows OpenGL-Rasterizer keine angemessene Leistung bietet. Wenn OpenGL Software Accelerator mit Ihren Anwendungen funktioniert, kann es Ihnen Kosten für GPU-Hardware sparen.

OpenGL Software Accelerator ist im Ordner "Support" auf dem Installationsmedium und wird auf allen gültigen VDA-Plattformen unterstützt.

Einsatzmöglichkeiten für OpenGL Software Accelerator

- Wenn die Leistung von OpenGL-Anwendungen in virtuellen Maschinen auf XenServer oder anderen Hypervisors unzureichend ist, verwenden Sie OpenGL Accelerator. Bei einigen Anwendungen werden mit OpenGL Accelerator durch den Einsatz von SSE4.1 und AVX bessere Ergebnisse erzielt als mit dem in Windows enthaltenen Microsoft OpenGL Rasterizer. OpenGL Accelerator unterstützt zudem Anwendungen, die OpenGL-Versionen bis 2.1 verwenden.
- Bei Anwendungen, die auf einer Arbeitsstation ausgeführt werden, sollte zunächst die Standardversion von OpenGL verwendet werden, die von der Arbeitsstation des Grafikadapters bereitgestellt wird. Wenn es sich um eine aktuelle Grafikkarte handelt, wird damit in den meisten Fällen die beste Leistung erzielt. Bei Grafikkarten älterer Versionen oder weniger leistungsstarken Grafikkarten sollte OpenGL Software Accelerator eingesetzt werden.
- 3D OpenGL-Anwendungen, die nicht angemessen bereitgestellt wurden und CPU-basierte Softwarerasterisierung verwenden, profitieren möglicherweise von der OpenGL GPU-Hardwarebeschleunigung. Dieses Feature kann auf Bare-Metal- oder virtuellen Maschinen verwendet werden.

Audiofeatures

Feb 29, 2016

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 in den Artikeln Einstellungen der Richtlinie "Audio", Einstellungen der Richtlinie "Bandbreite" und Einstellungen der Richtlinie "Multistreamverbindungen".

Wichtig: Die meisten Audiofeatures werden über den ICA-Stream transportiert und werden auf dieselbe Weise gesichert wie anderer ICA-Datenverkehr. Bei UDP (User Datagram Protocol) wird ein separater, ungesicherter Übertragungsmechanismus verwendet, wenn NetScaler Access Gateway nicht im Pfad ist. Ist NetScaler Access Gateway für den Zugriff auf XenApp- und XenDesktop-Ressourcen konfiguriert, wird der Audioverkehr zwischen Endpunktgerät und NetScaler Access Gateway mittels DTLS gesichert.

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 Audioqualität auf Hoch - High Definition-Audio eingestellt. Diese Einstellung bietet HiFi-Stereo-Audio, verbraucht aber mehr Bandbreite als die anderen Einstellungen. Verwenden Sie diese Audioqualität nicht für nicht optimierte Chat- und Videochat-Anwendungen (z. B. Softphones), da es hierbei zu Verzögerungen im Audiopfad kommen kann, was bei Echtzeitkommunikation ungeeignet ist.

Sie können auch die Erstellung separater Richtlinien für Benutzergruppen mit Einwählverbindungen und für Benutzer, die über ein LAN oder WAN eine Verbindung herstellen, in Erwägung ziehen. Benutzern ist bei DFÜ-Verbindungen, bei denen die Bandbreite im Allgemeinen begrenzt ist, die Download-Geschwindigkeit gewöhnlich wichtiger als die Audioqualität. Erstellen Sie daher für DFÜ-Verbindungen eine Richtlinie, die für Audio einen hohen Komprimierungsgrad anwendet, sowie eine weitere Richtlinie für LAN- oder WAN-Verbindungen, die einen geringen Komprimierungsgrad anwendet.

Informationen zu Einstellungen finden Sie unter Einstellungen der Richtlinie "Audio". Denken Sie daran, die Clientaudioeinstellungen auf dem Benutzergerät zu aktivieren (siehe Audioeinstellungsrichtlinien für Benutzergeräte).

Clientaudioumleitung

Damit der Audioempfang von einer Anwendung auf dem Server über Lautsprecher oder andere Soundgeräte (z. B. Kopfhörer) auf dem Benutzergerät zugelassen wird, fügen Sie die Einstellung Clientaudioumleitung hinzu, die standardmäßig zugelassen ist.

Die Clientaudiozuordnung kann dazu führen, dass eine hohe Last auf dem Server und dem Netzwerk entsteht. Durch Nichtzulassen der Clientaudioumleitung werden jedoch alle HDX-Audiofunktionen deaktiviert.

Informationen zu Einstellungen finden Sie unter Einstellungen der Richtlinie "Audio". Denken Sie daran, die Clientaudioeinstellungen auf dem Benutzergerät zu aktivieren (siehe Audioeinstellungsrichtlinien für Benutzergeräte).

Clientmikrofonumleitung

Damit die Audioaufzeichnung mit Eingabegeräten wie Mikrofonen auf dem Benutzergerät zugelassen wird, fügen Sie die Einstellung Clientmikrofonumleitung hinzu, die standardmäßig zugelassen ist.

Aus Sicherheitsgründen werden Benutzer darauf hingewiesen, wenn Server, die keine vertrauenswürdige Beziehung zu den Benutzergeräten haben, auf Mikrofone zugreifen und können dann den Zugriff vor Verwenden des Mikrofons akzeptieren oder ablehnen. Benutzer können die diesbezügliche Warnung in Citrix Receiver deaktivieren.

Informationen zu Einstellungen finden Sie unter Einstellungen der Richtlinie "Audio". Denken Sie daran, die Clientaudioeinstellungen auf dem Benutzergerät zu aktivieren (siehe Audioeinstellungsrichtlinien für Benutzergeräte).

Audio Plug & Play

Die Richtlinie Audio Plug & Play steuert, ob mehrere Audiogeräte zum Aufzeichnen und Wiedergeben zulässig sind. Diese Einstellung ist standardmäßig aktiviert.

Diese Einstellung gilt nur für Windows-Serverbetriebssystemmaschinen.

Informationen zu Einstellungen finden Sie unter Einstellungen der Richtlinie "Audio".

Bandbreitenlimit für die Audioumleitung und Bandbreitenlimit für die Audioumleitung (Prozent)

Die Richtlinieneinstellung Bandbreitenlimit für die Audioumleitung gibt die maximale Bandbreite (in Kilobits pro Sekunde) für die Wiedergabe und Aufzeichnung von Audio in einer Sitzung an. Die Einstellung Bandbreitenlimit für die Audioumleitung (Prozent) gibt die maximale Bandbreite für die Umleitung als Prozentsatz der insgesamt verfügbaren Bandbreite an. Standardmäßig ist Null (Maximum) für beide Einstellungen angegeben. Wenn beide Einstellungen konfiguriert sind, wird die Einstellung mit dem niedrigsten Bandbreitenlimit verwendet.

Informationen zu Einstellungen finden Sie unter Einstellungen der Richtlinie "Bandbreite". Denken Sie daran, die Clientaudioeinstellungen auf dem Benutzergerät zu aktivieren (siehe Audioeinstellungsrichtlinien für Benutzergeräte).

Audio über UDP - Real-time Transport und Audio-UDP-Portbereich

Standardmäßig ist Audio über UDP - Real-time Transport auf "Zugelassen" eingestellt (sofern die entsprechende Option bei der Installation ausgewählt wurde), sodass ein UDP-Port auf dem Server für alle Verbindungen geöffnet wird, die für die Echtzeitübertragung von Audio über UDP konfiguriert wurden. Citrix empfiehlt, dass Sie UDP/RTP für Audio konfigurieren, um auch bei Netzwerküberlastung oder Paketverlust die beste Benutzererfahrung sicherzustellen.
Wichtig: Mit UDP übertragene Audiodaten werden nicht verschlüsselt, wenn NetScaler Access Gateway nicht im Pfad ist. Ist NetScaler Access Gateway für den Zugriff auf XenApp- und XenDesktop-Ressourcen konfiguriert, wird der Audioverkehr zwischen Endpunktgerät und NetScaler Access Gateway mittels DTLS gesichert.
Mit der Einstellung Audio-UDP-Portbereich geben Sie den Bereich der Portnummern an, die der Virtual Delivery Agent (VDA) zum Austausch von Audiopaketdaten mit dem Benutzergerät verwendet.

Standardmäßig ist der Bereich 16500 bis 16509.

Informationen zu den Einstellungen von "Audio über UDP - Real-time Transport" finden Sie unter Einstellungen der Richtlinie "Audio". Informationen zu "Audio-UDP-Portbereich" finden Sie unter Einstellungen der Richtlinie "Multistreamverbindungen". Denken Sie daran, die Clientaudioeinstellungen auf dem Benutzergerät zu aktivieren (siehe Audioeinstellungsrichtlinien für Benutzergeräte).

Audioeinstellungsrichtlinien für Benutzergeräte

1. Laden Sie die Gruppenrichtlinienvorlagen gemäß den Anweisungen unter in Konfigurieren von Receiver mit der Gruppenrichtlinienobjektvorlage herunter.
2. Erweitern Sie im Gruppenrichtlinien-Editor "Administrative Vorlagen > Citrix Komponenten> Citrix Receiver > Benutzerfreundlichkeit".

3. Wählen Sie für **Clientaudioeinstellungen** die Option **Nicht konfiguriert**, **Aktiviert** oder **Deaktiviert**.
   - **Nicht konfiguriert**: Standardmäßig ist die Audioumleitung mit hoher Qualität oder zuvor konfigurierten benutzerdefinierten Audioeinstellungen aktiviert.
   - **Aktiviert**: Die Audioumleitung wird mit den ausgewählten Optionen aktiviert.
   - **Deaktiviert**: Die Audioumleitung wird deaktiviert.
4. Wenn Sie **Aktiviert** festlegen, wählen Sie eine Audioqualität. Verwenden Sie für UDP-Audio die Standardeinstellung **Mittel**.
5. Aktivieren Sie nur für UDP-Audio die Einstellung **Real-Time Transport** und legen Sie den Bereich der eingehenden Ports so fest, dass der Durchgang durch die lokale Windows-Firewall gewährleistet ist.
6. Zur Verwendung von UDP-Audio mit NetScaler Access Gateway wählen Sie die Option **Allow Real-Time Transport Through gateway**. NetScaler Access Gateway muss mit DTLS konfiguriert werden. Weitere Informationen finden Sie unter UDP Audio Through a Netscaler Gateway.

Wenn Sie als Administrator auf Endpunktgeräten solche Änderungen nicht vornehmen können (beispielsweise im Fall von BYOD-Geräten oder Heimcomputern), aktivieren Sie UDP-Audio über die default.ica-Attribute von StoreFront.

1. Öffnen Sie auf dem Computer mit StoreFront die Datei C:\inetpub\wwwroot\Citrix\\App_Data\default.ica in einem Texteditor.
2. Fügen Sie unter dem Abschnitt [Application] Folgendes hinzu:

```
command
; This is to enable Real-Time Transport

EnableRtpAudio=true

; This is to Allow Real-Time Transport Through gateway

EnableUDPThroughGateway=true

; This is to set audio quality to Medium

AudioBandwidthLimit=1-

; UDP Port range

RtpAudioLowestPort=16500

RtpAudioHighestPort=16509
```

KOPIEREN

Wird UDP-Audio über die Datei default.ica aktiviert, gilt die Aktivierung für alle Benutzer des Stores.

Vermeiden von Echo in Multimediakonferenzen

Teilnehmer von Audio- oder Videokonferenzen hören eventuell ein Echo. Echos treten normalerweise auf, wenn der Abstand zwischen Lautsprechern und Mikrofonen nicht groß genug ist. Aus diesem Grund empfiehlt Citrix, dass Sie für Audio- und Videokonferenzen Kopfhörer verwenden.

HDX verfügt über eine Option zur Echounterdrückung (standardmäßig aktiviert), die das Auftreten von Echo minimiert. Die Qualität der Echounterdrückung hängt stark vom Abstand zwischen den Lautsprechern und dem Mikrofon ab. Der Abstand zwischen den Geräten darf nicht zu groß aber auch nicht zu klein sein.

Sie können eine Registrierungseinstellung ändern, um die Echounterdrückung zu deaktivieren. 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. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.

1. Navigieren Sie mit dem Registrierungs-Editor auf dem Benutzergerät zu einer der folgenden Optionen:
   - 32-Bit-Computer: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio\EchoCancellation
   - 64-Bit-Computer: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio\EchoCancellation
2. Ändern Sie den Wert im Feld Wert zu FALSE.

Prioritäten für den Netzwerkdatenverkehr

Feb 29, 2016

Prioritäten für den Netzwerkdatenverkehr über mehrere Verbindungen für eine Sitzung werden zugewiesen, indem Diensteigenschaft(QoS)-fähige Router verwendet werden. Vier TCP/IP-Streams (real-time, interactive, background und bulk) und ein UDP/RTP-Stream (für Voice) sind zum Ausführen von ICA-Datenverkehr zwischen dem Benutzergerät und dem Server verfügbar. Jeder virtuelle Kanal ist mit einer bestimmten Priorität verknüpft und wird von der entsprechenden TCP-Verbindung transportiert. Sie können die Kanäle basierend auf der Portnummer, die für die Verbindung verwendet wird, unabhängig voneinander festlegen.

Gestreamte Mehrkanalverbindungen werden für Virtual Delivery Agents (VDAs) unterstützt, die auf Windows 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.

Achtung: Verwenden Sie Transportsicherheit, wenn Sie dieses Feature einsetzen. Citrix empfiehlt die Verwendung von Internetprotokollsicherheit (IPsec) oder Transport Layer Security (TLS). TLS-Verbindungen werden nur unterstützt, wenn die Verbindungen durch ein NetScaler Gateway passieren, das Multistream 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 eine Priorität aus der Liste CGP-Standardportpriorität 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 sowie entsprechende Prioritäten ein. 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 Cloudbridge mit Multistream-Unterstützung in Ihrer Umgebung verwenden, müssen Sie diese Einstellung nicht konfigurieren. Konfigurieren Sie diese Richtlinieneinstellung, wenn Sie Router von Drittanbietern oder Legacy-Branch Repeater verwenden, um die gewünschte Quality of Service (QoS) zu erzielen.
- Multistreambenutzereinstellung: Diese Einstellung ist standardmäßig deaktiviert.

Damit die Richtlinien mit diesen Einstellungen wirksam werden, müssen sich Benutzer abmelden und dann am Netzwerk anmelden.

Überlegungen zu USB und Clientlaufwerk

Feb 29, 2016

Mit HDX USB-Geräteumleitung können Benutzer eine Verbindung zum USB-Flashlaufwerk auf einem lokalen Computer herstellen und dann remote von einem virtuellen Desktop oder einer desktopgehosteten Anwendung darauf zugreifen. Während einer Sitzung können Benutzer Plug-n-Play-Geräte verwenden, einschließlich PTP-Geräte (Picture Transfer Protocol) wie digitale Kameras, MTP-Geräte (Media Transfer Protocol) wie digitale Audio Player oder tragbare Media Player und POS-Geräte (Point of Sale).

Double-Hop-USB wird bei Sitzungen mit über Desktop gehosteten Anwendungen nicht unterstützt.

USB-Umleitung ist verfügbar für Citrix Receiver für Windows und Citrix Receiver für Linux.

Standardmäßig ist die USB-Umleitung für bestimmte Klassen von USB-Geräten zulässig bzw. nicht zulässig. Weitere Informationen hierzu finden Sie in der Citrix Receiver-Dokumentation. Sie können festlegen, welche USB-Geräte einem virtuellen Desktop verfügbar gemacht werden, indem Sie die Liste der unterstützten USB-Geräte für die Umleitung beschränken.

> **Important**
>
> In Umgebungen, in denen aus Sicherheitsgründen eine Trennung zwischen dem Benutzergerät und dem Server erforderlich ist, müssen Sie die Benutzer darüber informieren, welche Typen von USB-Geräten zu vermeiden sind.

Die beliebtesten USB-Geräte können über optimierte virtuelle Kanäle umgeleitet werden und liefern Leistung und Bandbreiteneffizienz über ein WAN. Der Grad der Unterstützung hängt vom auf dem Benutzergerät installierten Citrix Receiver ab. Optimierte virtuelle Kanäle sind normalerweise die beste Option, insbesondere in Umgebungen mit hoher Latenz.

Für die Umleitung von USB-Geräten gilt, dass ein SMART-Board ebenso wie eine Maus behandelt wird.

Das Produkt unterstützt die Verwendung von optimierten virtuellen Kanälen mit USB 3.0-Geräten und USB 3.0-Ports, wie ein virtueller CDM-Kanal, der zum Anzeigen von Dateien auf einer Kamera oder zur Audiowiedergabe über ein Headset verwendet wird. Das Produkt unterstützt zudem die generische USB-Umleitung von USB 3.0-Geräten, die mit einem USB 2.0-Port verbunden sind.

Spezialgeräte, für die es keine optimierten virtuellen Kanäle gibt, werden durch die Verwendung eines allgemeinen virtuellen Kanals für USB unterstützt, der eine unformatierte USB-Umleitung bietet. Informationen zu allen mit XenDesktop getesteten USB-Geräten finden Sie unter CTX123569.

Einige erweiterte gerätespezifischen Features, wie z. B. auf HID-Schaltflächen (Human Interface Device) auf einer Webcam, funktionieren möglicherweise mit dem optimierten virtuellen Kanal nicht wie erwartet. Wenn dies ein Problem darstellt, können Sie den allgemeinen virtuellen Kanal für USB verwenden.

Einige Geräte werden standardmäßig nicht umgeleitet und sind nur in der lokalen Sitzung verfügbar. Es wäre beispielsweise nicht angemessen, eine über internes USB an der Hauptplatine des Benutzergeräts angeschlossene Netzwerkkarte umzuleiten.

Die folgenden Citrix Richtlinieneinstellungen steuern die USB-Unterstützung:

- **Regeln für die Client-USB-Geräteoptimierung:** Der Optimierungsmodus wird für Eingabegeräte der Klasse 3 ("class=03") unterstützt, z. B. Signaturgeräte und Grafiktablets. Wenn keine Regel angegeben ist, wird das Gerät im interaktiven Modus behandelt (02). Aufnahmemodus (04) ist der empfohlene Modus für Signaturgeräte.
- **Client-USB-Geräteumleitung:** Die Standardeinstellung ist Nicht zugelassen.
- **Regeln für die Client-USB-Geräteumleitung:** Die Regeln gelten nur für Geräte, die generische USB-Umleitung verwenden, und nicht für Geräte, die spezielle oder optimierte Umleitung verwenden, wie CDM.
- **Client-USB-Geräteumleitung für Plug & Play-Geräte:** Die Standardeinstellung Zugelassen ermöglicht Plug & Play von PTP-, MTP- und POS-Geräten in einer Sitzung.
- **Bandbreitenlimit für Client-USB-Geräteumleitung:** Der Standardwert ist 0 (kein Maximum).
- **Bandbreitenlimit für Client-USB-Geräteumleitung (Prozent):** Der Standardwert ist 0 (kein Maximum).

Info zur generischen USB-Umleitung

Generische USB-Umleitung ist für spezielle USB-Geräte, für die es keinen optimierten virtuellen Kanal gibt. Diese Funktion leitet beliebige USB-Geräte von Clientmaschinen an virtuelle Desktops um. Durch dieses Feature können Endbenutzer mit vielen generischen USB-Geräten in der Desktopsitzung so interagieren, als wären die Geräte direkt angeschlossen.

Vorteile von generischer USB-Umleitung:

- Benutzer müssen keine Gerätetreiber auf den Benutzergeräten installieren.
- USB-Clienttreiber werden auf der VDA-Maschine installiert.

Dieses Feature wird für Desktopsitzungen auf VDAs für Desktop-OS ab Version 7.6 unterstützt.

Dieses Feature wird mit den folgenden Einschränkungen auch für Desktopsitzungen auf VDAs für Server-OS ab Version 7.6 unterstützt:

- Auf der VDA-Maschine muss Windows Server 2012 R2 ausgeführt werden
- Nur Single-Hop-Szenarios werden unterstützt
- Die USB-Clienttreiber müssen mit RDSH für Windows 2012 R2 kompatibel sein
- USB-Speichergeräte, Audiogeräte, Smartcardleser und Geräte, die nicht voll virtualisiert sind, werden nicht unterstützt

Weitere Informationen zur generischen USB-Umleitung finden Sie unter CTX137939.

Aktivieren von USB-Unterstützung

1. Fügen Sie die Einstellung Client-USB-Geräteumleitung einer Richtlinie hinzu und stellen Sie den Wert auf Zugelassen ein.
2. (Optional) Zum Aktualisieren der für Remoting verfügbaren USB-Geräteliste fügen Sie die Einstellung Regeln für die Client-USB-Geräteumleitung einer Richtlinie hinzu und stellen Sie die USB-Standardrichtlinienregeln ein.
3. Aktivieren Sie die USB-Unterstützung, wenn Sie Citrix Receiver auf Benutzergeräten installieren. Wenn Sie im vorigen Schritt die USB-Richtlinienregeln für den VDA festgelegt haben, geben Sie nun die gleichen Richtlinienregeln für Citrix Receiver ein. Informationen zur USB-Unterstützung Für Thin Clients und die erforderliche Konfiguration erhalten Sie vom Hersteller.

Aktualisieren der für Remoting verfügbaren USB-Geräteliste (Citrix Receiver für Windows 4.2)

USB-Geräte werden automatisch umgeleitet, wenn die USB-Unterstützung aktiviert ist und die USB-Einstellungen für eine automatische Verbindung der USB-Geräte konfiguriert wurden. USB-Geräte werden auch automatisch umgeleitet, wenn das Gerät im Modus "Desktop Appliance" ist und der Verbindungsbalken nicht angezeigt wird. In manchen Fällen empfiehlt es sich jedoch, die automatische Umleitung nicht für alle USB-Geräte zu aktivieren. Weitere Informationen finden Sie unter CTX123015.

Benutzer können Geräte, die nicht automatisch umgeleitet werden, explizit umleiten, indem sie sie aus der USB-Geräteliste auswählen. Um zu verhindern, dass Geräte überhaupt aufgeführt oder umgeleitet werden, können Sie auf dem Client und für VDA die nachfolgenden Geräteregeln festlegen.

Sie können die USB-Geräte, die für Remoting verfügbar sind, aktualisieren, indem Sie Regeln für die Client-USB-Geräteumleitung für Citrix Receiver und VDA definieren, die dann die USB-Standardrichtlinienregeln außer Kraft setzen.

- Bearbeiten Sie die Benutzergeräteregistrierung. Eine administrative Vorlage (ADM-Datei) ist auf dem Installationsmedium enthalten, sodass Sie das Gerät über die Active Directory-Gruppenrichtlinie ändern können: dvd root \os\lang\Support\Configuration\icaclient_usb.adm.
- Bearbeiten Sie die Administrator-Überschreibungsregeln der Serverbetriebssystemmaschinen mit den Gruppenrichtlinienregeln. Die Gruppenrichtlinien-Verwaltungskonsole ist auf dem Installationsmedium enthalten:
  - Für x64: dvd root \os\lang\x64\Citrix Policy\ CitrixGroupPolicyManagement_x64.msi
  - Für x86: dvd root \os\lang\x86\Citrix Policy\ CitrixGroupPolicyManagement_x86.msi

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. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.

Die Produktstandardregeln sind in HKLM\SOFTWARE\Citrix\PortICA\GenericUSB\DeviceRules gespeichert. Ändern Sie diese Produktstandardregeln nicht. Verwenden Sie sie als Anleitung zum Erstellen von Administrator-Überschreibungsregeln, wie nachfolgend beschrieben. Die GPO-Überschreibungen werden ausgewertet, bevor die Produktstandardregeln angewendet werden.

Die Administrator-Override-Regeln sind in HKLM\SOFTWARE\Citrix\PortICA\GenericUSB\DeviceRules gespeichert. GPO-Richtlinienregeln haben das Format {Allow:|Deny:} gefolgt von Tag=Wert-Ausdrücken, die durch Leerzeichen getrennt sind. Die folgenden Tags werden unterstützt:

Tag	Beschreibung
VID	Vendor-ID vom Gerätedeskriptor
PID	Produkt-ID vom Gerätedeskriptor
REL	Release-ID vom Gerätedeskriptor
Klasse	Klasse vom Gerätedeskriptor oder einem Schnittstellendeskriptor; verfügbare USB-Klassencodes finden Sie auf der USB-Website unter http://www.usb.org/.
SubClass	Unterklasse vom Gerätedeskriptor oder ein Schnittstellendeskriptor
Prot	Protokoll vom Gerätedeskriptor oder ein Schnittstellendeskriptor

Wenn Sie neue Richtlinienregeln erstellen, beachten Sie Folgendes:

- Bei Regeln wird die Groß- und Kleinschreibung nicht berücksichtigt.
- Regeln können optional von einen Kommentar gefolgt werden, der mit # eingeleitet wird. Ein Trennzeichen ist nicht erforderlich, der Kommentar wird beim Abgleichen ignoriert.
- Leere Zeilen und Kommentare werden ignoriert.
- Leerzeichen dienen als Trennzeichen, sie können nicht in einer Zahl oder Kennung verwendet werden. Beispielsweise ist Deny: Class = 08 SubClass=05 eine gültige Regel; Deny: Class=0 Sub Class=05 hingegen nicht.
- Tags müssen den Übereinstimmungsoperator = verwenden. Beispielsweise VID=1230.
- Jede Regel muss auf einer neuen Zeile beginnen oder Teil einer durch Semikolon getrennten Liste sein.

Important

Wenn Sie die ADM-Vorlagendatei verwenden, müssen Sie die Regeln in einer einzigen Zeile mit Semikolons getrennt eingeben.

Bei optimierten Geräten, wie Massenspeichergeräten, wird das Gerät normalerweise über den speziellen CDM-Kanal umgeleitet und nicht mit Richtlinienregeln. Sie können dieses Verhalten auf die folgende Weise überschreiben:

- Leiten Sie das optimierte Gerät manuell mit der generischen USB-Umleitung um: Wählen Sie im Dialogfeld Einstellungen auf der Registerkarte Geräte die Option Zu allgemein wechseln.
- Leiten Sie das optimierte Gerät automatisch mit der generischen USB-Umleitung um, indem Sie die automatische Umleitung für das Speichergerät festlegen (z. B. AutoRedirectStorage = 1) und die USB-Einstellungen für eine automatische Verbindung der USB-Geräte konfigurieren. Weitere Informationen finden Sie unter CTX123015.

Beispiele:

- Das folgende Beispiel zeigt eine vom Administrator definierte USB-Richtlinienregel für Vendor- 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

Aktualisieren der für Remoting verfügbaren USB-Geräteliste

Standardmäßig werden USB-Geräte 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 für Desktopgerätesites oder desktopgehostete Anwendungen automatisch umgeleitet. In manchen Fällen empfiehlt es sich jedoch, die automatische Umleitung nicht für alle USB-Geräte zu aktivieren. Weitere Informationen finden Sie unter CTX123015.

Benutzer von Desktop Viewer können Geräte umleiten, die nicht automatisch umgeleitet werden, indem Sie sie aus der USB-Geräteliste auswählen. Um zu verhindern, dass Geräte aufgeführt oder umgeleitet werden, legen Sie auf dem Benutzergerät und dem VDA die Geräteregeln fest.

Sie können die USB-Geräte, die für Remoting verfügbar sind, aktualisieren, indem Sie Regeln für die Client-USB-Geräteumleitung für Citrix Receiver und VDA definieren, die dann die USB-Standardrichtlinienregeln außer Kraft setzen. Geräteregeln werden sowohl für Citrix Receiver als auch Virtual Desktop Agent zwingend umgesetzt. Achten Sie darauf, die Regeln für beide zu ändern, damit die Geräteumleitung wie vorgesehen funktioniert.

- Bearbeiten Sie die Benutzergeräteregistrierung (oder die INI-Dateien bei Citrix Receiver für Linux). Eine administrative Vorlage (ADM-Datei) ist auf dem Installationsmedium enthalten, sodass Sie das Gerät über die Active Directory-Gruppenrichtlinie ändern können: dvd root \os\lang\Support\Configuration\icaclient_usb.adm.
- Bearbeiten Sie die Administrator-Override-Regeln der VDA-Registrierung auf den Serverbetriebssystemmaschinen. Eine administrative Vorlage (ADM-Datei) ist auf dem Installationsmedium enthalten, sodass Sie VDA über die Active Directory-Gruppenrichtlinie ändern können: dvd root \os\lang\Support\Configuration\vda_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. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.

Die Produktstandardregeln sind in HKLM\SOFTWARE\Citrix\PortICA\GenericUSB\DeviceRules gespeichert. Ändern Sie diese Produktstandardregeln nicht. Verwenden Sie sie als Anleitung zum Erstellen von Administrator-Überschreibungsregeln, wie nachfolgend beschrieben. Die GPO-Überschreibungen werden ausgewertet, bevor die Produktstandardregeln angewendet werden.

Die Administrator-Override-Regeln sind in HKLM\SOFTWARE\Citrix\PortICA\GenericUSB\DeviceRules gespeichert. GPO-Richtlinienregeln haben das Format {Allow:|Deny:} gefolgt von Tag=Wert-Ausdrücken, die durch Leerzeichen getrennt sind. Die folgenden Tags werden unterstützt:

Tag	Beschreibung
VID	Vendor-ID vom Gerätedeskriptor
PID	Produkt-ID vom Gerätedeskriptor
REL	Release-ID vom Gerätedeskriptor
Klasse	Klasse vom Gerätedeskriptor oder einem Schnittstellendeskriptor; verfügbare USB-Klassencodes finden Sie auf der USB-Website unter http://www.usb.org/.
SubClass	Unterklasse vom Gerätedeskriptor oder ein Schnittstellendeskriptor
Prot	Protokoll vom Gerätedeskriptor oder ein Schnittstellendeskriptor

Wenn Sie neue Richtlinienregeln erstellen, beachten Sie Folgendes:

- Bei Regeln wird die Groß- und Kleinschreibung nicht berücksichtigt.
- Regeln können optional von einen Kommentar gefolgt werden, der mit # eingeleitet wird. Ein Trennzeichen ist nicht erforderlich, der Kommentar wird beim Abgleichen ignoriert.
- Leere Zeilen und Kommentare werden ignoriert.
- Leerzeichen dienen als Trennzeichen, sie können nicht in einer Zahl oder Kennung verwendet werden. Beispielsweise ist Deny: Class = 08 SubClass=05 eine gültige Regel; Deny: Class=0 Sub Class=05 hingegen nicht.
- Tags müssen den Übereinstimmungsoperator = verwenden. Beispielsweise VID=1230.
- Jede Regel muss auf einer neuen Zeile beginnen oder Teil einer durch Semikolon getrennten Liste sein.

Important

Wenn Sie die ADM-Vorlagendatei verwenden, müssen Sie die Regeln in einer einzigen Zeile mit Semikolons getrennt eingeben.

Bei optimierten Geräten, wie Massenspeichergeräten, wird das Gerät normalerweise über den speziellen CDM-Kanal umgeleitet und nicht mit Richtlinienregeln. Sie können dieses Verhalten auf die folgende Weise überschreiben:

- Leiten Sie das optimierte Gerät manuell mit der generischen USB-Umleitung um: Wählen Sie im Dialogfeld Einstellungen auf der Registerkarte Geräte die Option Zu allgemein wechseln.
- Leiten Sie das optimierte Gerät automatisch mit der generischen USB-Umleitung um, indem Sie die automatische Umleitung für das Speichergerät festlegen (z. B. AutoRedirectStorage = 1) und die USB-Einstellungen für eine automatische Verbindung der USB-Geräte konfigurieren. Weitere Informationen finden Sie unter CTX123015.

Beispiele:

- Das folgende Beispiel zeigt eine vom Administrator definierte USB-Richtlinienregel für Vendor- 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 Citrix Receiver für Windows arbeiten, gilt Folgendes:

- Geräte, die nach dem Sitzungsbeginn angeschlossen werden, werden unmittelbar im USB-Menü von Desktop Viewer angezeigt.
- Wenn ein USB-Gerät nicht richtig umgeleitet wird, können Sie das Problem u. U. beheben, indem Sie das Gerät erst nach dem Beginn der virtuellen Sitzung anschließen.
- Um Datenverlust zu verhindern, verwenden Sie das Windows-Symbol "Hardware sicher entfernen", bevor Sie das USB-Gerät entfernen.

USB-Massenspeichergeräte

Nur bei Massenspeichergeräten ist Remotezugriff auch durch Clientlaufwerkszuordnung verfügbar. Hierbei werden Laufwerke auf dem Benutzergerät automatisch Laufwerksbuchstaben auf dem

virtuellen Desktop zugeordnet, wenn Benutzer sich anmelden. Die Laufwerke werden als freigegebene Ordner mit zugeordneten Laufwerksbuchstaben angezeigt. Um Clientlaufwerkzuordnung zu konfigurieren, verwenden Sie unter den ICA-Richtlinieneinstellungen im Abschnitt "Dateiumleitung" die Einstellung Clientwechseldatenträger.

Die Hauptunterschiede zwischen den beiden Typen der Remotingrichtlinie sind:

Feature	Clientlaufwerkszuordnung	Generische USB-Umleitung
Diese Option ist in der Standardeinstellung aktiviert.	Ja	Nein
Konfigurierbare Leserechte	Ja	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 und für ein Gerät die automatische Umleitung konfiguriert wurde (siehe http://support.citrix.com/article/CTX123015) und wenn ein Massenspeichergerät vor oder nach dem Sitzungsstart angeschlossen wird, wird es mit der generischen USB-Umleitung umgeleitet.

> **Hinweis**
>
> Die USB-Umleitung wird für Verbindungen mit geringer Bandbreite (z. B. 50 KBit/s) unterstützt, das Kopieren großer Dateien funktioniert jedoch nicht.

Dateizugriff für zugeordnete Clientlaufwerke

Sie können steuern, ob Benutzer Dateien von ihren virtuellen Umgebungen auf ihre Benutzergeräte kopieren können. Standardmäßig ist in der Sitzung Lese-/Schreibzugriff auf Dateien und Ordner auf zugeordneten Clientlaufwerken möglich.

Um zu verhindern, dass Benutzer Dateien und Ordner auf zugeordneten Clientlaufwerken hinzufügen oder ändern, aktivieren Sie die Richtlinieneinstellung Schreibgeschützter Zugriff auf Clientlaufwerke. Wenn Sie diese Einstellung einer Richtlinie hinzufügen, müssen Sie die Einstellung Clientlaufwerkumleitung auf Zugelassen festlegen und zur Richtlinie hinzufügen.

Thinwire-Kompatibilitätsmodus

Feb 29, 2016

Durch neue Techniken bei der Bildschirmanalyse und -zwischenspeicherung gewährleistet der ThinWire-Kompatibilitätsmodus niedrige Bandbreitenauslastung und hohe Serverskalierbarkeit, ohne die Benutzererfahrung zu beeinträchtigen.

Der ThinWire-Kompatibilitätsmodus umfasst die folgenden Features:

- Intelligente Bitmapzuordnung für Anbieter von Bitmaps.
  - Bitmap-Übersetzungsanalyse ermöglicht effizientes Verschieben der Fenster und gleichmäßigen Bildlauf.
- Abwärtskompatibilität. Upgrades von Client oder Citrix Receiver oder Hardwarebeschleunigung sind nicht erforderlich.
  - Getestet mit zahlreichen älteren Thin Clients, bis zu 5 Jahren alt und älter.
- Optimiert für sehr niedrige Server-CPU-Auslastung und verbesserte Serverskalierbarkeit.
- Ein emulierter 16-Bit-Modus reduziert die Bandbreite um weitere 15-20 % bei typischen Arbeitslasten.
- Übergangserkennung für serverseitige Wiedergabe von Videoinhalt.
  - Verarbeitung mehrerer Übergangsbereiche für eine bessere Multimediaerfahrung. Beispiel: Wiedergabe mehrerer Videos oder Liveticker.
  - Selektives Scharfzeichnen für Bereiche, die einen Übergangszustand verlassen.
- Optimiert für CloudBridge-Beschleunigung. Tests ergaben eine Verringerung der Bandbreite im Verhältnis 6:1 bei Büroarbeitslasten.
- Adaptive Anzeige, die über Richtlinieneinstellungen angepasst werden kann. Weitere Informationen finden Sie unter **Bewegtbildkomprimierung** in Einstellungen der Richtlinie "Bewegtbilder".
- VDAs und Windows-Betriebssysteme bis zu Windows 10 VDA werden unterstützt.
- Der neue Modus "Zu verlustfrei verbessern" für 3D Pro erhöht die Reaktion, Interaktivität und unterbrechbares Scharfzeichnen für eine bessere Benutzererfahrung bei niedriger Bandbreite.
- Die Standardqualität statischer fotografischer Bilder ist höher als im Legacygrafikmodus.

Zur Steigerung der Clientleistung und Senkung der Bandbreitenauslastung werden für die Bildqualitätseinstellungen "Niedrig", "Mittel" (Standard) und "Hoch" Bildschirmaktualisierungen von der Übergangserkennung dynamisch ausgewertet, um zu entscheiden, ob hoch animierte Bereiche entsprechend der Richtlinie für die adaptive Anzeige mit niedrigerer Qualität gesendet werden.

Für die Bildqualität **Zu verlustfrei verbessern** verwendet der ThinWire-Kompatibilitätsmodus bei großen Bildschirmaktualisierungen das Prinzip "zunächst unscharf". Diese Einstellung ist für 3D Pro-Benutzer gedacht, die mit 3D-Modellen oder anderen grafikintensiven Anwendungen arbeiten. Wird die Aktivität fortgesetzt, wird ein Übergangsmodus angenommen und nach dessen Ende wird der betroffene Bereich scharfgezeichnet und zwischengespeichert. Bei der anfänglichen großen Änderung findet eine oberflächliche Bildanalyse am Änderungsbereich statt, um festzustellen, ob es sich um einen unscharfen Übergang oder um einen scharfen (verlustfreien) Übergang handelt, z. B. beim Drehen eines Drahtmodells. In puncto Framerate und Bandbreite ist die Codierung einfacher Bilder mit dem verlustfreien Citrix Codec effizienter, wobei kein Qualitätsverlust entsteht.

Der Schritt beim Scharfzeichnen bei der Einstellung "Zu verlustfrei verbessern" ist ebenfalls anders. Der Bereich wird nicht auf einmal scharfgezeichnet, sondern in vorgegebenen Blöcken für eine gleichmäßige und interaktive Benutzererfahrung. Das Scharfzeichnen eines großen Änderungsbereichs mitten im Übergang (z. B. beim Verschieben eines 3D-Modells, das kurzzeitig angehalten und dann fortgesetzt wird) würde insbesondere bei Verbindungen mit geringer Bandbreite einen Stillstand verursachen. Die Größe der Blöcke beim Scharfzeichnen hängt davon ab, wie stark die Qualität reduziert wurde,

um die Mindestframerate (eine Richtlinieneinstellung für die adaptive Anzeige) zu erzielen. Wurde die Qualität stark reduziert, sind die Blöcke beim Scharfzeichnen kleiner, die Mindestgröße beträgt 128 x 128 Pixel. Wurde die Qualität nicht reduziert, z. B. wenn der Client über ausreichend Rechenleistung und Bandbreite verfügt, können beim Scharfzeichnen Blöcke der Maximalgröße von 384 x 384 Pixel verwendet werden.

Framehawk Virtual Channel

Feb 29, 2016

Einführung

Der virtuelle Framehawk-Kanal optimiert die Bereitstellung virtueller Desktops und Anwendungen für Benutzer über drahtlose Breitbandverbindungen mit hohem Paketverlust oder Überlastung. Sie können mit Citrix Richtlinien Framehawk oder ThinWire für Benutzergruppen in einer Weise implementieren, die den gegebenen Netzwerkeigenschaften angepasst ist und den allgemeinen Erwartungen an Skalierbarkeit und Leistung entspricht.

Bisher galten generell Framerate und Anzeigequalität als Basisparameter für eine positive Benutzererfahrung. Durch Framehawk wird diese Definition um den Begriff der Linearität erweitert. Die Benutzer sollten ohne Ablenkung in den Genuss einer guten Benutzererfahrung kommen. In einem problembehafteten Netzwerk tritt der bei allen Protokollen bekannte Gummibandeffekt auf. Dieser verleitet den Benutzer, der nicht sicher ist, ob der Bildschirm noch reagiert, zu erratischen Mausklicks und führt zu unerwünschten Ergebnissen. Framehawk vermindert dieses Problem, insbesondere bei schwierigen Netzwerkbedingungen.

Bei privaten High-Speed-Internet-Verbindungen treten häufig Leistungsprobleme auf, z. B. aufgrund von Konflikten mit benachbarten WiFi-Signalen oder Funkstörungen, die durch schnurlose Geräte verursacht werden. Immer mehr Benutzer stellen eine Verbindung mit gehosteten Apps und Daten über 3G- oder 4G/LTE-Mobilfunknetze her oder verwenden Inflight-Internet-Dienste. Beliebt sind auch öffentliche WLAN-Hotspots in Cafés und Hotels, wo ebenfalls häufig Netzwerkengpässe auftreten.

Mit Framehawk wird die Benutzererfahrung im Vergleich zu ThinWire bei hoher Latenz interaktiver (stärker lineares Echoback der Zeichen).

Wirkungsweise von Framehawk

Bei der Betrachtung des Inhalts des Framepuffers und der Unterscheidung verschiedener Inhaltsarten auf dem Bildschirm wirkt Framehawk wie das menschliche Auge. Was ist dem Benutzer wichtig? In Bildschirmbereichen mit schnellen Änderungen (Video, Animationen etc.) spielt es für das menschliche Auge keine Rolle, wenn einige Pixel verloren gehen, da sie schnell durch neue Daten überschrieben werden.

Bei statischen Bereichen, z. B. Symbolleisten oder Text kurz nach Ausführen eines Bildlaufs an, den der Benutzer direkt lesen möchte, ist das menschliche Auge sehr anspruchsvoll. Diese Bereiche müssen pixelgenau sein. Im Gegensatz zu Protokollen, bei denen dich technische Präzision im Sinne von Nullen und Einsen im Vordergrund steht, ist Framehawk stärker auf die menschlichen Nutzer von Technik ausgelegt.

Framehawk umfasst einen völlig neuen QoS-Signalverstärker sowie eine zeitabhängige Heatmap zur exakteren und effizienten Arbeitslasterkennung. Zusätzlich zur Datenkomprimierung werden in Framehawk autonome, selbstkorrigierende Transformationen verwendet, die erneute Übertragung von Daten wird zur Gewährleistung von Klickantwort, Linearität und konsistenter Kadenz vermieden. In einem verlustreichen Netzwerk kann Framehawk Verluste durch Interpolation ausgleichen, sodass der Benutzer die Bildqualität weiterhin als gut empfindet und die Benutzererfahrung sogar flüssiger wird. Die Algorithmen von Framehawk können darüber hinaus die verschiedenen Arten des Paketverlusts unterscheiden, etwa den wahllosen Verlust (weitere Daten zur Kompensierung senden) und den Verlust durch Engpässe (keine weiteren Daten senden, da der Kanal bereits blockiert ist).

Die Framehawk Intent Engine unterscheidet Bildlauf nach oben oder unten, Vergrößern, Verschieben nach links oder rechts, Lesen, Eingeben und weitere übliche Aktionen und steuert die Antwort an den Virtual Delivery Agent (VDA) mit einem freigegebenen Wörterbuch. Wenn der Benutzer lesen möchte, muss die visuelle Qualität des Texts hervorragend sein. Führt er einen Bildlauf durch, muss dieser schnell und gleichmäßig sein. Er muss außerdem unterbrochen werden können, damit der Benutzer die Interaktion mit der Anwendung oder dem Desktop jederzeit unter Kontrolle hat.

Durch die Messung der Kadenz der Netzwerkverbindung kann die Framehawk-Logik schneller reagieren und bei Verbindungen mit hoher Latenz eine bessere Benutzererfahrung ermöglichen. Dieses einzigartige, patentierte Verfahren liefert kontinuierlich aktuelle Rückmeldungen zu Netzwerkbedingungen, sodass Framehawk auf Änderungen bei Bandbreite, Latenz und Verlust sofort reagieren kann.

ThinWire und Framehawk – Überlegungen zur Auslegung

ThinWire ist branchenweit erste Wahl in puncto Bandbreiteneffizienz und eignet sich gut für viele Zugriffsszenarien und Netzwerkbedingungen. Allerdings wird zur Gewährleistung einer zuverlässigen Datenkommunikation bei ThinWire TCP verwendet, wodurch in verlustreichen oder überlasteten Netzwerken eine Paketneuübertragung erforderlich ist, um Verzögerungen beim Endbenutzer zu vermeiden.

Die Datenübertragung bei Framehawk basiert auf UDP und damit auf dem Ansatz "so gut wie möglich". UDP macht nur einen kleinen Teil der Überwindung von Paketverlusten bei Framehawk aus, was deutlich wird, wenn man seine Leistung mit der anderer UDP-basierter Protokolle vergleicht. Allerdings bildet UDP die Grundlage für die menschenorientierte Technik, die Framehawk von anderen Lösungen abhebt.

Wie viel Bandbreite benötigt Framehawk?

Die Bezeichnung Breitband-WLAN hängt von verschiedenen Faktoren ab, etwa der Zahl der Benutzer, die eine Verbindung teilen, der Qualität der Verbindung und der verwendeten Apps. Zur Erzielung einer optimalen Leistung empfiehlt Citrix einen Grundwert von 4 oder 5 MBit/s plus ca. 150 KBit/s pro gleichzeitig verbundenem Benutzer. Allerdings erbringt Framehawk bei einer 2-MBit/s-VSAT-Satellitenverbindung aufgrund der Kombination aus Paketverlust und hoher Latenz u. U. eine deutlich höhere Leistung als ThinWire.

Citrix empfiehlt für ThinWire generell eine Bandbreite von 1,5 MBit/s plus 150 KBit/s pro Benutzer (Details siehe Blog zu XenApp-/XenDesktop-Bandbreite), bei einem Paketverlust von 3 % benötigt ThinWire aber viel mehr Bandbreite als Framehawk, um eine gute Benutzererfahrung zu gewährleisten.

Hinweis: ThinWire ist weiterhin der Primärkanal für das Anzeigen-Remoting des ICA-Protokolls. Framehawk ist standardmäßig deaktiviert. Citrix empfiehlt die selektive Aktivierung für spezifische Breitband-WLAN-Szenarios in Ihrer Organisation.

Anforderungen und Überlegungen

Framehawk erfordert mindestens VDA 7.6.300 und Gruppenrichtlinienverwaltung 7.6.300.

Auf dem Endpunkt muss mindestens Citrix Receiver für Windows 4.3.100 oder Citrix Receiver für iOS 6.0.1 ausgeführt werden.

Standardmäßig verwendet Framehawk UDP-Ports im Bereich 3224-3324. Dieser kann über eine Richtlinieneinstellung angepasst werden. Jede einzelne Verbindung zwischen dem Client und dem virtuellen Desktop erfordert einen eigenen Port. In Betriebssystemumgebungen mit mehreren Benutzern (z. B. XenApp-Server) müssen Sie ausreichend Ports für die maximale Zahl gleichzeitiger Benutzersitzungen definieren. Bei Einzelbenutzer-Betriebssystemen wie etwa VDI-Desktops reicht ein UDP-Port. Framehawk versucht die Verwendung der Ports beginnend vom ersten bis zum letzten im angegebenen Bereich. Dies gilt sowohl für Verbindungen über NetScaler Gateway als auch für direkte interne Verbindungen mit dem StoreFront-Server.

Für den Remotezugriff muss NetScaler Gateway bereitgestellt sein. Standardmäßig verwendet NetScaler UDP-Port 443 für die verschlüsselte Kommunikation zwischen Citrix Receiver auf dem Client und dem Gateway. Dieser Port muss in allen externen Firewalls geöffnet sein, damit eine sichere Kommunikation in beide Richtungen möglich ist. Das Feature wird als "Datagram Transport Security" (DTLS) bezeichnet.

Hinweis: Framehawk Virtual Channel wird unter NetScaler Unified Gateway ab Version 11.0.64.34 unterstützt.

Bei der Implementierung virtueller Framehawk-Kanäle empfehlen sich folgende bewährte Methoden:

- Vergewissern Sie sich beim Sicherheitsadministrator, dass die für Framehawk definierten UDP-Ports in der Firewall geöffnet sind. Die Firewall wird bei der Installation nicht automatisch konfiguriert.
- In vielen Fällen ist NetScaler Gateway in der DMZ umgeben von einer externen und einer internen Firewall installiert. UDP-Port 443 muss in der externen Firewall geöffnet sein. Wenn die Standardportbereiche verwendet werden, muss der UDP-Portbereich 3224-3324 in der internen Firewall geöffnet sein.

Konfiguration

Achtung: Framehawk sollte nur für Benutzer mit hohem Paketverlust aktiviert werden. Es wird außerdem empfohlen, Framehawk nicht als universelle Richtlinie für alle Objekte der Site zu aktivieren.

Framehawk Virtual Channel ist standardmäßig deaktiviert. Wenn das Feature aktiviert ist, versucht der Server, Framehawk Virtual Channel für die Grafiken und Eingaben der Benutzer zu verwenden. Sind die Voraussetzungen nicht erfüllt, wird die Verbindung im Standardmodus (ThinWire) hergestellt.

Die folgenden Richtlinieneinstellungen wirken sich auf Framehawk aus:

- Framehawk-Anzeigekanal: aktiviert oder deaktiviert das Feature.
- Portbereich für Framehawk-Anzeigekanal: Bereich der UDP-Portnummern (niedrigste Portnummer bis höchste Portnummer), die der VDA für den Austausch von Framehawk-Anzeigekanaldaten mit dem Benutzergerät verwendet. Der VDA versucht die Verwendung eines Ports, beginnend bei dem Port mit der niedrigsten Nummer und geht dann ggf. zu dem Port mit der nächsthöheren Nummer über. Über den Port erfolgen eingehende und ausgehende Datenübertragungen.

NetScaler Gateway-Unterstützung für Framehawk

HDX Framehawk Virtual Channel wird von NetScaler Gateway ab Version 11.0 Build 62.10 unterstützt. Es wird auch von NetScaler Unified Gateway ab Version 11.0.64.34 unterstützt.

- NetScaler Gateway bezieht sich auf eine Bereitstellungsarchitektur, in der der virtuelle Gateway-VPN-Server direkt für

das Gerät des Endbenutzers zugänglich ist, d. h. der virtuelle VPN-Server hat eine öffentliche IP-Adresse und der Benutzer stellt direkt eine Verbindung mit dieser IP-Adresse her.
- NetScaler Unified Gateway bezieht sich auf eine Bereitstellung, in der der virtuelle Gateway-VPN-Server als Ziel an den virtuellen Content Switching-Server (CS) gebunden ist. In einer solchen Bereitstellung hat der virtuelle CS-Server die öffentliche IP-Adresse und der virtuelle Gateway-VPN-Server hat eine Pseudo-IP-Adresse.

Zum Aktivieren der Framehawk-Unterstützung unter NetScaler Gateway muss der DTLS-Parameter auf der Ebene des virtuellen Gateway-VPN-Servers aktiviert sein. Wenn der Parameter aktiviert ist und die Komponenten in XenApp bzw. XenDesktop ordnungsgemäß aktualisiert wurden, wird der Audio-, Video- und Interaktionsdatenverkehr von Framehawk zwischen dem virtuellen Gateway-VPN--Server und dem Benutzergerät verschlüsselt.

NetScaler Gateway, Unified Gateway und NetScaler Gateway + Global Server Load Balancing werden mit Framehawk unterstützt.

Folgendes wird mit Framehawk nicht unterstützt:

- HDX Insight
- NetScaler Gateway im IPv6-Modus
- NetScaler Gateway Double Hop
- Mehrere Secure Ticket Authoritys (STA) für NetScaler Gateway
- NetScaler Gateway mit hoher Verfügbarkeit
- NetScaler Gateway im Cluster

Konfigurieren von NetScaler Gateway für Framehawk-Unterstützung

Diese Konfiguration ist erforderlich, wenn Sie die UDP-Verschlüsselung unter NetScaler Gateway für den Remotezugriff aktivieren.

NetScaler-Unterstützung für Framehawk erfordert Folgendes:

- UDP-Port 443 muss in der externen Firewall geöffnet sein.
- DTLS muss in den Einstellungen des virtuellen VPN-Servers aktiviert sein.
- Lösen Sie die Bindung des SSL-Zertifikatschlüsselpaars und binden Sie es erneut. Dies ist nicht erforderlich, wenn Sie NetScaler ab Version 11.0.64.34 verwenden.

Konfigurieren der NetScaler-Unterstützung für Framehawk

1. Stellen Sie NetScaler Gateway bereit und konfigurieren Sie es für die Kommunikation mit StoreFront und zur Authentifizierung der Benutzer von XenApp und XenDesktop.
2. Erweitern Sie auf der Registerkarte "Configuration" von NetScaler die Option "NetScaler Gateway" und wählen Sie **Virtual Servers**.
3. Klicken Sie auf **Edit**, um die Grundeinstellungen des virtuellen VPN-Servers anzuzeigen und prüfen Sie die DTLS-Einstellung.
4. Klicken Sie auf **More**, um weitere Konfigurationsoptionen aufzurufen:
5. Wählen Sie **DTLS**, um die Sicherheit für Datagramm-Protokolle wie Framehawk zu aktivieren. Klicken Sie auf **OK**. Im Bereich mit den Grundeinstellungen des virtuellen VPN-Servers wird das DTLS-Flag mit der Einstellung **True** angezeigt.
6. Öffnen Sie den Bildschirm "Server Certificate Binding" erneut und klicken Sie auf **+**, um das Zertifikatschlüsselpaar zu binden.
7. Wählen Sie das Zertifikatschlüsselpaar (s. oben) und dann **Select**.
8. Speichern Sie die Änderungen an der Serverzertifikatbindung.

9. Nach dem Speichern wird das Zertifikatschlüsselpaar angezeigt. Klicken Sie auf **Bind**.
10. Ignorieren Sie Meldung "No usable ciphers configured on the SSL vserver/service", sofern sie angezeigt wird.

Note: Steps 6-10 are not required if you are using Unified Gateway version 11.0.64.34 or later.

Konfigurieren von Unified Gateway für Framehawk-Unterstützung

Konfigurieren der Unified Gateway-Unterstützung für Framehawk

1. Vergewissern Sie sich, dass Unified Gateway installiert und ordnungsgemäß konfiguriert ist (Installation entweder mit dem Installationsassistenten oder manuell). Weitere Informationen finden Sie auf der Website mit der Citrix Produktdokumentation unter Unified Gateway.
2. Aktivieren Sie DTLS auf dem virtuellen Server, der an den virtuellen CS-Server als virtueller Zielserver gebunden ist.

Konfigurieren von Citrix Receiver 6.0.1 für iOS zur Framehawk-Unterstützung

Zum Konfigurieren von Citrix Receiver für iOS zur Framehawk-Unterstützung müssen Sie die Datei default.ica manuell bearbeiten.

1. Öffnen Sie auf dem StoreFront-Server das App_Data-Verzeichnis im Pfad c:\inetpub\wwwroot\.
2. Öffnen Sie die Datei default.ica und fügen Sie im Abschnitt "WFClient" die Zeile "Framehawk=On" hinzu.
3. Speichern Sie die Änderung.

Damit können Framehawk-Sitzungen von kompatiblen Citrix Receiver-Instanzen auf iOS-Geräten hergestellt werden.

Framehawk Support Matrix

Scenario	Framehawk support
NetScaler Gateway	Yes
NetScaler + Global Server Load Balancing	Yes
NetScaler with Unified Gateway	Yes **Note**: Unified Gateway version 11.0.64.34 and later is supported.
HDX Insight	No
NetScaler Gateway in IPv6 mode	No
NetScaler Gateway Double Hop	No

Multiple Secure Ticket Authority (STA) on NetScaler Gateway	No
NetScaler Gateway with High Availability (HA)	No
NetScaler Gateway with Cluster setup	No

Überwachen von Framehawk

Sie können die Verwendung und Leistung von Framehawk über Citrix Director überwachen. Die Detailansicht für den virtuellen HDX-Kanal enthält nützliche Informationen zur Überwachung und Problembehandlung des virtuellen Framehawk-Kanals in jeder Sitzung. Zum Anzeigen von Zahlen für Framehawk wählen Sie **Grafiken - Framehawk**.

Wenn die Framehawk-Verbindung steht, wird auf der Detailseite **Anbieter = VD3D** und **Verbunden = True** angezeigt. Der Status "Im Leerlauf" des virtuellen Kanals ist normal, da er den Signalkanal überwacht, der nur beim ersten Handshake verwendet wird. Die Seite bietet auch andere nützliche Statistiken zu der Verbindung.

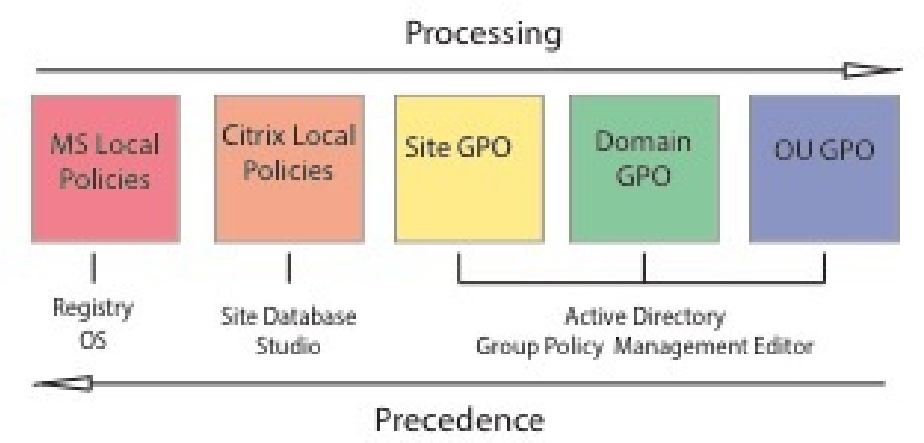
Wenn Probleme auftreten, besuchen Sie das Blog zur Problembehandlung bei Framehawk.

Richtlinien

Feb 29, 2016

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 bestimmten Kriterien und Regeln, und wenn Sie die Richtlinien nicht ausdrücklich zuweisen, gelten die Einstellungen für alle Verbindungen.



Sie können Richtlinien auf unterschiedliche Ebenen des Netzwerks zuweisen. Richtlinieneinstellungen, die auf der GPO-Ebene der Organisationseinheit zugewiesen werden, haben die höchste Priorität im Netzwerk. Richtlinien auf der Domänen-GPO-Ebene überschreiben Richtlinien auf der Ebene der Sitegruppenrichtlinienobjekte, die wiederum alle lokalen Richtlinien von Microsoft und Citrix überschreiben, die mit ihnen in Konflikt stehen.

Alle lokalen Citrix Richtlinien werden in der Citrix Studio-Konsole erstellt und verwaltet und in der Sitedatenbank gespeichert. Gruppenrichtlinien werden hingegen mit der Microsoft-Gruppenrichtlinien-Verwaltungskonsole (GPMC) erstellt und verwaltet und in Active Directory gespeichert. Lokale Microsoft-Richtlinien werden im Windows-Betriebssystem erstellt und in der Registrierung gespeichert.

Studio verwendet einen Modellierungsassistenten, mit dem Administratoren Konfigurationseinstellungen in Vorlagen und Richtlinien vergleichen können, um miteinander in Konflikt stehende und redundante Einstellungen zu eliminieren. Administratoren können Gruppenrichtlinienobjekte mit der Gruppenrichtlinien-Verwaltungskonsole festlegen, um Einstellungen zu konfigurieren und diese Einstellungen auf eine Zielgruppe von Benutzern auf unterschiedlichen Ebenen des Netzwerks anzuwenden.

Diese Gruppenrichtlinienobjekte werden in Active Directory gespeichert und die meisten IT-Mitarbeiter haben aus Sicherheitsgründen nur eingeschränkten Zugriff auf die Verwaltung dieser Einstellungen.

Einstellungen werden entsprechend ihrer Priorität und Bedingung zusammengefasst. Deaktivierte Einstellungen haben Vorrang vor aktivieren Einstellungen mit niedriger Priorität. Richtlinieneinstellungen, die nicht konfiguriert sind, werden ignoriert und setzen keine Einstellungen mit niedrigerer Priorität außer Kraft.

Lokale Richtlinien können auch mit Gruppenrichtlinien in Active Directory in Konflikt stehen. Abhängig von der Situation könnten sie einander überschreiben.

Alle Richtlinien werden in der folgenden Reihenfolge verarbeitet:

1. Der Endbenutzer meldet sich mit Domänenanmeldeinformationen an einer Maschine an.
2. Die Anmeldeinformationen werden an den Domänencontroller gesendet.
3. Active Directory wendet alle Richtlinien an (Endbenutzer, Endpunk, Organisationseinheit und Domäne).
4. Der Endbenutzer meldet sich bei Receiver an und greift auf eine Anwendung oder einen Desktop zu.
5. Richtlinien von Citrix und Microsoft werden für den Endbenutzer und die Maschine, die die Ressource hostet, verarbeitet.
6. Active Directory bestimmt die Priorität für die Richtlinieneinstellungen und wendet sie auf die Registrierung des Endpunktgeräts und die Maschine an, auf der die Ressource gehostet wird.
7. Der Endbenutzer meldet sich von der Ressource ab. Citrix Richtlinien für Endbenutzer und Endpunktgerät sind nicht mehr aktiv.
8. Der Endbenutzer meldet sich vom Benutzergerät ab, das die GPO-Benutzerrichtlinien freigibt.
9. Der Endbenutzer schaltet das Gerät aus und die GPO-Maschinenrichtlinien werden freigegeben.

Beim Erstellen von Richtlinien für Benutzergruppen, Geräte und Maschinen haben einige Mitglieder u. U. unterschiedliche Anforderungen und benötigen Ausnahmen zu einigen Einstellungen. Ausnahmen werden durch Filter in Studio und in der Gruppenrichtlinien-Verwaltungskonsole erstellt und bestimmten, für wen oder was die Richtlinie gilt.

Hinweis: Die Verwendung von Windows- und Citrix Richtlinien im gleichen GPO wird nicht unterstützt.

Verwandter Inhalt

- Arbeiten mit Richtlinien
- Richtlinienvorlagen
- Erstellen von Richtlinien
- Vergleichen, Priorisieren, Modellieren und Problembehandlung für Richtlinien
- Standardrichtlinieneinstellungen
- Referenz für Richtlinieneinstellungen

Arbeiten mit Richtlinien

Feb 29, 2016

Durch das Konfigurieren von Citrix Richtlinien steuern Sie den Benutzerzugriff und die Sitzungsumgebung. Citrix Richtlinien sind die effizienteste Methode zum Steuern der Verbindungs-, Sicherheits- und Bandbreiteneinstellungen. Sie erstellen Richtlinien für bestimmte Benutzergruppen, Geräte oder Verbindungstypen. Jede Richtlinie kann mehrere Einstellungen enthalten.

Tools zum Arbeiten mit Citrix Richtlinien

Sie können die folgenden Tools zum Arbeiten mit Citrix Richtlinien verwenden.

- **Studio**: Wenn Sie ein Citrix Administrator ohne Berechtigung zum Verwalten von Gruppenrichtlinien sind, verwenden Sie Studio, um Richtlinien für Ihre Site zu erstellen. Mit Studio erstellte Richtlinien werden in der Sitedatenbank gespeichert und Updates werden per Push auf den virtuellen Desktop übertragen, wenn der virtuelle Desktop beim Broker registriert wird oder ein Benutzer eine Verbindung mit dem virtuellen Desktop herstellt.
- **Editor für lokale Gruppenrichtlinien** (Snap-In der Microsoft Management Console): Wenn Sie in Ihrer Netzwerkumgebung Active Directory verwenden und Sie die Berechtigungen zur Verwaltung von Gruppenrichtlinien haben, können Sie den Editor für lokale Gruppenrichtlinien verwenden, um Richtlinien für Ihre Site zu erstellen. Die Einstellungen, die Sie konfigurieren, beeinträchtigen die Gruppenrichtlinienobjekte, die Sie in der Gruppenrichtlinien-Verwaltungskonsole angeben.
  Wichtig: Sie müssen den Editor für lokale Gruppenrichtlinien zum Konfigurieren einiger Einstellungen verwenden, u. a. die Einstellungen zum Registrieren von VDAs bei einem Controller und die Einstellungen für Microsoft App-V Server.

Reihenfolge und Priorität bei der Richtlinienverarbeitung

Gruppenrichtlinieneinstellungen (GPOs) werden in der folgenden Reihenfolge verarbeitet:

1. Lokale GPO
2. XenApp- bzw. XenDesktop-Site-GPO (in der Sitedatenbank gespeichert)
3. GPOs auf Siteebene
4. GPOs auf Domänenebene
5. Organisationseinheiten

Bei einem Konflikt können Richtlinieneinstellungen, die zuletzt verarbeitet werden, vorher verarbeitete überschreiben. Das heißt, dass Richtlinieneinstellungen die folgende Rangfolge haben:

1. Organisationseinheiten
2. GPOs auf Domänenebene
3. GPOs auf Siteebene
4. XenApp- bzw. XenDesktop-Site-GPO (in der Sitedatenbank gespeichert)
5. Lokale GPO

Beispiel: Ein Citrix Administrator erstellt eine Richtlinie (Richtlinie A) über Studio, mit der die Clientdateiumleitung für die Vertriebsmitarbeiter des Unternehmens aktiviert wird. Gleichzeitig erstellt ein anderer Administrator mit dem Gruppenrichtlinien-Editor eine Richtlinie (Richtlinie B), mit der die Clientdateiumleitung für die Vertriebsmitarbeiter deaktiviert wird. Wenn sich die Vertriebsmitarbeiter an den virtuellen Desktops anmelden, wird Richtlinie B angewendet und Richtlinie A ignoriert, da Richtlinie B auf der Domänenebene und Richtlinie A auf der Ebene der XenApp- bzw. XenDesktop-Site-GPOs verarbeitet wurde.

Beachten Sie jedoch, dass die Citrix Sitzungseinstellungen die gleichen Einstellungen in einer Active Directory-Richtlinie oder

einer Remotedesktop-Sitzungshostkonfiguration überschreiben, wenn ein Benutzer eine ICA- oder Remotedesktopprotokoll (RDP)-Sitzung startet. Zu diesen Einstellungen gehören solche, die mit typischen RDP-Clientverbindungseinstellungen zusammenhängen, wie Desktophintergrund, Menüanimationen und das Anzeigeverhalten bei Drag & Drop.

Wenn Sie mehrere Richtlinien verwenden, können Sie Richtlinien, deren Einstellungen Konflikte verursachen, Prioritäten zuweisen. Weitere Informationen hierzu finden Sie unter Vergleichen, Priorisieren, Modellieren und Problembehandlung für Richtlinien.

Arbeitsablauf bei Citrix Richtlinien

Der Prozess für das Konfigurieren von Richtlinien ist:

1. Erstellen Sie die Richtlinie.
2. Konfigurieren Sie Richtlinieneinstellungen.
3. Weisen Sie die Richtlinie Benutzer- und Maschinenobjekten zu.
4. Weisen Sie der Richtlinie eine Priorität zu.
5. Prüfen Sie die effektive Richtlinie durch Ausführen des Gruppenrichtlinien-Modellierungsassistenten.

Navigieren durch die Citrix Richtlinien und Einstellungen

Im Editor für lokale Gruppenrichtlinien werden Richtlinien und Einstellungen in zwei Hauptkategorien eingeteilt: Computerkonfiguration und Benutzerkonfiguration. Jede Kategorie hat einen Knoten für Citrix Richtlinien. Weitere Informationen zum Verwenden dieses Snap-Ins finden Sie in der Dokumentation von Microsoft.

In Studio sind die Richtlinieneinstellungen je nach Funktionalität bzw. Feature, für die bzw. das sie gelten, in Kategorien eingeteilt. Beispielsweise enthält der Bereich "Profilverwaltung" Richtlinieneinstellungen für die Profilverwaltung.

- Computereinstellungen (Richtlinieneinstellungen für Maschinen) definieren das Verhalten von virtuellen Desktops und werden beim Start eines virtuellen Desktops angewendet. Diese Einstellungen werden auch angewendet, wenn keine aktiven Benutzersitzungen auf dem virtuellen Desktop durchgeführt werden. Benutzerrichtlinieneinstellungen definieren die Benutzererfahrung bei Verbindungen über ICA. Benutzerrichtlinien werden angewendet, wenn ein Benutzer eine Verbindung über ICA herstellt oder erneut herstellt. Benutzerrichtlinien werden nicht angewendet, wenn ein Benutzer eine Verbindung über RDP herstellt oder sich direkt bei der Konsole anmeldet.
  Sie greifen auf Richtlinien, Einstellungen oder Vorlagen zu, indem Sie im Navigationsbereich von Studio Richtlinien auswählen.
  - Die Registerkarte **Richtlinien** listet alle Richtlinien auf. Wenn Sie eine Richtlinie auswählen, wird auf den Registerkarten rechts Folgendes angezeigt: Übersicht (Name, Priorität, Status: Aktiviert bzw. Deaktiviert, und Beschreibung), Einstellungen (Liste der konfigurierten Einstellungen) und Zugewiesen zu (Benutzer- und Maschinenobjekte, denen die Richtlinie momentan zugewiesen ist). Weitere Informationen finden Sie unter Erstellen von Richtlinien.
  - Auf der Registerkarte **Vorlagen** werden von Citrix bereitgestellte und benutzerdefinierte Vorlagen, die Sie erstellt haben, aufgelistet. Wenn Sie eine Vorlage auswählen, wird auf den Registerkarten rechts Folgendes angezeigt: Beschreibung (Zweck der Vorlage) und Einstellungen (Liste der konfigurierten Einstellungen). Weitere Informationen finden Sie unter Richtlinienvorlagen.
  - Mit der Registerkarte **Vergleich** können Sie die Einstellungen einer Richtlinie oder Vorlage mit denen in anderen Richtlinien oder Vorlagen vergleichen. Sie können beispielsweise Einstellungswerte prüfen, um sicherzustellen, dass optimale Verfahren eingehalten werden. Weitere Informationen finden Sie unter Vergleichen, Priorisieren, Modellieren und Problembehandlung für Richtlinien.
  - Auf der Registerkarte **Modellierung** können Sie Verbindungsszenarios mit Citrix Richtlinien simulieren. Weitere Informationen finden Sie unter Vergleichen, Priorisieren, Modellieren und Problembehandlung für Richtlinien.

  Suchen nach einer Einstellung in einer Richtlinie oder Vorlage

1. Wählen Sie die Richtlinie oder Vorlage aus.
2. Wählen Sie im Aktionsbereich Richtlinie bearbeiten oder Vorlage bearbeiten.
3. Geben Sie auf der Seite Einstellungen den Namen der Einstellung ein.
   Sie können die Suche verfeinern, indem Sie eine bestimmte Produktversion oder Kategorie (z. B. Bandbreite) auswählen oder indem Sie das Kontrollkästchen Nur ausgewählte anzeigen aktivieren. Außerdem können Sie nur die Einstellungen suchen, die der ausgewählten Richtlinie hinzugefügt wurden. Für eine ungefilterte Suche wählen Sie Alle Einstellungen.

- Suchen nach einer Einstellung in einer Richtlinie
  1. Markieren Sie die Richtlinie.
  2. Geben Sie auf der Registerkarte Einstellungen den Namen der Einstellung ein.

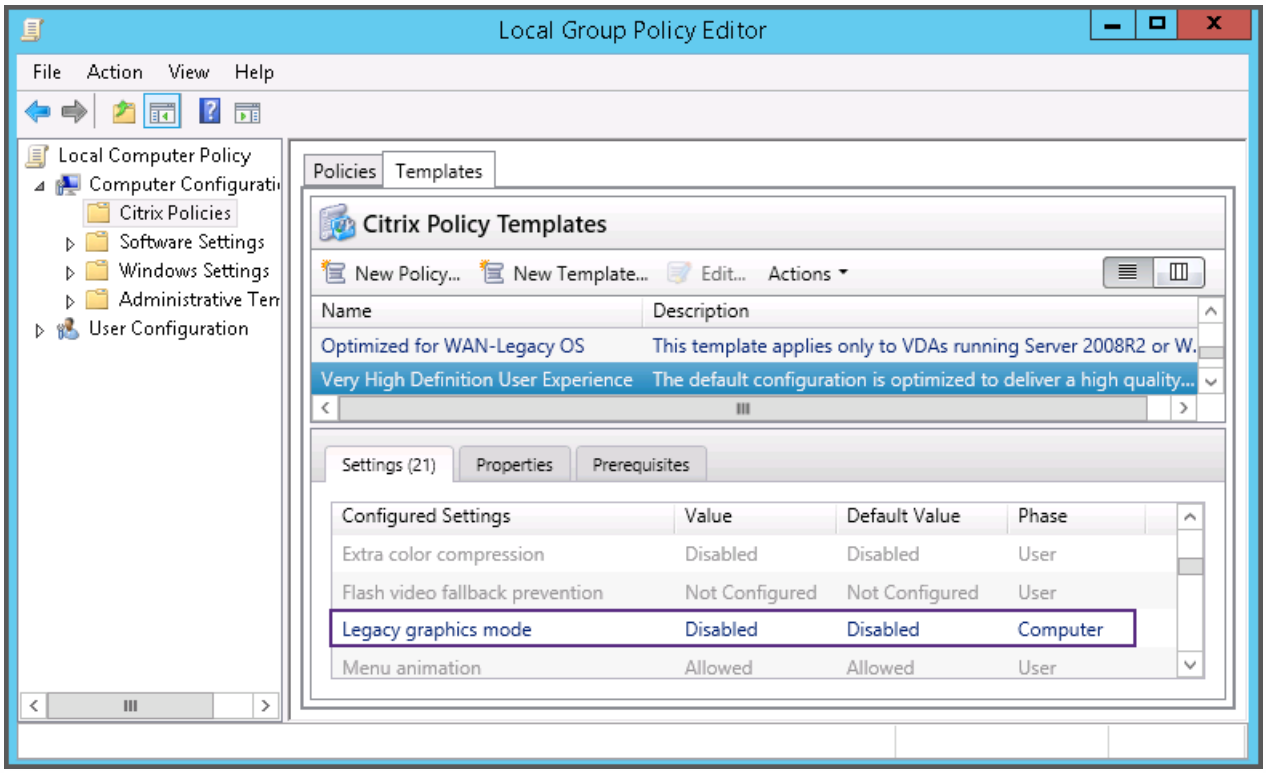
Sie können die Suche verfeinern, indem Sie eine bestimmte Produktversion oder Kategorie auswählen. Für eine ungefilterte Suche wählen Sie Alle Einstellungen.

Eine Richtlinie ist nach ihrer Erstellung völlig unabhängig von der verwendeten Vorlage. Sie können in das Feld "Beschreibung" eingeben, auf welcher Vorlage die neue Richtlinie basiert.

In Studio werden Richtlinien und Vorlagen in einer Liste angezeigt, unabhängig davon, ob sie Benutzer- oder Computereinstellungen oder beide Arten von Einstellungen enthalten, und sie können zudem mit Benutzer- und Computerfiltern angewendet werden.

Im Gruppenrichtlinien-Editor müssen Computer- und Benutzereinstellungen separat angewendet werden, selbst wenn sie auf einer Vorlage basieren, die beide Arten von Einstellungen enthält. In diesem Beispiel wird "Besonders gute High Definition-Benutzererfahrung" in Computerkonfiguration verwendet:

- Der Legacy-Grafikmodus ist eine Computereinstellung, die in einer mit dieser Vorlage erstellten Richtlinie verwendet wird.
- Die Benutzereinstellungen, grau dargestellt, werden nicht in einer mit dieser Vorlage erstellten Richtlinie verwendet.



Richtlinienvorlagen

Feb 29, 2016

Vorlagen ermöglichen das Erstellen von Richtlinien von einem vordefinierten Ausgangspunkt aus. Integrierte Citrix Vorlagen sind für bestimmte Umgebungen oder Netzwerkbedingungen optimiert und können für Folgendes verwendet werden:

- Als Ausgangspunkt für das Erstellen Ihrer eigenen Richtlinien und Vorlagen, die Sie für verschiedene Sites freigeben können.
- Eine Referenz für einfacheres Vergleichen der Ergebnisse zwischen Bereitstellungen, da Sie sich auf Ergebnisse beziehen können, zum Beispiel "... wenn Sie die Citrix Vorlage x oder y verwenden ...".
- Eine Methode für das Übermitteln von Richtlinien an Citrix Support oder vertrauenswürdige Dritte durch Importieren oder Exportieren von Vorlagen.

Richtlinienvorlagen können importiert und exportiert werden. Weitere Vorlagen und/oder Updates für die integrierten Vorlagen finden Sie unter CTX202000.

Informationen zur Verwendung von Vorlagen für die Erstellung von Richtlinien finden Sie unter CTX202330.

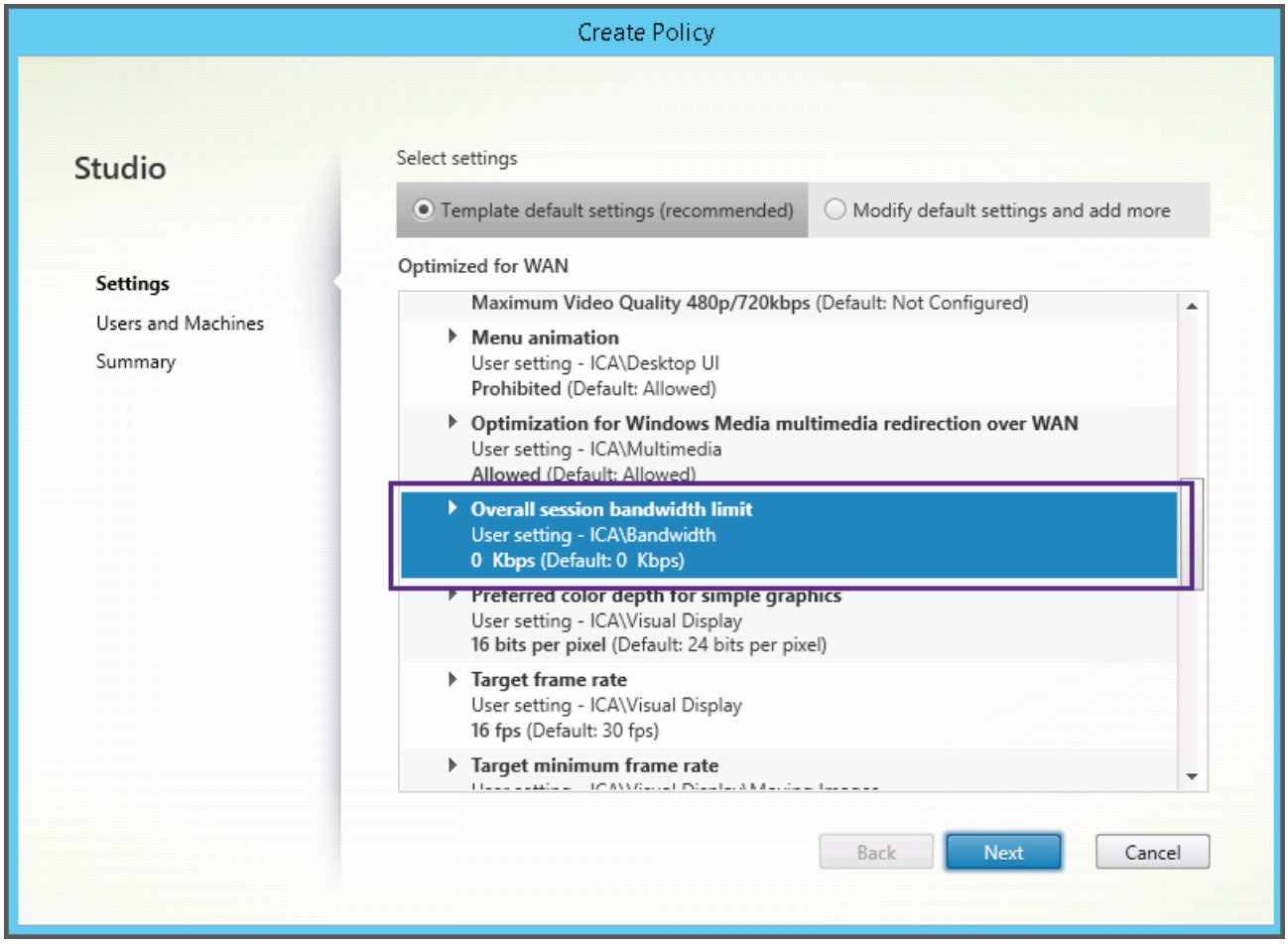
Integrierte Citrix Vorlagen

Die folgenden Richtlinienvorlagen sind verfügbar:

- **Besonders gute High Definition-Benutzererfahrung**: Diese Vorlage erzwingt Standardeinstellungen, die die Benutzererfahrung optimieren. Verwenden Sie diese Vorlage in Szenarios, in denen mehrere Richtlinien in der Reihenfolge der Priorität verarbeitet werden.
- **Hohe Serverskalierbarkeit**: Mit dieser Vorlage können Sie Serverressourcen sparen, da Benutzererfahrung und Serverskalierbarkeit ausbalanciert werden. Die Vorlage ermöglicht eine gute Benutzererfahrung und erhöht gleichzeitig die Anzahl an Benutzern, die auf einem einzelnen Server gehostet werden können. Diese Vorlage verwendet keinen Videocodec für die Komprimierung von Grafiken und verhindert das serverseitige Multimediarendering.
- **Hohe Serverskalierbarkeit – Legacy-OS**: Diese Vorlage für hohe Serverskalierbarkeit gilt nur für VDAs, die unter Windows Server 2008 R2, Windows 7 und älteren Betriebssystemen ausgeführt werden. Die Vorlage stützt sich auf den Legacy-Grafikmodus, der für diese Betriebssysteme effizienter ist.
- **Für 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**: Diese Vorlage gilt nur für VDAs, die unter Windows Server 2008 R2, Windows 7 oder älteren Betriebssystemen ausgeführt werden. Die Vorlage stützt sich auf den Legacy-Grafikmodus, der für diese Betriebssysteme effizienter ist.
- **Sicherheit und Steuerung**: Verwenden Sie diese Vorlage in Umgebungen mit niedriger Fehlertoleranz, um die in XenApp und XenDesktop standardmäßig aktivierten Features zu minimieren. Die in dieser Vorlage enthaltenen Einstellungen deaktivieren den Zugriff auf Drucker, Zwischenablage, Peripheriegeräte, Laufwerkzuordnung, Portumleitung und Flash-Beschleunigung auf Benutzergeräten. Bei Anwendung dieser Vorlage wird möglicherweise mehr Bandbreite genutzt und die Benutzerdichte pro Server verringert.

Wir empfehlen zwar, die integrierten Citrix Vorlagen mit den Standardeinstellungen zu verwenden, jedoch haben einige Einstellungen keine empfohlenen Werte (z. B. die Einstellung "Bandbreitenlimit für Sitzung insgesamt" in der Vorlage "Für

WAN optimiert"). In diesem Fall wird die Einstellung durch die Vorlage verfügbar gemacht, damit der Administrator die Wirkung dieser Einstellung in diesem Szenario versteht.



Wenn Sie eine Bereitstellung (Richtlinienverwaltung und VDAs) vor XenApp und XenDesktop 7.6 FP3 betreiben und die Vorlagen "Hohe Serverskalierbarkeit" und "Für WAN optimiert" benötigen, verwenden Sie die Vorlagenversionen für ältere Betriebssysteme ("Legacy-OS").

> ## Hinweis
>
> Integrierte Vorlagen werden von Citrix erstellt und aktualisiert. Diese Vorlagen dürfen nicht geändert oder gelöscht werden.

Erstellen und Verwalten von Vorlagen mit Studio

Erstellen einer neuen Vorlage basierend auf einer Vorlage

1. Wählen Sie im Studio-Navigationsbereich **Richtlinien** aus.
2. Wählen Sie die Registerkarte **Vorlagen** und dann die Vorlage, mit der Sie eine neue Vorlage erstellen möchten.
3. Wählen Sie im Aktionsbereich **Vorlage erstellen**.
4. Wählen und konfigurieren Sie die Richtlinieneinstellungen, die Sie in die Vorlage einschließen möchten. Entfernen Sie vorhandene Einstellungen, die nicht eingeschlossen werden sollen. Geben Sie einen Namen für die Vorlage ein.

Nachdem Sie auf **Fertig stellen** geklickt haben, wird die neue Vorlage auf der Registerkarte **Vorlagen** angezeigt.

Erstellen einer neuen Vorlage basierend auf einer Richtlinie

1. Wählen Sie im Studio-Navigationsbereich **Richtlinien** aus.
2. Wählen Sie die Registerkarte **Richtlinien** und dann die Richtlinie, mit der Sie die neue Vorlage erstellen möchten.
3. Wählen Sie im Aktionsbereich **Als Vorlage speichern**.
4. Wählen und konfigurieren Sie die neuen Richtlinieneinstellungen, die Sie in die Vorlage einschließen möchten. Entfernen Sie vorhandene Einstellungen, die nicht eingeschlossen werden sollen. Geben Sie einen Namen und eine Beschreibung für die Vorlage ein und klicken Sie auf **Fertig stellen**.

Importieren einer Vorlage

1. Wählen Sie im Studio-Navigationsbereich **Richtlinien** aus.
2. Wählen Sie die Registerkarte **Vorlagen** und dann **Vorlage importieren**.
3. Wählen Sie die Vorlagendatei, die Sie importieren möchten, und klicken Sie auf **Öffnen**. Wenn Sie eine Vorlage importieren, die denselben Namen wie eine vorhandene hat, können Sie die vorhandene Vorlage überschreiben oder die Vorlage unter einem anderen Namen speichern, der automatisch generiert wird.

Exportieren einer Vorlage

1. Wählen Sie im Studio-Navigationsbereich **Richtlinien** aus.
2. Wählen Sie die Registerkarte **Vorlagen** und dann **Vorlage exportieren**.
3. Legen Sie den Speicherort für die Vorlage fest, und klicken Sie auf **Speichern**.

Im angegebenen Speicherort wird eine GPT-Datei erstellt.

Erstellen und Verwalten von Vorlagen mit dem Gruppenrichtlinien-Editor

Navigieren Sie im Gruppenrichtlinien-Editor zu Computerkonfiguration oder Benutzerkonfiguration. Erweitern Sie den Knoten Richtlinien und wählen Sie dann Citrix Richtlinien. Wählen Sie die entsprechende Aktion aus.

Aufgabe	Anweisung
Erstellen einer Vorlage basierend auf einer vorhandenen Richtlinie	Wählen Sie auf der Registerkarte "Richtlinien" die Richtlinie aus, und wählen Sie dann Aktionen > Als Vorlage speichern.
Erstellen einer Richtlinie basierend auf einer vorhandenen Vorlage	Wählen Sie auf der Registerkarte "Vorlagen" die entsprechende Vorlage aus und klicken Sie dann auf Neue Richtlinie.
Erstellen einer Vorlage basierend auf einer vorhandenen Vorlage	Wählen Sie auf der Registerkarte "Vorlagen" die entsprechende Vorlage aus und klicken Sie dann auf Neue Vorlage.
Importieren einer Vorlage	Wählen Sie auf die Registerkarte "Vorlagen" die Optionen Aktionen > Importieren.
Exportieren einer Vorlage	Wählen Sie auf die Registerkarte "Vorlagen" die Optionen Aktionen > Exportieren.
Anzeigen der Vorlageneinstellungen	Wählen Sie auf der Registerkarte "Vorlagen" die entsprechende Vorlage aus und klicken Sie dann auf die Registerkarte "Einstellungen".

Aufgabe	Anweisung
Anzeigen einer Zusammenfassung von Vorlageneigenschaften	Wählen Sie auf der Registerkarte "Vorlagen" die entsprechende Vorlage aus und klicken Sie dann auf die Registerkarte "Eigenschaften".
Anzeigen von Vorlagenvoraussetzungen	Wählen Sie auf der Registerkarte "Vorlagen" die entsprechende Vorlage aus und klicken Sie dann auf die Registerkarte "Voraussetzungen".

Vorlagen und delegierte Administration

Richtlinienvorlagen werden auf der Maschine gespeichert, auf der das Richtlinienverwaltungspaket installiert wurde. Das ist entweder die Maschine mit dem Delivery Controller oder die Maschine für die Verwaltung der Gruppenrichtlinienobjekte, jedoch nicht die Maschine mit der XenApp- und XenDesktop-Sitedatenbank. Daher werden die Richtlinienvorlagen nicht über die Rollen und Geltungsbereiche der delegierten Site-Verwaltung, sondern über Windows-Administratorrechte gesteuert.

Dies bedeutet, dass ein Administrator, der über Leseberechtigungen für die Site verfügt, beispielsweise neue Vorlagen erstellen kann. Da Vorlagen jedoch lokale Dateien sind, werden an der Umgebung keine Änderungen vorgenommen.

Benutzerdefinierte Vorlagen sind für das Benutzerkonto sichtbar, das sie erstellt hat, und werden im Windows-Profil des Benutzers gespeichert. Wenn Sie eine benutzerdefinierte Vorlage umfassender verfügbar machen möchten, erstellen Sie daraus eine Richtlinie oder exportieren Sie die Vorlage in einen freigegebenen Speicherort.

Erstellen von Richtlinien

Feb 29, 2016

Legen Sie vor dem Erstellen einer Richtlinie fest, für welche Benutzergruppen oder Geräte sie gelten soll. Sie können Richtlinien basierend auf Aufgabenbereich, Verbindungstyp, Benutzergerät oder geografischer Position erstellen. Alternativ können Sie die gleichen Kriterien verwenden wie für Windows Active Directory-Gruppenrichtlinien.

Wenn Sie bereits eine Richtlinie für eine Gruppe erstellt haben, sollten Sie möglichst die Richtlinie bearbeiten und die entsprechenden Einstellungen konfigurieren, statt eine andere Richtlinie zu erstellen. Vermeiden Sie es, eine neue Richtlinie zu erstellen, deren einziger Zweck ist, eine bestimmte Einstellung zu aktivieren oder bestimmte Benutzer von der Richtlinie auszunehmen.

Wenn Sie eine Richtlinie erstellen, verwenden Sie als Basis eine Richtlinienvorlage und passen Sie die Einstellungen nach Bedarf an. Sie können die Richtlinie natürlich auch ohne Vorlage erstellen und alle benötigten Einstellungen hinzufügen.

Richtlinieneinstellungen

Richtlinieneinstellungen können deaktiviert, aktiviert oder nicht konfiguriert sein. Standardmäßig sind Richtlinieneinstellungen nicht konfiguriert, d. h. sie wurden keiner Richtlinie hinzugefügt. Einstellungen werden nur angewendet, wenn sie einer Richtlinie hinzugefügt wurden.

Manche Richtlinieneinstellungen können einen der folgenden Zustände haben:

- Mit Zugelassen oder Nicht zugelassen wird die durch die Einstellung gesteuerte Aktion ermöglicht oder verhindert. In manchen Fällen dürfen Benutzer die Aktion der Einstellung in der Sitzung verwalten, in anderen dürfen sie das nicht. Wenn beispielsweise für Menüanimation die Einstellung auf "Zugelassen" festgelegt ist, können Benutzer Menüanimationen in ihrer Clientumgebung steuern.
- Mit Aktiviert oder Deaktiviert schalten Sie die Einstellung ein oder aus. Wenn Sie eine Einstellung deaktivieren, wird sie nicht durch Richtlinien mit geringerer Priorität aktiviert.

Manche Einstellungen steuern außerdem die Wirksamkeit von abhängigen Einstellungen. Die Einstellung Clientlaufwerkumleitung steuert beispielsweise, ob Benutzer auf die Laufwerke ihres Geräts zugreifen können. Damit Benutzer auf Netzlaufwerke zugreifen können, muss sowohl diese Einstellung als auch die Einstellung Clientnetzlaufwerke der Richtlinie hinzugefügt werden. Wenn die Einstellung Clientlaufwerkumleitung deaktiviert ist, können Benutzer nicht auf ihre Netzlaufwerke zugreifen, selbst wenn die Einstellung Clientnetzlaufwerke aktiviert ist.

In der Regel treten Änderungen an Richtlinieneinstellungen, die sich auf Maschinen auswirken, in Kraft, wenn der virtuelle Desktop neu gestartet wird oder wenn sich ein Benutzer anmeldet. Änderungen an Richtlinieneinstellungen, die Auswirkungen auf Benutzer haben, treten in Kraft, wenn sich die Benutzer das nächste Mal anmelden. Wenn Sie Active Directory verwenden, werden die Richtlinieneinstellungen aktualisiert, wenn Active Directory die Richtlinien in 90-Minuten-Intervallen erneut evaluiert. Die Richtlinieneinstellungen werden angewendet, wenn der virtuelle Desktop neu gestartet wird oder wenn sich ein Benutzer anmeldet.

Für manche Richtlinieneinstellungen können Sie einen Wert eingeben oder auswählen, wenn Sie die Einstellung der Richtlinie hinzufügen. Sie können die Konfiguration der Einstellung einschränken, indem Sie Standardwert verwenden wählen. Dadurch deaktivieren Sie die Konfiguration der Einstellung und nur der Standardwert der Einstellung darf verwendet werden, wenn die Richtlinie angewendet wird, unabhängig von dem Wert, der vor dem Aktivieren von Standardwert verwenden eingegeben wurde.

Bewährte Methoden:

- Weisen Sie Richtlinien Gruppen statt einzelnen Benutzern zu. Wenn Sie Richtlinien Gruppen zuweisen, werden Zuweisungen automatisch aktualisiert, wenn Sie Benutzer Gruppen hinzufügen oder sie daraus entfernen.
- Aktivieren Sie nicht widersprechende oder überlappende Einstellungen in der Konfiguration des Remotedesktop-Sitzungshosts. In manchen Fällen bietet die Remotedesktop-Sitzungshostkonfiguration ähnliche Funktionalität wie Citrix Richtlinieneinstellungen. Wählen Sie nach Möglichkeit für alle Einstellungen den gleichen Status (aktiviert oder deaktiviert), um die Problembehandlung zu erleichtern.
- Deaktivieren Sie Richtlinien, die nicht verwendet werden. Richtlinien, denen keine Einstellungen hinzugefügt wurden, verursachen unnötigen Verarbeitungsaufwand.

Richtlinienzuweisungen

Wenn Sie eine Richtlinie erstellen und bestimmten Benutzer- und Maschinenobjekten zuweisen, wird sie gemäß bestimmter Kriterien oder Regeln auf Verbindungen angewendet. Basierend auf einer Kombination von Kriterien können Sie in der Regel beliebig viele Zuweisungen für eine Richtlinie hinzufügen. Wenn keine Zuweisung angegeben wurde, gilt die Richtlinie für alle Verbindungen.

In der folgenden Tabelle werden verfügbare Zuweisungen aufgelistet:

Name	**Anwendung der Richtlinie basierend auf**
Zugriffssteuerung	Zugriffssteuerungsbedingungen, unter denen Clients eine Verbindung herstellen • Verbindungstyp: Ob die Richtlinie auf Verbindungen anzuwenden ist, die mit oder ohne NetScaler Gateway hergestellt wurden. • NetScaler Gateway-Farmname: Name des virtuellen NetScaler Gateway-Servers. • Zugriffsbedingung: Name der zu verwendenden Endpunktanalyserichtlinie oder Sitzungsrichtlinie.
Citrix CloudBridge	Ob eine Benutzersitzung über Citrix CloudBridge gestartet wird. Hinweis: Sie können einer Richtlinie nur eine Citrix CloudBridge-Zuweisung hinzufügen.
Client-IP-Adresse	IP-Adresse des Benutzergeräts, das zum Verbinden der Sitzung verwendet wird • IPv4-Beispiele: 12.0.0.0, 12.0.0.*, 12.0.0.1-12.0.0.70, 12.0.0.1/24 • IPv6-Beispiele: 2001:0db8:3c4d:0015:0:0:abcd:ef12, 2001:0db8:3c4d:0015::/54
Clientname	Name des Benutzergeräts • Genaue Übereinstimmung: ClientABCName • Verwenden von Platzhalter: Client*Name
Bereitstellungsgruppe	Bereitstellungsgruppen-Mitgliedschaft
Bereitstellungsgruppentyp	Desktop- oder Anwendungstyp: privater Desktop, freigegebener Desktop, private Anwendung oder freigegebene Anwendung
Organisationseinheit	Organisationseinheit

Tag Name	Tags Anwendung der Richtlinie basierend auf
	Hinweis: Installieren Sie den unter CTX142439 verfügbaren Hotfix, um sicherzustellen, dass die Richtlinien bei der Verwendung von Tags richtig angewendet werden.
Benutzer oder Gruppe	Benutzer- oder Gruppenname

Alle Richtlinien, die mit den Zuweisungen für die Verbindung übereinstimmen, werden bei der Anmeldung eines Benutzers identifiziert. Die Richtlinien werden nach Priorität sortiert und mehrere Instanzen jeder Einstellung werden verglichen. Die einzelnen Einstellungen werden gemäß der Richtlinien-Prioritätsreihenfolge angewendet. Jede deaktivierte Richtlinieneinstellung hat Vorrang vor einer aktivierten Richtlinieneinstellung, deren Priorität niedriger ist. Richtlinieneinstellungen, die nicht konfiguriert sind, werden ignoriert.

Wichtig: Bei der Konfiguration von Active Directory- und Citrix Richtlinien mit der Gruppenrichtlinien-Verwaltungskonsole werden Zuweisungen und Einstellungen möglicherweise nicht wie erwartet angewendet. Weitere Informationen finden Sie unter CTX127461.
Eine Richtlinie mit dem Namen "Ungefiltert" ist standardmäßig verfügbar.

- Wenn Sie Studio zur Verwaltung von Citrix Richtlinien verwenden, werden die Einstellungen, die Sie der Richtlinie "Ungefiltert" hinzufügen, auf alle Server, Desktops und Verbindungen einer Site angewendet.
- Wenn Sie mit dem Editor für lokale Gruppenrichtlinien Citrix Richtlinien verwalten, gelten Einstellungen, die Sie der Richtlinie "Ungefiltert" hinzufügen, für alle Sites und Verbindungen, die zu dem Geltungsbereich des Gruppenrichtlinienobjekts gehören, das die Richtlinie enthält. Beispiel: Die Organisationseinheit (OU) "Verkauf" enthält ein Gruppenrichtlinienobjekt "Verkauf-USA", das alle Mitarbeiter des US-Verkaufsteams einschließt. Das Gruppenrichtlinienobjekt "Verkauf-USA" ist mit einer Richtlinie "Ungefiltert" konfiguriert, die mehrere Benutzerrichtlinieneinstellungen enthält. Wenn der US-Verkaufsleiter sich an der Site anmeldet, werden die Einstellungen der Richtlinie "Ungefiltert" automatisch auf die Sitzung angewendet, weil der Benutzer Mitglied des Gruppenrichtlinienobjekts "Verkauf-USA" ist.

Der Modus einer Zuweisung entscheidet, ob die Richtlinie nur auf Verbindungen angewendet wird, die alle Zuweisungskriterien erfüllen. Wenn der Modus Zulassen (Standardwert) ist, wird die Richtlinie nur auf Verbindungen angewendet, die die Zuweisungskriterien erfüllen. Wenn der Modus Verweigern ist, wird die Richtlinie angewendet, wenn eine Verbindung die Zuweisungskriterien nicht erfüllt. Das folgende Beispiel zeigt, wie Zuweisungsmodi sich auf Citrix Richtlinien auswirken, wenn mehrere Zuweisungen vorhanden sind.

- **Beispiel: Zuweisungen des gleichen Typs mit unterschiedlichen Modi**: In Richtlinien mit zwei Zuweisungen des gleichen Typs, eine mit der Einstellung Zulassen und die andere mit der Einstellung Verweigern, hat die Zuweisung mit der Einstellung Verweigern Vorrang, wenn die Verbindung die Kriterien beider Zuweisungen erfüllt. Beispiel:
  Richtlinie 1 enthält die folgenden Zuweisungen:
  - Zuweisung A bestimmt die Verkaufsgruppe, und der Modus ist Zulassen
  - Zuweisung B bestimmt das Konto des Verkaufsleiters, und der Modus ist Verweigern

  Da der Modus für Zuweisung B Verweigern ist, wird die Richtlinie nicht angewendet, wenn der Verkaufsleiter sich bei der Site anmeldet, obwohl er Mitglied der Verkaufsgruppe ist.

- **Beispiel: Zuweisungen unterschiedlichen Typs mit gleichen Modi**: In Richtlinien mit zwei oder mehr Zuweisungen unterschiedlichen Typs, für die Zulassen eingestellt ist, muss die Verbindung die Kriterien von mindestens einer Zuweisung jedes Typs erfüllen, damit die Richtlinie angewendet wird. Beispiel:
  Richtlinie 2 enthält die folgenden Zuweisungen:
  - Zuweisung C ist eine Benutzerzuweisung, die die Verkaufsgruppe angibt, und der Modus ist Zulassen

- Zuweisung D ist eine Client-IP-Adressenzuweisung, die 10.8.169.* festlegt (das Unternehmensnetzwerk), und der Modus ist Zulassen.

Wenn der Verkaufsleiter sich im Büro bei der Site anmeldet, wird die Richtlinie angewendet, weil die Verbindung die Kriterien beider Zuweisungen erfüllt.

Richtlinie 3 enthält die folgenden Zuweisungen:

- Zuweisung E ist eine Benutzerzuweisung, die die Verkaufsgruppe angibt, und der Modus ist Zulassen
- Zuweisung F ist eine Zugriffssteuerungszuweisung, die NetScaler Gateway-Verbindungsbedingungen angibt, und der Modus ist Zulassen.

Wenn der Verkaufsleiter sich im Büro bei der Site anmeldet, wird die Richtlinie nicht angewendet, weil die Verbindung nicht die Kriterien von Zuweisung F erfüllt.

Erstellen einer Richtlinie basierend auf einer Vorlage mit Studio

1. Wählen Sie im Studio-Navigationsbereich Richtlinien aus.
2. Wählen Sie die Registerkarte "Vorlagen" und wählen Sie dann eine Vorlage.
3. Wählen Sie im Aktionsbereich Richtlinie aus Vorlage erstellen.
4. Standardmäßig verwendet die neue Richtlinie alle Standardeinstellungen der Vorlage (das Optionsfeld Standardeinstellungen der Vorlage ist ausgewählt). Um die Einstellungen zu ändern, wählen Sie das Optionsfeld Standardeinstellungen ändern und Einstellungen hinzufügen, und fügen Sie Einstellungen hinzu oder entfernen Sie sie.
5. Legen Sie fest, wie die Richtlinie angewendet werden soll, indem Sie eine der folgenden Optionen auswählen:
   - Ausgewählten Benutzer- und Maschinenobjekten zuweisen und wählen Sie dann die Benutzer- und Maschinenobjekte, auf die Sie die Richtlinie anwenden möchten.
   - Allen Objekten in der Site zuweisen, damit die Richtlinie auf alle Benutzer- und Maschinenobjekte in der Site angewendet wird.
6. Geben Sie einen Namen für die Richtlinie ein (oder akzeptieren Sie den Standardwert). Empfehlenswert sind Richtliniennamen, die beschreiben, wer von der Richtlinie betroffen ist, z. B. Buchhaltung oder Remotebenutzer. Geben Sie optional eine Beschreibung ein.
   Die Richtlinie ist standardmäßig aktiviert. Sie können sie deaktivieren. Wenn die Richtlinie aktiviert ist, kann sie sofort auf Benutzer, die sich anmelden, angewendet werden. Deaktivieren der Richtlinie verhindert, dass sie angewendet wird. Wenn Sie die Priorität der Richtlinie ändern müssen oder später weitere Einstellungen hinzufügen möchten, können Sie die Richtlinie deaktivieren, bis Sie damit fertig sind, und die Richtlinie dann anwenden.

Erstellen einer Richtlinie mit Studio

1. Wählen Sie im Studio-Navigationsbereich Richtlinien aus.
2. Wählen Sie die Registerkarte Richtlinien.
3. Wählen Sie im Aktionsbereich Richtlinie erstellen.
4. Fügen Sie Richtlinieneinstellungen nach Bedarf hinzu und konfigurieren Sie diese.
5. Legen Sie fest, wie die Richtlinie angewendet werden soll, indem Sie eine der folgenden Optionen auswählen:
   - Ausgewählten Benutzer- und Maschinenobjekten zuweisen und wählen Sie dann die Benutzer- und Maschinenobjekte, auf die Sie die Richtlinie anwenden möchten.
   - Allen Objekten in der Site zuweisen, damit die Richtlinie auf alle Benutzer- und Maschinenobjekte in der Site angewendet wird.
6. Geben Sie einen Namen für die Richtlinie ein (oder akzeptieren Sie den Standardwert). Empfehlenswert sind Richtliniennamen, die beschreiben, wer von der Richtlinie betroffen ist, z. B. Buchhaltung oder Remotebenutzer. Geben Sie optional eine Beschreibung ein.
   Die Richtlinie ist standardmäßig aktiviert. Sie können sie deaktivieren. Wenn die Richtlinie aktiviert ist, kann sie sofort auf

Benutzer, die sich anmelden, angewendet werden. Deaktivieren der Richtlinie verhindert, dass sie angewendet wird. Wenn Sie die Priorität der Richtlinie ändern müssen oder später weitere Einstellungen hinzufügen möchten, können Sie die Richtlinie deaktivieren, bis Sie damit fertig sind, und die Richtlinie dann anwenden.

Erstellen und Verwalten von Richtlinien mit dem Gruppenrichtlinien-Editor

Navigieren Sie im Gruppenrichtlinien-Editor zu Computerkonfiguration oder Benutzerkonfiguration. Erweitern Sie den Knoten Richtlinien und wählen Sie dann Citrix Richtlinien. Wählen Sie die entsprechende Aktion aus.

Aufgabe	**Anweisung**
Erstellen einer Richtlinie	Klicken Sie auf der Registerkarte "Richtlinien" auf Neu.
Bearbeiten einer bestehenden Richtlinie	Wählen Sie auf der Registerkarte "Richtlinien" die entsprechende Richtlinie aus und klicken Sie dann auf Bearbeiten.
Ändern der Priorität einer bestehenden Richtlinie	Wählen Sie auf der Registerkarte "Richtlinien" die entsprechende Richtlinie aus und klicken Sie dann auf Höhere Priorität oder Geringere Priorität.
Anzeigen einer Zusammenfassung über eine Richtlinie	Wählen Sie auf der Registerkarte "Richtlinien" die entsprechende Richtlinie aus und klicken Sie dann auf die Registerkarte Zusammenfassung.
Anzeigen und Ändern der Richtlinieneinstellungen	Wählen Sie auf der Registerkarte "Richtlinien" die entsprechende Richtlinie aus und klicken Sie dann auf die Registerkarte Einstellungen.
Anzeigen und Ändern der Richtlinienfilter	Wählen Sie auf der Registerkarte "Richtlinien" die entsprechende Richtlinie aus und klicken Sie dann auf die Registerkarte Einstellungen.
Aktivieren oder Deaktivieren einer Richtlinie	Wählen Sie auf der Registerkarte "Richtlinien" die entsprechende Richtlinie aus und klicken Sie dann auf Aktionen > Aktivieren oder Aktionen > Deaktivieren.
Erstellen einer Richtlinie basierend auf einer vorhandenen Vorlage	Wählen Sie auf der Registerkarte "Vorlagen" die entsprechende Vorlage aus und klicken Sie dann auf Neue Richtlinie.

Vergleichen, Priorisieren, Modellieren und Problembehandlung für Richtlinien

Feb 29, 2016

Sie können mit mehreren Richtlinien Ihre Umgebung an die Anforderungen der Benutzer, basierend auf deren Aufgabengebiet, geografischem Standort oder Verbindungstyp anpassen. Beispielsweise sind Sie vielleicht aus Sicherheitsgründen gezwungen, Benutzergruppen, die regelmäßig mit sensiblen Daten arbeiten, Beschränkungen aufzuerlegen. Sie können eine Richtlinie erstellen, die Benutzer daran hindert, vertrauliche Daten auf ihren lokalen Clientlaufwerken zu speichern. Wenn jedoch manche Mitglieder dieser Benutzergruppe Zugang zu ihren lokalen Laufwerken benötigen, können Sie eine andere Richtlinie für diese Benutzer erstellen. Anschließend können Sie den beiden Richtlinien jeweils eine Priorität zuweisen und damit festlegen, welche Richtlinie Vorrang haben soll.

Wenn Sie mehrere Richtlinien verwenden, müssen Sie festlegen, wie Prioritäten zugewiesen und Ausnahmen erstellt werden und wie die wirksame Richtlinie bei Richtlinienkonflikten angezeigt wird.

In der Regel setzen Richtlinien ähnliche Einstellungen, die für die gesamte Site, für bestimmte Delivery Controller oder auf dem Benutzergerät konfiguriert wurden, außer Kraft. Die Ausnahme von diesem Prinzip sind Sicherheitseinstellungen. Die höchste Verschlüsselungseinstellung in der Umgebung, einschließlich Betriebssystem, und die Spiegelungseinstellung mit der größten Einschränkung haben immer Vorrang vor allen anderen Einstellungen und Richtlinien.

Citrix Richtlinien interagieren mit den Richtlinien, die Sie im Betriebssystem eingestellt haben. In einer Citrix Umgebung überschreiben Citrix Einstellungen die gleichen Einstellungen in einer Active Directory-Richtlinie oder in der Konfiguration des Remotedesktop-Sitzungshosts. Dazu gehören auch Einstellungen, die mit typischen Remotedesktopprotokoll-Clientverbindungseinstellungen zusammenhängen, wie Desktophintergrund, Menüanimation und das Anzeigeverhalten beim Drag & Drop. Manche Richtlinieneinstellungen, wie SecureICA, müssen mit den Richtlinien und Einstellungen im Betriebssystem übereinstimmen. Wenn anderswo ein höherer Verschlüsselungsgrad festgelegt wurde, kann die SecureICA-Richtlinieneinstellung oder die Einstellung beim Veröffentlichen einer Anwendung außer Kraft gesetzt werden.

Die beim Erstellen von Bereitstellungsgruppen angegebenen Verschlüsselungseinstellungen sollten beispielsweise den gleichen Verschlüsselungsgrad verwenden, den Sie an anderer Stelle in der Umgebung verwenden.

Hinweis: Wenn im zweiten Hop eines Double-Hop-Szenarios ein Desktopbetriebssystem-VDA eine Verbindung mit einem Serverbetriebssystem-VDA herstellt, ist die Wirkung der Citrix Richtlinien auf den Desktopbetriebssystem-VDA die gleiche wie beim Benutzergerät. Wenn Richtlinien beispielsweise das Zwischenspeichern von Bildern auf dem Benutzergerät festlegen, werden die Bilder, die während des zweiten Hop in einem Double-Hop-Szenario zwischengespeichert werden, auf der Desktopbetriebssystem-VDA-Maschine zwischengespeichert.

Vergleichen von Richtlinien und Vorlagen

Sie können die Einstellungen einer Richtlinie oder Vorlage mit denen in anderen Richtlinien oder Vorlagen vergleichen. Sie können beispielsweise Einstellungswerte prüfen, um sicherzustellen, dass optimale Verfahren eingehalten werden. Außerdem ist ggf. ein Vergleich von Einstellungen in einer Richtlinie oder Vorlage mit den Standardeinstellungen von Citrix erforderlich.

1. Wählen Sie im Studio-Navigationsbereich Richtlinien aus.
2. Klicken Sie auf die Registerkarte "Vergleich" und dann auf Auswählen.
3. Wählen Sie die Richtlinien oder Vorlagen aus, die Sie vergleichen möchten. Aktivieren Sie das Kontrollkästchen Mit Standardeinstellungen vergleichen, um Standardwerte im Vergleich einzuschließen.
4. Wenn Sie auf Vergleichen klicken, werden die konfigurierten Einstellungen in Spalten angezeigt.
5. Zum Anzeigen aller Einstellungen wählen Sie Alle Einstellungen anzeigen. Sie kehren zur Standardansicht zurück, indem Sie

Gemeinsame Einstellungen anzeigen auswählen.

Festlegen der Richtlinienpriorität

Durch Festlegen der Richtlinienpriorität definieren Sie, welche Richtlinie Vorrang hat, wenn es Konflikte gibt. Alle Richtlinien, die mit den Zuweisungen für die Verbindung übereinstimmen, werden bei der Anmeldung eines Benutzers identifiziert. Die Richtlinien werden nach Priorität sortiert und mehrere Instanzen jeder Einstellung werden verglichen. Die einzelnen Einstellungen werden gemäß der Richtlinien-Prioritätsreihenfolge angewendet.

Sie weisen Richtlinien Prioritäten zu, indem Sie ihnen unterschiedliche Prioritätswerte in Studio geben. Neue Richtlinien erhalten standardmäßig die niedrigste Priorität. Falls widersprüchliche Richtlinieneinstellungen auftreten, setzt eine Richtlinie mit einem höheren Prioritätswert (eine Priorität von "1" hat die höchste Priorität) eine Richtlinie mit einem niedrigeren Prioritätswert außer Kraft. Einstellungen werden nach der Priorität und dem Zustand der Einstellung, z. B. ob die Einstellung deaktiviert oder aktiviert ist, zusammengeführt. Jede deaktivierte Einstellung hat Vorrang vor einer aktivierten Einstellung, deren Priorität niedriger ist. Richtlinieneinstellungen, die nicht konfiguriert sind, werden ignoriert und setzen keine Einstellungen mit niedrigerer Priorität außer Kraft.

1. Wählen Sie im Studio-Navigationsbereich Richtlinien aus. Wählen Sie die Registerkarte "Richtlinien" aus.
2. Wählen Sie eine Richtlinie.
3. Wählen Sie im Aktionsbereich Geringere Priorität oder Höhere Priorität.

Ausnahmen

Wenn Sie Richtlinien für Benutzergruppen, Benutzergeräte oder Maschinen erstellen, werden Sie möglicherweise feststellen, dass für einige Mitglieder einer Gruppe Ausnahmen zu einigen Einstellungen erstellt werden müssen. Sie können Ausnahmen wie folgt erstellen:

- Erstellen Sie eine Richtlinie für die Gruppenmitglieder, für die Ausnahmen erforderlich sind, und stufen Sie die Richtlinie mit höherer Priorität ein als die Richtlinie für die gesamte Gruppe.
- Verwenden Sie den Modus Verweigern in einer Zuweisung, die Sie der Richtlinie hinzufügen.

Die Zuweisung im Modus Verweigern wendet eine Richtlinie nur auf Verbindungen an, die nicht den Zuweisungskriterien entsprechen. Beispielsweise könnte eine Richtlinie folgende Zuweisungen enthalten:

- Zuweisung A ist eine Client-IP-Adressenzuweisung, die den Bereich 208.77.88.* festlegt, und der Modus ist Zulassen
- Zuweisung B ist eine Benutzerzuweisung, die ein spezifisches Benutzerkonto angibt, und der Modus ist Verweigern

Die Richtlinie wird auf alle Benutzer angewendet, die sich mit IP-Adressen aus dem in Zuweisung A festgelegten Bereich bei der Site anmelden. Die Richtlinie wird aber nicht auf den Benutzer angewendet, der sich mit dem in Zuweisung B festgelegten Konto anmeldet, obwohl dem Computer dieses Benutzers eine IP-Adresse aus dem in Zuweisung A festgelegten Bereich zugewiesen wurde.

Ermitteln der auf eine Verbindung angewendeten Richtlinien

Manchmal reagiert eine Verbindung nicht wie erwartet, weil mehrere Richtlinien gelten. Wenn eine Richtlinie mit einer höheren Priorität auf eine Verbindung angewendet wird, kann sie Einstellungen, die Sie in der ursprünglichen Richtlinie konfigurieren, außer Kraft setzen. Sie können ermitteln, wie die Richtlinieneinstellungen am Ende für eine Verbindung zusammengeführt werden, indem sie den Richtlinienergebnissatz berechnen.

Sie berechnen den Richtlinienergebnissatz mit folgenden Methoden:

- Verwenden Sie den Assistenten für die Citrix Gruppenrichtlinienmodellierung, um ein Verbindungsszenario zu simulieren und festzustellen, wie Citrix Richtlinien angewendet werden können. Sie können Bedingungen für ein Verbindungsszenario angeben, z. B. Domänencontroller, Benutzer, Citrix Richtlinienzuweisungsbeweiswerte und simulierte Umgebungseinstellungen wie langsame Netzwerkverbindungen. Der von dem Assistenten erstellte Bericht listet die Citrix

Richtlinien auf, die in dem Szenario wahrscheinlich wirksam werden. Wenn Sie beim Controller als Domänenbenutzer angemeldet sind, berechnet der Assistent den Richtlinienergebnissatz anhand von Richtlinieneinstellungen für die Site und Active Directory-Gruppenrichtlinienobjekten.

- Verwenden Sie das Tool "Gruppenrichtlinienergebnisse", um einen Bericht zu erstellen, der beschreibt, welche Citrix Richtlinien für einen bestimmten Benutzer oder einen bestimmten Controller angewendet werden. Das Tool "Gruppenrichtlinienergebnisse" unterstützt Sie dabei, den aktuellen Zustand von Gruppenrichtlinienobjekten in der Umgebung zu evaluieren, und generiert einen Bericht, in dem beschrieben wird, wie diese Objekte, einschließlich Citrix Richtlinien, derzeit auf einen bestimmten Benutzer und Controller angewendet werden.

Sie können den Assistenten für die Citrix Gruppenrichtlinienmodellierung im Bereich "Aktionen" in Studio starten. Sie können beide Tools in der Gruppenrichtlinien-Verwaltungskonsole von Windows starten.

Wenn Sie den Assistenten für die Citrix Gruppenrichtlinienmodellierung oder das Tool "Gruppenrichtlinienergebnisse" über die Gruppenrichtlinien-Verwaltungskonsole ausführen, werden die mit Studio erstellten Site-Richtlinieneinstellungen nicht in den Richtlinienergebnissatz einbezogen.

Um sicherzustellen, dass Sie den umfassendsten Richtlinienergebnissatz erhalten, empfiehlt Citrix das Starten des Assistenten für die Citrix Gruppenrichtlinienmodellierung über Studio, es sei denn, Sie erstellen Richtlinien nur über die Gruppenrichtlinien-Verwaltungskonsole.

Verwenden des Assistenten für die Citrix Gruppenrichtlinienmodellierung

Öffnen Sie den Assistenten für die Citrix Gruppenrichtlinienmodellierung mit einer der folgenden Optionen:

- Wählen Sie Richtlinien im Navigationsbereich von Studio, wählen Sie dann die Registerkarte "Modellierung" und dann im Aktionsbereich die Option Modellierungsassistenten starten.
- Starten Sie die Gruppenrichtlinien-Verwaltungskonsole (gpmc.msc), klicken Sie mit der rechten Maustaste in der Konsolenstruktur auf Citrix Gruppenrichtlinienmodellierung und wählen Sie dann Citrix Gruppenrichtlinienmodellierungsassistent aus.

Folgen Sie den Anweisungen des Assistenten, um den Domänencontroller, Benutzer, Computer, Umgebungseinstellungen und Citrix Zuweisungskriterien für die Simulation auszuwählen. Wenn Sie auf Fertig stellen klicken, erstellt der Assistent einen Bericht mit den Modellierungsergebnissen. In Studio wird der Bericht im mittleren Bereich unter der Registerkarte Modellierung angezeigt.

Zum Anzeigen des Berichts wählen Sie Modellierungsbericht anzeigen.

Problembehandlung bei Richtlinien

Für Benutzer, IP-Adressen und andere zugewiesene Objekte können mehrere Richtlinien gleichzeitig gelten. Dies kann zu Konflikten führen, wenn eine Richtlinie sich nicht wie erwartet verhält. Wenn Sie den Citrix Gruppenrichtlinienmodellierungsassistenten oder das Gruppenrichtlinienergebnisse-Tool ausführen, entdecken Sie möglicherweise, dass keine Richtlinien auf die Benutzerverbindungen angewendet werden. In diesen Fall sind Benutzer nicht von Richtlinieneinstellungen betroffen, wenn sie sich unter Bedingungen mit Anwendungen verbinden, die den Richtlinienkriterien entsprechen. Dies passiert in folgenden Fällen:

- Keine Richtlinie hat eine Zuweisung, die den Richtlinienkriterien entspricht.
- Richtlinien, die der Zuweisung entsprechen, haben keine konfigurierten Einstellungen.
- Richtlinien, die der Zuweisung entsprechen, sind deaktiviert.

Wenn Sie Richtlinieneinstellungen auf Verbindungen anwenden möchten, die bestimmten Kriterien entsprechen, stellen Sie Folgendes sicher:

- Die Richtlinien, die auf diese Verbindungen angewendet werden sollen, sind aktiviert.
- In den Richtlinien, die Sie anwenden möchten, sind die geeigneten Einstellungen konfiguriert.

Standardrichtlinieneinstellungen

Feb 29, 2016

Die folgenden Tabellen enthalten Richtlinieneinstellungen, die Standardeinstellungen und die VDA-Versionen, für die sie gelten.

ICA

Name	Standardeinstellung	VDA
Clientzwischenablagenumleitung	Zugelassen	Alle VDA-Versionen
Desktop starten	Nicht zugelassen	VDA für Server-OS 7 bis aktuelle Version
ICA-Listener - Verbindungstimeout	120.000 Millisekunden	VDA 5, 5.5, 5.6 FP1, VDA für Desktop-OS 7 bis aktuelle Version
ICA-Listenerportnummer	1494	Alle VDA-Versionen
Starten nicht-veröffentlichter Programme bei Clientverbindung	Nicht zugelassen	VDA für Server-OS 7 bis aktuelle Version
Zum Schreiben in Clientzwischenablage zugelassene Formate	Keine Formate angegeben	VDA 7.6 bis aktuelle Version
Schreiben in Clientzwischenablage einschränken	Nicht zugelassen	VDA 7.6 bis aktuelle Version
Schreiben in Sitzungszwischenablage einschränken	Nicht zugelassen	VDA 7.6 bis aktuelle Version
Zum Schreiben in Sitzungszwischenablage zugelassene Formate	Keine Formate angegeben	VDA 7.6 bis aktuelle Version

ICA/Adobe Flash-Bereitstellung/Flash-Umleitung

Name	Standardeinstellung	VDA
Verhindern von Flash-Videofallback	Nicht konfiguriert	VDA 7.6 FP3 bis aktuelle Version
Fehler beim Verhindern von Flash-Videofallback *.swf		VDA 7.6 FP3 bis aktuelle Version

ICA/Audio

Name	Standardeinstellung	VDA

Name	Standardeinstellung	VDA
Audio Plug & Play	Zugelassen	VDA für Server-OS 7 bis aktuelle Version
Audioqualität	Hoch - High Definition Audio	Alle VDA-Versionen
Clientaudioumleitung	Zugelassen	Alle VDA-Versionen
Clientmikrofonumleitung	Zugelassen	Alle VDA-Versionen

ICA/Automatische Wiederverbindung von Clients

Name	Standardeinstellung	VDA
Automatische Wiederverbindung von Clients	Zugelassen	Alle VDA-Versionen
Authentifizierung bei automatischer Wiederverbindung von Clients	Keine Authentifizierung erforderlich	Alle VDA-Versionen
Protokollierung der automatischen Wiederverbindung von Clients	Kein Protokollieren von Wiederverbindungsereignissen	Alle VDA-Versionen

ICA/Bandwidth

Name	Standardeinstellung	VDA
Bandbreitenlimit für die Audioumleitung	0 KBit/s	Alle VDA-Versionen
Bandbreitenlimit für die Audioumleitung (Prozent)	0	Alle VDA-Versionen
Bandbreitenlimit für Client-USB-Geräteumleitung	0 KBit/s	VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
Bandbreitenlimit für Client-USB-Geräteumleitung (Prozent)	0	VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
Bandbreitenlimit für Zwischenablagenumleitung	0 KBit/s	Alle VDA-Versionen
Bandbreitenlimit für Zwischenablagenumleitung (Prozent)	0	Alle VDA-Versionen
Bandbreitenlimit für COM-Portumleitung	0 KBit/s	Alle VDA-Versionen; bei VDA 7 bis aktuelle Version müssen Sie diese Einstellung in der Registrierung konfigurieren.
Bandbreitenlimit für COM-	0	Alle VDA-Versionen; bei VDA 7 bis aktuelle Version

Name	Standardeinstellung	VDA
Portumleitung (Prozent)		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 FP 1, VDA für Server-OS 7 und VDA für Desktop-OS 7 bis zum aktuellen VDA für Server-OS und VDA für Desktop-OS
Bandbreitenlimit für HDX MediaStream-Multimediabeschleunigung (Prozent)	0	VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
Bandbreitenlimit für LPT-Portumleitung	0 KBit/s	Alle VDA-Versionen; bei VDA 7 bis aktuelle Version müssen Sie diese Einstellung in der Registrierung konfigurieren.
Bandbreitenlimit für LPT-Portumleitung (Prozent)	0	Alle VDA-Versionen; bei VDA 7 bis aktuelle Version müssen Sie diese Einstellung in der Registrierung konfigurieren.
Bandbreitenlimit für Sitzung insgesamt	0 KBit/s	Alle VDA-Versionen
Bandbreitenlimit für Druckerumleitung	0 KBit/s	Alle VDA-Versionen
Bandbreitenlimit für Druckerumleitung (Prozent)	0	Alle VDA-Versionen
Bandbreitenlimit für TWAIN-Geräteumleitung	0 KBit/s	VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
Bandbreitenlimit für TWAIN-Geräteumleitung (Prozent)	0	VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version

ICA/Clientsensoren

Name	Standardeinstellung	VDA
Anwendungen können den physischen Standort des Clientgeräts verwenden	Nicht zugelassen	VDA 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version

ICA/Desktopbenutzeroberfläche

Name	Standardeinstellung	VDA
Desktopgestaltungsumleitung	Aktiviert	VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
Grafikqualität Desktopgestaltung	Mittel	VDA 5, 5.5, 5.6 FP1, VDA für Desktop-OS 7 bis aktuelle Version
Desktophintergrund	Zugelassen	Alle VDA-Versionen
Menüanimation	Zugelassen	Alle VDA-Versionen
Fensterinhalt beim Verschieben anzeigen	Zugelassen	Alle VDA-Versionen

ICA/Endbenutzerüberwachung

Name	Standardeinstellung	VDA
ICA-Roundtripberechnung	Aktiviert	Alle VDA-Versionen
Intervall für ICA-Roundtripberechnung	15 Sekunden	Alle VDA-Versionen
ICA-Roundtrip für Verbindungen im Leerlauf berechnen	Deaktiviert	Alle VDA-Versionen

ICA/Enhanced Desktop Experience

Name	Standardeinstellung	VDA
Enhanced Desktop Experience	Zugelassen	VDA für Server-OS 7 bis aktuelle Version

ICA/Dateiumleitung

Name	Standardeinstellung	VDA
Clientlaufwerke automatisch verbinden	Zugelassen	Alle VDA-Versionen
Clientlaufwerkumleitung	Zugelassen	Alle VDA-Versionen
Lokale Clientfestplattenlaufwerke	Zugelassen	Alle VDA-Versionen
Clientdiskettenlaufwerke	Zugelassen	Alle VDA-Versionen

Name	Standardeinstellung	VDA
Clientnetzlaufwerke	Zugelassen	Alle VDA-Versionen
Optische Clientlaufwerke	Zugelassen	Alle VDA-Versionen
Clientwechsellaufwerke	Zugelassen	Alle VDA-Versionen
Host-zu-Client-Umleitung	Deaktiviert	VDA für Server-OS 7 bis aktuelle Version
Clientlaufwerksbuchstaben erhalten	Deaktiviert	VDA 5, 5.5, 5.6 FP1, VDA für Desktop-OS 7 bis aktuelle Version
Schreibgeschützter Zugriff auf Clientlaufwerke	Deaktiviert	VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
Umleitung spezieller Ordner	Zugelassen	Nur Webinterface-Bereitstellungen; VDA für Server-OS 7 bis aktuelle Version
Asynchrones Schreiben verwenden	Deaktiviert	Alle VDA-Versionen

ICA/Graphics

Name	Standardeinstellung	VDA
Anzeigespeicherlimit	65536 KBit	VDA 5, 5.5, 5.6 FP1, VDA für Desktop-OS 7 bis aktuelle Version
Herabsetzungspräferenz für Anzeigemodus	Zuerst Farbtiefe herabsetzen	Alle VDA-Versionen
Dynamische Fenstervorschau	Aktiviert	VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
Bildzwischenspeicherung	Aktiviert	VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
Legacygrafikmodus	Deaktiviert	VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
Maximal zugelassene Farbtiefe	32 Bit pro Pixel	Alle VDA-Versionen
Benutzer beim Herabsetzen des Anzeigemodus benachrichtigen	Deaktiviert	VDA für Server-OS 7 bis aktuelle Version
Warteschlange und Verwerfen	Aktiviert	Alle VDA-Versionen

ICA/Graphics/Caching

Name	Standardeinstellung	VDA
Schwellenwert für permanenten Cache	3000000 Bit/s	VDA für Server-OS 7 bis aktuelle Version

ICA/Graphics/Framehawk

Name	Standardeinstellung	VDA
Framehawk-Anzeigekanal	Deaktiviert	VDA 7.6 FP2 bis aktuelle Version
Portbereich für Framehawk-Anzeigekanal	3224,3324	VDA 7.6 FP2 bis aktuelle Version

ICA/Keep-Alive

Name	Standardeinstellung	VDA
ICA-Keep-Alive - Timeout	60 Sekunden	Alle VDA-Versionen
ICA-Keep-Alives	Keine ICA-Keep-Alive-Meldungen senden	Alle VDA-Versionen

ICA/Zugriff auf lokale Anwendungen

Name	Standardeinstellung	VDA
Lokalen App-Zugriff zulassen	Nicht zugelassen	VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
URL-Umleitungssperrliste	Keine Sites angegeben	VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
URL-Umleitungspositivliste	Keine Sites angegeben	VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version

ICA/Mobilerfahrung

Name	Standardeinstellung	VDA
Automatische Anzeige der Tastatur	Nicht zugelassen	VDA 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
Für Fingereingabe optimierten Desktop starten	Zugelassen	VDA 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version Diese Einstellung ist deaktiviert und für Windows 10-

Name	Standardeinstellung	VDA
Kombinationsfelder remoten	Nicht zugelassen	VDA 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version

Maschinen nicht verfügbar.

ICA/Multimedia

Name	Standardeinstellung	VDA
Videoqualität beschränken	Nicht konfiguriert	VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
Multimediakonferenzen	Zugelassen	Alle VDA-Versionen
Optimierung von Windows Media-Multimediaumleitung über WAN	Zugelassen	VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
GPU für die Optimierung von Windows Media-Multimediaumleitung über WAN verwenden	Nicht zugelassen	VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
Richtlinieneinstellung für Videolastverwaltung	Nicht konfiguriert	VDA 7.6 FP3 bis aktuelle Version
Clientseitiger Abruf von Windows Media-Inhalten	Zugelassen	VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
Windows Media-Umleitung	Zugelassen	Alle VDA-Versionen
Windows Media-Umleitungspuffergröße	5 Sekunden	VDA 5, 5.5, 5.6 FP1
Verwendung von Windows Media-Umleitungspuffergröße	Deaktiviert	VDA 5, 5.5, 5.6 FP1

ICA/Multistreamverbindungen

Name	Standardeinstellung	VDA
Audio über UDP	Zugelassen	VDA für Server-OS 7 bis aktuelle Version
Audio-UDP-Portbereich	16500, 16509	VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
Multiportrichtlinie	Primärer Port (2598) hat hohe Priorität	VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
Multistreamcomputereinstellung	Deaktiviert	VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
Multistreambenutzereinstellung	Deaktiviert	VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version

ICA\Portumleitung

Name	Standardeinstellung	VDA
Client-COM-Ports automatisch verbinden	Deaktiviert	Alle VDA-Versionen; bei VDA 7.x müssen Sie diese Einstellung in der Registrierung konfigurieren
Client-LPT-Ports automatisch verbinden	Deaktiviert	Alle VDA-Versionen; bei VDA 7.x müssen Sie diese Einstellung in der Registrierung konfigurieren
Client-COM-Portumleitung	Nicht zugelassen	Alle VDA-Versionen; bei VDA 7.x müssen Sie diese Einstellung in der Registrierung konfigurieren
Client-LPT-Portumleitung	Nicht zugelassen	Alle VDA-Versionen; bei VDA 7.x müssen Sie diese Einstellung in der Registrierung konfigurieren

ICA/Printing

Name	Standardeinstellung	VDA
Clientdruckerumleitung	Zugelassen	Alle VDA-Versionen
Standarddrucker	Hauptdrucker des Clients als Standarddrucker verwenden	Alle VDA-Versionen
Druckerzuweisungen	Der aktuelle Drucker des Benutzers wird als Standarddrucker in der Sitzung verwendet.	Alle VDA-Versionen
Ereignisprotokollpräferenz für die automatische Druckererstellung	Fehler und Warnungen protokollieren	Alle VDA-Versionen
Sitzungsdrucker	Keine Drucker angegeben	Alle VDA-

Name	Standardeinstellung	VDA Versionen
Warten bis Drucker erstellt sind (Desktop)	Deaktiviert	Alle VDA-Versionen

ICA/Drucken/Clientdrucker

Name	Standardeinstellung	VDA
Clientdrucker automatisch erstellen	Alle Clientdrucker automatisch erstellen	Alle VDA-Versionen
Generischen universellen Drucker automatisch erstellen	Deaktiviert	Alle VDA-Versionen
Clientdruckernamen	Standarddruckernamen	Alle VDA-Versionen
Direkte Verbindungen zu Druckservern	Aktiviert	Alle VDA-Versionen
Druckertreiberzuordnung und -kompatibilität	Keine Regeln angegeben	Alle VDA-Versionen
Speicherung von Druckereigenschaften	Im Profil speichern, wenn sie nicht auf dem Client gespeichert sind	Alle VDA-Versionen
Gespeicherte und wiederhergestellte Clientdrucker	Zugelassen	VDA 5, 5.5, 5.6 FP1

ICA/Printing/Drivers

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

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=False Zwischenspeichern von Bildern und Schriftarten • Zwischenspeichern eingebetteter Bilder zulassen=True • Zwischenspeichern eingebetteter Schriftarten zulassen=True Nicht-Administratoren können diese Einstellungen anpassen=False	Alle VDA-Versionen
Universelles Drucken - Vorschaueinstellung	Druckvorschau für automatisch erstellte oder generische universelle Drucker nicht verwenden	Alle VDA-Versionen
Universelles Drucken - Druckqualitätslimit	Kein Limit	Alle VDA-Versionen

ICA/Security

Name	Standardeinstellung	VDA
SecureICA-Mindestverschlüsselungsgrad	Standard	VDA für Server-OS 7 bis aktuelle Version

ICA/Serverlimits

Name	Standardeinstellung	VDA

Name	Standardeinstellung	VDA
Serverleerlauf-Zeitintervall	0 Millisekunden	VDA für Server-OS 7 bis aktuelle Version

ICA/Sitzungslimits

Name	Standardeinstellung	VDA
Timer für getrennte Sitzung	Deaktiviert	VDA 5, 5.5, 5.6 FP1, VDA für Desktop-OS 7 bis aktuelle Version
Getrennte Sitzungen - Timerintervall	1440 Minuten	VDA 5, 5.5, 5.6 FP1, VDA für Desktop-OS 7 bis aktuelle Version
Sitzungsverbindungstimer	Deaktiviert	VDA 5, 5.5, 5.6 FP1, VDA für Desktop-OS 7 bis aktuelle Version
Sitzungsverbindung - Timerintervall	1440 Minuten	VDA 5, 5.5, 5.6 FP1, VDA für Desktop-OS 7 bis aktuelle Version
Sitzungsleerlauftimer	Enabledf	VDA 5, 5.5, 5.6 FP1, VDA für Desktop-OS 7 bis aktuelle Version
Sitzungsleerlauf - Timerintervall	1440 Minuten	VDA 5, 5.5, 5.6 FP1, VDA für Desktop-OS 7 bis aktuelle Version

ICA/Sitzungszuverlässigkeit

Name	Standardeinstellung	VDA
Sitzungszuverlässigkeit - Verbindungen	Zugelassen	Alle VDA-Versionen
Sitzungszuverlässigkeit - Portnummer	2598	Alle VDA-Versionen
Sitzungszuverlässigkeit - Timeout	180 Sekunden	Alle VDA-Versionen

ICA/Zeitzonensteuerung

Name	Standardeinstellung	VDA
Lokale Zeitzone für Legacyclients schätzen	Aktiviert	VDA für Server-OS 7 bis aktuelle Version
Lokale Zeit des Clients verwenden	Serverzeitzone verwenden	Alle VDA-Versionen

ICA/TWAIN-Geräte

Name	Standardeinstellung	VDA

Name	Standardeinstellung	VDA
TWAIN-Geräteumleitung für Client	Zugelassen	VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
TWAIN-Komprimierungsgrad	Mittel	VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version

ICA/USB-Geräte

Name	Standardeinstellung	VDA
Regeln für die Client-USB-Geräteoptimierung	Keine Regeln angegeben	VDA 7.6 FP3 bis aktuelle Version
Client-USB-Geräteumleitung	Nicht zugelassen	Alle VDA-Versionen
Regeln für die Client-USB-Geräteumleitung	Keine Regeln angegeben	Alle VDA-Versionen
Client-USB-Geräteumleitung für Plug & Play-Geräte	Zugelassen	VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version

ICA/Visuelle Anzeige

Name	Standardeinstellung	VDA
Bevorzugte Farbtiefe für einfache Grafiken	24 Bit pro Pixel	VDA 7.6 FP3 bis aktuelle Version
Frameratesollwert	30 F/s	Alle VDA-Versionen
Bildqualität	Mittel	VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
Verwenden von Videocodec für die Komprimierung	Verwenden von Videocodec wenn verfügbar	VDA 7.6 FP3 bis aktuelle Version

ICA/Visuelle Anzeige/Bewegtbilder

Name	Standardeinstellung	VDA
Mindestbildqualität	Normal	VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version

Name	Standardeinstellung	VDA
Bewegtbildkomprimierung	Aktiviert	VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
Grad der progressiven Komprimierung	Keine	VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
Schwellenwert für progressive Komprimierung	2147483647 KBit/s	VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
Mindestframeratesollwert	10 F/s	VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version

ICA/Visuelle Anzeige/Festbilder

Name	Standardeinstellung	VDA
Zusätzliche Farbkomprimierung	Deaktiviert	Alle VDA-Versionen
Schwellenwert für zusätzliche Farbkomprimierung	8192 KBit/s	Alle VDA-Versionen
Heavyweight-Komprimierung	Deaktiviert	Alle VDA-Versionen
Grad der verlustreichen Komprimierung	Mittel	Alle VDA-Versionen
Schwellenwert für verlustreiche Komprimierung	2147483647 KBit/s	Alle VDA-Versionen

ICA/WebSockets

Name	Standardeinstellung	VDA
WebSockets-Verbindungen	Nicht zugelassen	VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
WebSockets-Portnummer	8008	VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
Vertrauenswürdige WebSockets-Ursprungsserverliste	Bei Verwendung des Platzhalters * wird allen Receiver für Web-URLs vertraut.	VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version

Load Management

Name	Standardeinstellung	VDA
Toleranzwert für gleichzeitige Anmeldungen	2	VDA für Server-OS 7 bis aktuelle Version

Name	Standardeinstellung	VDA
CPU-Nutzung	Deaktiviert	VDA für Server-OS 7 bis aktuelle Version
CPU-Nutzung ausschließlich Prozesspriorität	Unter normal oder niedrig	VDA für Server-OS 7 bis aktuelle Version
Datenträgernutzung	Deaktiviert	VDA für Server-OS 7 bis aktuelle Version
Sitzungshöchstanzahl	250	VDA für Server-OS 7 bis aktuelle Version
Speichernutzung	Deaktiviert	VDA für Server-OS 7 bis aktuelle Version
Speichernutzung - Ausgangslast	Nulllast: 768 MB	VDA für Server-OS 7 bis aktuelle Version

Profilverwaltung/Erweiterte Einstellungen

Name	Standardeinstellung	VDA
Automatische Konfiguration deaktivieren	Deaktiviert	Alle VDA-Versionen
Benutzer bei Problem abmelden	Deaktiviert	Alle VDA-Versionen
Anzahl Wiederholungen beim Zugriff auf gesperrte Dateien	5	Alle VDA-Versionen
Internet-Cookiedateien bei Abmeldung verarbeiten	Deaktiviert	Alle VDA-Versionen

Profilverwaltung/Grundeinstellungen

Name	Standardeinstellung	VDA
Aktiv zurückschreiben	Deaktiviert	Alle VDA-Versionen
Profilverwaltung aktivieren	Deaktiviert	Alle VDA-Versionen
Ausgeschlossene Gruppen	Deaktiviert: Mitglieder aller Benutzergruppen werden verarbeitet.	Alle VDA-Versionen
Unterstützung von Offlineprofilen	Deaktiviert	Alle VDA-Versionen
Pfad zum Benutzerspeicher	Windows	Alle VDA-Versionen
Anmeldungen lokaler Administratoren	Deaktiviert	Alle VDA-

Name	Standardeinstellung	VDA
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 plattformübergreifende Einstellungen	Deaktiviert	Alle VDA-Versionen

Profilverwaltung/Dateisystem/Ausschlüsse

Name	Standardeinstellung	VDA
Ausschlussliste - Verzeichnisse	Deaktiviert: Alle Ordner im Benutzerprofil werden synchronisiert.	Alle VDA-Versionen
Ausschlussliste - Dateien	Deaktiviert: Alle Dateien im Benutzerprofil werden synchronisiert.	Alle VDA-Versionen

Profilverwaltung/Dateisystem/Synchronisierung

Name	Standardeinstellung	VDA
Zu synchronisierende Verzeichnisse	Deaktiviert: Nur nicht ausgeschlossene Ordner werden synchronisiert.	Alle VDA-Versionen
Zu synchronisierende Dateien	Deaktiviert: Nur nicht ausgeschlossene Dateien werden synchronisiert.	Alle VDA-Versionen
Zu spiegelnde Ordner	Deaktiviert: Es werden keine Ordner gespiegelt.	Alle VDA-Versionen

Profilverwaltung/Ordnerumleitung

Name	Standardeinstellung	VDA
Administratorzugriff gewähren	Deaktiviert	Alle VDA-Versionen
Domänennamen einschließen	Deaktiviert	Alle VDA-Versionen

Profilverwaltung/Ordnerumleitung/AppData(Roaming)

Name	Standardeinstellung	VDA
AppData(Roaming)-Pfad	Deaktiviert: Kein Speicherort angegeben.	Alle VDA-Versionen
Umleitungseinstellungen für AppData(Roaming)	Inhalte werden zu dem in der Richtlinieneinstellung AppData(Roaming)-Pfad angegebenen UNC-Pfad umgeleitet.	Alle VDA-Versionen

Profilverwaltung/Ordnerumleitung/Kontakte

Name	Standardeinstellung	VDA
'Kontakte'-Pfad	Deaktiviert: Kein Speicherort angegeben.	Alle VDA-Versionen
Umleitungseinstellungen für 'Kontakte'	Inhalte werden zu dem in der Richtlinieneinstellung 'Kontakte'-Pfad angegebenen UNC-Pfad umgeleitet.	Alle VDA-Versionen

Profilverwaltung/Ordnerumleitung/Desktop

Name	Standardeinstellung	VDA
'Desktop'-Pfad	Deaktiviert: Kein Speicherort angegeben.	Alle VDA-Versionen
Umleitungseinstellungen für 'Desktop'	Inhalte werden zu dem in der Richtlinieneinstellung 'Desktop'-Pfad angegebenen UNC-Pfad umgeleitet.	Alle VDA-Versionen

Profilverwaltung/Ordnerumleitung/Dokumente

Name	Standardeinstellung	VDA
'Dokumente'-Pfad	Deaktiviert: Kein Speicherort angegeben.	Alle VDA-Versionen
Umleitungseinstellungen für 'Dokumente'	Inhalte werden zu dem in der Richtlinieneinstellung 'Dokumente'-Pfad angegebenen UNC-Pfad umgeleitet.	Alle VDA-Versionen

Profilverwaltung/Ordnerumleitung/Downloads

Name	Standardeinstellung	VDA
'Downloads'-Pfad	Deaktiviert: Kein Speicherort angegeben.	Alle VDA-Versionen
Umleitungseinstellungen für 'Downloads'	Inhalte werden zu dem in der Richtlinieneinstellung 'Downloads'-Pfad angegebenen UNC-Pfad umgeleitet.	Alle VDA-Versionen

Profilverwaltung/Ordnerumleitung/Favoriten

Name	Standardeinstellung	VDA
'Favoriten'-Pfad	Deaktiviert: Kein Speicherort angegeben.	Alle VDA-Versionen
Umleitungseinstellungen für 'Favoriten'	Inhalte werden zu dem in der Richtlinieneinstellung 'Favoriten'-Pfad angegebenen UNC-Pfad umgeleitet.	Alle VDA-Versionen

Profilverwaltung/Ordnerumleitung/Links

Name	Standardeinstellung	VDA
'Links'-Pfad	Deaktiviert: Kein Speicherort angegeben.	Alle VDA-Versionen
Umleitungseinstellungen für 'Links'	Inhalte werden zu dem in der Richtlinieneinstellung 'Links'-Pfad angegebenen UNC-Pfad umgeleitet.	Alle VDA-Versionen

Profilverwaltung/Ordnerumleitung/Musik

Name	Standardeinstellung	VDA
'Musik'-Pfad	Deaktiviert: Kein Speicherort angegeben.	Alle VDA-Versionen
Umleitungseinstellungen für 'Musik'	Inhalte werden zu dem in der Richtlinieneinstellung 'Musik'-Pfad angegebenen UNC-Pfad umgeleitet.	Alle VDA-Versionen

Profilverwaltung/Ordnerumleitung/Bilder

Name	Standardeinstellung	VDA
'Bilder'-Pfad	Deaktiviert: Kein Speicherort angegeben.	Alle VDA-Versionen
Umleitungseinstellungen für 'Bilder'	Inhalte werden zu dem in der Richtlinieneinstellung 'Bilder'-Pfad angegebenen UNC-Pfad umgeleitet.	Alle VDA-Versionen

Profilverwaltung/Ordnerumleitung/Gespeicherte Spiele

Name	Standardeinstellung	VDA
'Gespeicherte Spiele'-Pfad	Deaktiviert: Kein Speicherort angegeben.	Alle VDA-Versionen
Umleitungseinstellungen für 'Gespeicherte Spiele'	Inhalte werden zu dem in der Richtlinieneinstellung 'Gespeicherte Spiele'-Pfad angegebenen UNC-Pfad umgeleitet.	Alle VDA-Versionen

Profilverwaltung/Ordnerumleitung/Suchen

Name	Standardeinstellung	VDA
'Suchen'-Pfad	Deaktiviert: Kein Speicherort angegeben.	Alle VDA-Versionen
Umleitungseinstellungen für 'Suchen'	Inhalte werden zu dem in der Richtlinieneinstellung 'Suchen'-Pfad angegebenen UNC-Pfad umgeleitet.	Alle VDA-Versionen

Profilverwaltung/Ordnerumleitung/Startmenü

Name	Standardeinstellung	VDA
Startmenü-Pfad	Deaktiviert: Kein Speicherort angegeben.	Alle VDA-Versionen
Umleitungseinstellungen für 'Startmenü'	Inhalte werden zu dem in der Richtlinieneinstellung 'Startmenü'-Pfad angegebenen UNC-Pfad umgeleitet.	Alle VDA-Versionen

Profilverwaltung/Ordnerumleitung/Videos

Name	Standardeinstellung	VDA
'Videos'-Pfad	Deaktiviert: Kein Speicherort angegeben.	Alle VDA-Versionen
Umleitungseinstellungen für 'Videos'	Inhalte werden zu dem in der Richtlinieneinstellung 'Videos'-Pfad angegebenen UNC-Pfad umgeleitet.	Alle VDA-Versionen

Profilverwaltung/Protokolleinstellungen

Name	Standardeinstellung	VDA
Active Directory-Aktionen	Deaktiviert	Alle VDA-Versionen
Allgemeine Informationen	Deaktiviert	Alle VDA-Versionen

Name	Standardeinstellung	VDA
Allgemeine Warnungen	Deaktiviert	Alle VDA-Versionen
Protokollierung aktivieren	Deaktiviert	Alle VDA-Versionen
Dateisystemaktionen	Deaktiviert	Alle VDA-Versionen
Dateisystembenachrichtigungen	Deaktiviert	Alle VDA-Versionen
Abmeldung	Deaktiviert	Alle VDA-Versionen
Anmeldebildschirm	Deaktiviert	Alle VDA-Versionen
Max. Größe der Protokolldatei	1048576	Alle VDA-Versionen
Pfad zur Protokolldatei	Deaktiviert: Protokolldateien werden im Standardspeicherort gespeichert: %SystemRoot%\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-

Name	Standardeinstellung	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
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
Gruppen mit gestreamten Benutzerprofilen	Deaktiviert: Alle Benutzerprofile in einer Organisationseinheit werden normal verarbeitet.	Alle VDA-Versionen
Timeout für bevorstehende Sperrdateien (Tage)	1 Tag	Alle VDA-Versionen

Receiver

Name	Standardeinstellung	VDA
StoreFront-	Keine Stores	VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis

Name	Standardeinstellung	VDA
Kontenliste	angegeben.	aktuelle Version

Virtual Delivery Agent

Name	Standardeinstellung	VDA
IPv6-Netzwerkmaske für Controllerregistrierung	Keine Netzwerkmaske angegeben.	VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
Controllerregistrierungsport	80	Alle VDA-Versionen
Controller-SIDs	Keine SIDs angegeben	Alle VDA-Versionen
Controller	Keine Controller angegeben	Alle VDA-Versionen
Automatische Controllerupdates aktivieren	Aktiviert	VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
Nur IPv6-Controllerregistrierung verwenden	Deaktiviert	VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
Site-GUID	Kein GUID angegeben.	Alle VDA-Versionen

Virtuelle IP

Name	Standardeinstellung	VDA
Virtuelle IP - Loopbackunterstützung	Deaktiviert	VDA 7.6 bis aktuelle Version
Virtuelle IP - Programme für virtuelles Loopback	Keine	VDA 7.6 bis aktuelle Version

HDX 3D Pro

Name	Standardeinstellung	VDA
Verlustfrei aktivieren	Aktiviert	VDA 5.5, 5.6 FP1
HDX3DPro-Qualitätseinstellungen		VDA 5.5, 5.6 FP1

Referenz für Richtlinieneinstellungen

Feb 29, 2016

Richtlinien enthalten Einstellungen, die gelten, wenn die Richtlinie angewendet wird. Die Beschreibungen in diesem Abschnitt geben auch an, ob zusätzliche Einstellungen zum Aktivieren eines Features erforderlich sind oder ob Einstellungen sich ähnlich sind.

Kurzanleitung

Die folgenden Tabellen listen die Einstellungen auf, die Sie in einer Richtlinie konfigurieren können. In der linken Spalte finden Sie die Aufgaben, in der rechten die dazugehörigen Einstellungen.

Audio

Aufgabe	**Richtlinieneinstellung**
Steuern der Verwendung mehrerer Audiogeräte	Audio Plug & Play
Steuern, ob Audioeingaben vom Mikrofon auf dem Benutzergerät zulässig sind	Clientmikrofonumleitung
Steuern der Audioqualität auf dem Benutzergerät	Audioqualität
Steuern der Audiozuordnung für Lautsprecher am Benutzergerät	Clientaudioumleitung

Bandbreite für Benutzergeräte

Beschränken der Bandbreite	**Richtlinieneinstellung**
Clientaudiozuordnung	• Bandbreitenlimit für die Audioumleitung oder • Bandbreitenlimit für die Audioumleitung (Prozent)
Kopieren und Einfügen mit der lokalen Zwischenablage	• Bandbreitenlimit für Zwischenablagenumleitung 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-

Beschränken der Bandbreite	Richtlinieneinstellung
	Multimediabeschleunigung oder • Bandbreitenlimit für HDX MediaStream-Multimediabeschleunigung (Prozent)
Clientsitzung	Bandbreitenlimit für Sitzung insgesamt
Drucken	• Bandbreitenlimit für Druckerumleitung oder • Bandbreitenlimit für Druckerumleitung (Prozent)
TWAIN-Geräte (wie Kameras oder Scanner)	• Bandbreitenlimit für TWAIN-Geräteumleitung oder • Bandbreitenlimit für TWAIN-Geräteumleitung (Prozent)
USB-Geräte	• Bandbreitenlimit für Client-USB-Geräteumleitung oder • Bandbreitenlimit für Client-USB-Geräteumleitung (Prozent)

Umleitung von Clientlaufwerken und Benutzergeräten

Aufgabe	Richtlinieneinstellung
Steuern, ob Laufwerke des Benutzergeräts verbunden werden, wenn Benutzer sich am Server anmelden	Clientlaufwerke automatisch verbinden
Steuern der Datenübertragung mit Kopier- und Einfügeoperationen zwischen dem Server und der lokalen Zwischenablage	Clientzwischenablagenumleitung
Steuern der Laufwerkzuordnung des Benutzergeräts	Clientlaufwerkumleitung
Steuern, ob die lokalen Festplatten des Benutzers in einer Sitzung verfügbar sind	• Lokale Clientlaufwerke und • Clientlaufwerkumleitung
Steuern, ob die lokalen Diskettenlaufwerke des Benutzers in einer Sitzung verfügbar sind	• Clientdiskettenlaufwerke und • Clientlaufwerkumleitung
Steuern, ob die Netzlaufwerke des Benutzers in einer Sitzung verfügbar sind	• Clientnetzlaufwerke und • Clientlaufwerkumleitung

Aufgabe	Richtlinieneinstellung
Steuern, ob die lokalen CD-, DVD- oder Blu-ray-Laufwerke des Benutzers in einer Sitzung verfügbar sind	• Optische Clientlaufwerke und • Clientlaufwerkumleitung
Steuern, ob die lokalen Clientwechseldatenträger des Benutzers in einer Sitzung verfügbar sind	• Clientwechsellaufwerke und • Clientlaufwerkumleitung
Steuern, ob TWAIN-Geräte, wie Scanner und Kameras, in einer Sitzung verfügbar sind und Steuern der Komprimierung bei der Übertragung von Bilddaten	• TWAIN-Geräteumleitung für Client • TWAIN-Umleitung
Steuern, ob die USB-Geräte in einer Sitzung verfügbar sind	• Client-USB-Geräteumleitung und • Regeln für die Client-USB-Geräteumleitung
Geschwindigkeit beim Schreiben und Kopieren von Dateien auf einen Clientdatenträger über ein WAN erhöhen	Asynchrones Schreiben verwenden

Inhaltsumleitung

Aufgabe	Richtlinieneinstellung
Steuern der Verwendung der Inhaltsumleitung vom Server zum Benutzergerät	Host-zu-Client-Umleitung

Desktopbenutzeroberfläche

Aufgabe	Richtlinieneinstellung
Steuern, ob der Desktophintergrund in Benutzersitzungen angezeigt wird	Desktophintergrund
Anzeigen des Fensterinhalts beim Verschieben des Fensters	Fensterinhalt beim Verschieben anzeigen

Grafiken & Multimedia

Aufgabe	Richtlinieneinstellung
Steuern der maximalen Anzahl von Frames pro Sekunde, die an Benutzergeräte von virtuellen Desktops gesendet werden	Frameratesollwert

Aufgabe	Richtlinieneinstellung
Steuern der visuellen Qualität der auf dem Benutzergerät angezeigten Bilder	Bildqualität
Steuern, ob Flash-Inhalte in Sitzungen wiedergegeben werden	Flash-Standardverhalten
Steuern, ob Flash-Inhalte auf Websites in Sitzungen angezeigt werden	• URL-Liste für serverseitigen Flash-Inhaltsabruf • Flash-URL-Kompatibilitätsliste • Einstellung der Richtlinie zum Verhindern von Videofallback • Fehler beim Verhindern von Flash-Videofallback *.swf

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	• Clientdrucker automatisch erstellen und • Clientdruckerumleitung
Steuern des Speicherorts für die Druckereigenschaften	Speicherung von Druckereigenschaften
Steuern, ob Druckanfragen vom Client oder vom Server verarbeitet werden	Direkte Verbindungen zu Druckservern
Steuern, ob Benutzer auf Drucker zugreifen können, die an die Benutzergeräte angeschlossen sind	Clientdruckerumleitung
Steuern, ob bei der automatischen Erstellung von Client- und Netzwerkdruckern native Windows-Treiber installiert werden	Automatische Installation von mitgelieferten Druckertreibern

Aufgabe	Richtlinieneinstellung
Steuern, wann der universelle Druckertreiber verwendet wird	Verwendung universeller Druckertreiber
Wählen des Druckers anhand von Sitzungsinformationen eines mobilen Benutzers	Standarddrucker

Hinweis: Richtlinien können nicht zum Aktivieren eines Bildschirmschoners in einer Desktop- oder Anwendungssitzung verwendet werden. Wenn Benutzer einen Bildschirmschoner benötigen, muss dieser auf dem Benutzergerät eingerichtet werden.

Einstellungen der Richtlinie "ICA"

Feb 29, 2016

Der Abschnitt "ICA" enthält Richtlinieneinstellungen für ICA-Listenerverbindungen und die Zwischenablagenzuordnung.

Clientzwischenablagenumleitung

Mit dieser Einstellung legen Sie fest, ob die Zwischenablage auf dem Clientgerät der Zwischenablage auf dem Server zugeordnet wird.

Standardmäßig ist die Umleitung der Zwischenablage zugelassen.

Wenn Sie verhindern möchten, dass Daten durch Kopieren und Einfügen über die Zwischenablage zwischen einer Sitzung und der lokalen Zwischenablage übertragen werden, wählen Sie Nicht zugelassen. Benutzer können weiterhin die Zwischenablage für das Kopieren von Daten zwischen Anwendungen einsetzen, die in Sitzungen ausgeführt werden.

Nachdem diese Einstellung zugelassen wurde, konfigurieren Sie die maximal zulässige Bandbreite, die die Zwischenablage in einer Clientverbindung verbrauchen darf. Verwenden Sie dazu die Einstellung Bandbreitenlimit für Zwischenablagenumleitung oder Bandbreitenlimit für Zwischenablagenumleitung (Prozent).

Zum Schreiben in Clientzwischenablage zugelassene Formate

Wenn die Einstellung Schreiben in Clientzwischenablage einschränken aktiviert ist, können Hostzwischenablagedaten nicht für den Clientendpunkt freigegeben werden. Mit dieser Einstellung können jedoch 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

Die folgenden benutzerdefinierten Formate sind in XenApp und XenDesktop vordefiniert:
- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8

Zusätzliche benutzerdefinierte Formate können hinzugefügt werden. Der Name des benutzerdefinierten Formats muss mit den Formaten übereinstimmen, die mit dem System registriert werden. Bei Formatnamen muss die Groß- und Kleinschreibung beachtet werden.

Diese Einstellung wird nicht angewendet, wenn Clientzwischenablagenumleitung oder Schreiben in Clientzwischenablage einschränken auf "Nicht zugelassen" festgelegt sind.

Desktop starten

Mit dieser Einstellung legen Sie fest, ob Benutzer ohne Administratorrechte, die in der Gruppe der Benutzer mit direktem Zugriff eines VDAs sind, über eine ICA-Verbindung eine Verbindung zu einer Sitzung auf dem VDA herstellen können.

Standardmäßig können Benutzer ohne Administratorrechte keine Verbindung zu diesen Sitzungen herstellen.

Diese Einstellung hat keine Auswirkungen auf Benutzer ohne Administratorrechte, die in der Gruppe der Benutzer mit direktem Zugriff eines VDAs sind und eine RDP-Verbindung verwenden. Diese Benutzer können eine Verbindung zum VDA herstellen, unabhängig davon, ob diese Einstellung aktiviert ist. Diese Einstellung hat keine Auswirkungen auf Benutzer ohne Administratorrechte, die nicht in der Gruppe der Benutzer mit direktem Zugriff eines VDAs sind. Diese Benutzer können unabhängig vom Status dieser Einstellung keine Verbindung zum VDA herstellen.

ICA-Listener - Verbindungstimeout

Hinweis: Diese Einstellung gilt nur für Virtual Delivery Agents 5.0, 5.5 und 5.6 Feature Pack 1.

Mit dieser Einstellung geben Sie die maximale Wartezeit an, bis eine Verbindung mit dem ICA-Protokoll abgeschlossen wird.

Standardmäßig ist die maximale Wartezeit 120000 Millisekunden oder zwei Minuten.

ICA-Listenerportnummer

Mit dieser Einstellung konfigurieren Sie die TCP/IP-Portnummer, die vom ICA-Protokoll auf dem Server verwendet wird.

Die Standardeinstellung der Portnummer ist "1494".

Gültige Portnummern müssen zwischen 0 und 65535 liegen. Sie dürfen keinen Konflikt mit anderen gängigen Portnummern verursachen. Wenn Sie die Portnummer ändern, muss der Server neu gestartet werden, damit der neue Wert wirksam werden kann. Wenn Sie die Portnummer auf dem Server ändern, müssen Sie sie auch in jedem Citrix Receiver oder Plug-In ändern, das eine Verbindung zu diesem Server herstellt.

Starten nicht-veröffentlichter Programme bei Clientverbindung

Mit dieser Einstellung geben Sie an, ob Startanwendungen über RDP auf dem Server gestartet werden.

Standardmäßig ist das Starten von Startanwendungen über RDP auf dem Server nicht zulässig.

Schreiben in Clientzwischenablage einschränken

Wenn diese Einstellung zugelassen ist, können Hostzwischenablagedaten nicht für den Clientendpunkt freigegeben werden. Durch Aktivieren der Einstellung Zum Schreiben in Clientzwischenablage zugelassene Formate können Sie bestimmte Formate zulassen.

Die Standardeinstellung ist "Nicht zugelassen".

Schreiben in Sitzungszwischenablage einschränken

Wenn diese Einstellung zugelassen ist, können Clientzwischenablagedaten nicht für die Benutzersitzung freigegeben werden. Durch Aktivieren der Einstellung Zum Schreiben in Sitzungszwischenablage zugelassene Formate können Sie bestimmte Formate zulassen.

Die Standardeinstellung ist "Nicht zugelassen".

Zum Schreiben in Sitzungszwischenablage zugelassene Formate

Wenn die Einstellung Schreiben in Sitzungszwischenablage einschränken aktiviert ist, können Clientzwischenablagedaten nicht für Sitzungsanwendungen freigegeben werden. Mit dieser Einstellung können jedoch bestimmte Datenformate für die Sitzungszwischenablage freigegeben werden.

Die folgenden Zwischenablageformate sind vom System definiert:

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE

Die folgenden benutzerdefinierten Formate sind in XenApp und XenDesktop vordefiniert:

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8

Zusätzliche benutzerdefinierte Formate können hinzugefügt werden. Der Name des benutzerdefinierten Formats muss mit den Formaten übereinstimmen, die mit dem System registriert werden. Bei Formatnamen muss die Groß- und Kleinschreibung beachtet werden.

Diese Einstellung wird nicht angewendet, wenn die Einstellung Clientzwischenablagenumleitung oder Schreiben in Sitzungszwischenablage einschränken auf "Nicht zugelassen" festgelegt sind.

Einstellungen der Richtlinie "Automatische Wiederverbindung von Clients"

Feb 29, 2016

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.

Standardmäßig ist die automatische Wiederverbindung zugelassen.

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.

Bei der automatischen Wiederverbindung kann es aber dazu kommen, dass eine neue Sitzung gestartet wird (statt die Verbindung mit der bestehenden Sitzung wiederherzustellen), wenn das Citrix Receiver-Cookie, das den Schlüssel für Sitzungs-ID und Anmeldeinformationen enthält, nicht verwendet wird. Das Cookie wird nicht verwendet, wenn es abgelaufen ist, z. B. weil die Wiederverbindung verzögert wird, oder wenn die Anmeldeinformationen neu eingegeben werden müssen. Die automatische Wiederverbindung von Clients wird nicht ausgelöst, wenn Benutzer die Sitzung absichtlich trennen.

Wenn die automatische Wiederverbindung zugelassen ist, versucht Citrix Receiver bei Anwendungssitzungen, die Verbindung mit der Sitzung wiederherzustellen, bis die Wiederverbindung erfolgreich war oder der Benutzer die Wiederverbindung abbricht.

Wenn die automatische Wiederverbindung zugelassen ist, versucht Citrix Receiver bei Desktopsitzungen eine festgelegte Zeit lang, die Verbindung mit der Sitzung wiederherzustellen, bis die Wiederverbindung erfolgreich war oder der Benutzer die Wiederverbindung abbricht. Der Standardwert für diese Zeit ist fünf Minuten. Um die Zeit zu ändern, bearbeiten Sie die Registrierung auf dem Benutzergerät:

HKLM\Software\Citrix\ICA Client\TransportReconnectRetryMaxTimeSeconds; DWORD;<seconds>
wobei <Sekunden> die Zeit in Sekunden ist, nach deren Ablauf keine weiteren Versuche der Sitzungswiederherstellung erfolgen.

Authentifizierung bei automatischer Wiederverbindung von Clients

Mit dieser Einstellung ist die Authentifizierung erforderlich, wenn die Verbindung zum Client automatisch wiederhergestellt wird.

Standardmäßig ist die Authentifizierung nicht erforderlich.

Wenn sich ein Benutzer erstmals anmeldet, werden seine Anmeldeinformationen verschlüsselt und gespeichert und es wird ein Cookie mit dem Schlüssel erstellt und an Citrix Receiver gesendet. Wenn diese Einstellung konfiguriert ist, werden keine Cookies verwendet. Stattdessen wird ein Dialogfeld mit der Aufforderung zur Eingabe der Anmeldeinformationen angezeigt, wenn Citrix Receiver versucht, die Verbindung automatisch wiederherzustellen.

Protokollierung der automatischen Wiederverbindung von Clients

Mit dieser Einstellung legen Sie fest, ob die automatischen Wiederverbindungen im Ereignisprotokoll aufgezeichnet werden.

Standardmäßig ist die Protokollierung deaktiviert.

Wenn die Protokollierung aktiviert ist, werden Informationen über erfolgreiche und fehlgeschlagene Wiederverbindungsereignisse im Systemprotokoll des Servers aufgezeichnet. Eine Site stellt kein kombiniertes Protokoll zu Wiederverbindungsereignissen auf allen Servern zur Verfügung.

Einstellungen der Richtlinie "Audio"

Feb 29, 2016

Der Abschnitt "Audio" enthält Richtlinieneinstellungen, mit denen Sie das Senden und Empfangen von Audiodaten auf dem Benutzergerät konfigurieren können, ohne dass es dabei zu einer unerwünschten Verschlechterung der Leistung kommt.

Audio über UDP - Real-time Transport

Diese Einstellung aktiviert bzw. deaktiviert die Audioübertragung und den Audioempfang zwischen VDA und Benutzergeräten über RTP mit UDP (User Datagram Protocol). Wenn diese Einstellung deaktiviert ist, wird Audio über TCP gesendet und empfangen.

Standardmäßig ist Audio über UDP zugelassen.

Audio Plug & Play

Mit dieser Einstellung lassen Sie die Verwendung mehrerer Audiogeräte zum Aufzeichnen und zum Wiedergeben von Ton zu oder verhindern sie.

Standardmäßig ist die Verwendung mehrerer Audiogeräte zulässig.

Diese Einstellung gilt nur für Windows-Serverbetriebssystemmaschinen.

Audioqualität

Mit dieser Einstellung legen Sie die Tonqualität fest, die in Benutzersitzungen empfangen wird.

In der Standardeinstellung ist die Tonqualität auf Hoch - High Definition-Audio eingestellt.

Um die Tonqualität zu steuern, wählen Sie eine der folgenden Optionen:

- Wählen Sie Gering - für langsame Verbindungen für Verbindungen mit geringer Bandbreite. An das Benutzergerät gesendete Audiodaten werden bis auf 16 KBit/s komprimiert. Diese Komprimierung führt zu einer erheblichen Verringerung der Tonqualität, ermöglicht aber eine akzeptable Leistung bei einer Verbindung mit geringer Bandbreite.
- Wählen Sie Mittel - für Sprache optimiert, um VoIP-Anwendungen oder Medienanwendungen bei schwierigen Netzwerkverbindungen mit Leitungen unter 512 KBit/s oder bei erheblicher Überlastung und Paketverlust bereitzustellen. Dieses Codec bietet eine schnelle Codierung und ist daher ideal für Softphones und Unified Communications-Anwendungen geeignet, wenn Sie eine serverseitige Medienverarbeitung benötigen.
  Die an das Benutzergerät gesendeten Audiodaten werden bis auf 64 KBit/s komprimiert; diese Komprimierung führt zu einer moderaten Verringerung der Tonqualität auf dem Benutzergerät mit niedriger Latenz und geringem Bandbreitenverbrauch. Wenn die Einstellung eine unbefriedigende VoIP-Qualität liefert, stellen Sie sicher, dass die Richtlinie Audio über UDP - Real-time Transport auf Zugelassen eingestellt ist.
- Wählen Sie Hoch - High Definition Audio für Verbindungen, bei denen die Bandbreite keine Rolle spielt und bei denen die Tonqualität wichtig ist. Clients können Audiodaten mit der nativen Abspielrate wiedergeben. Audiodaten werden mit einer hohen Qualitätsstufe bei Erhaltung der CD-Qualität komprimiert, die bis zu 112 KBit/s Bandbreite benötigt. Die Übertragung dieser Datenmenge kann zu einer höheren CPU-Belastung und Engpässen im Netzwerk führen.

Die Bandbreite wird nur verbraucht, während Audio aufgenommen oder abgespielt wird. Wenn beides gleichzeitig stattfindet, verdoppelt sich der Bandbreitenverbrauch.

Konfigurieren Sie die Einstellungen Bandbreitenlimit für die Audioumleitung oder Bandbreitenlimit für die Audioumleitung

(Prozent), um die maximale Bandbreite anzugeben.

Clientaudioumleitung

Mit dieser Einstellung legen Sie fest, ob auf dem Server gehostete Anwendungen Audiodateien über ein auf dem Benutzergerät installiertes Audiogerät wiedergeben können. Diese Einstellung gibt auch an, ob Benutzer Audio aufzeichnen können.

Standardmäßig ist die Audioumleitung zugelassen.

Nachdem Sie diese Einstellung zugelassen haben, können Sie die Bandbreite beschränken, die durch die Wiedergabe oder das Aufzeichnen von Audio verbraucht wird. Durch Beschränken der Bandbreite, die durch Audio verbraucht wird, kann sich die Anwendungsleistung steigern, die Audioqualität wird aber herabgesetzt. Die Bandbreite wird nur verbraucht, während Audio aufgenommen oder abgespielt wird. Wenn beides gleichzeitig stattfindet, verdoppelt sich der Bandbreitenverbrauch. Konfigurieren Sie die Einstellungen Bandbreitenlimit für die Audioumleitung oder Bandbreitenlimit für die Audioumleitung (Prozent), um die maximale Bandbreite anzugeben.

Auf Windows-Serverbetriebssystemmaschinen müssen Sie sicherstellen, dass für Audio Plug & Play die Unterstützung mehrerer Audiogeräte aktiviert ist.

Wichtig: Wenn die Clientaudioumleitung nicht zugelassen ist, sind alle HDX-Audiofunktionen deaktiviert.

Clientmikrofonumleitung

Mit dieser Einstellung aktivieren oder deaktivieren Sie die Umleitung von Clientmikrofonen. Wenn aktiviert, können Benutzer Mikrofone für die Aufnahme von Audioeingaben in einer Sitzung verwenden.

Standardmäßig ist die Clientmikrofonumleitung zugelassen.

Aus Sicherheitsgründen werden Benutzer darauf hingewiesen, wenn Server, die keine vertrauenswürdige Beziehung zu den Geräten haben, auf Mikrofone zugreifen. Benutzer können den Zugriff ermöglichen oder ablehnen. Benutzer können die Warnung in Citrix Receiver deaktivieren.

Auf Windows-Serverbetriebssystemmaschinen müssen Sie sicherstellen, dass für Audio Plug & Play die Unterstützung mehrerer Audiogeräte aktiviert ist.

Wenn die Einstellung Clientaudioumleitung auf dem Benutzergerät deaktiviert ist, hat diese Regel keine Auswirkung.

Einstellungen der Richtlinie "Bandbreite"

Feb 29, 2016

Der Abschnitt "Bandbreite" enthält Richtlinieneinstellungen, mit denen Sie Leistungsprobleme vermeiden können, die sich aus der Bandbreitenverwendung in der Clientsitzung ergeben.

Wichtig: Die Verwendung dieser Richtlinieneinstellungen mit den Richtlinieneinstellungen Multistream kann zu unerwarteten Ergebnissen führen. Wenn Sie Multistreameinstellungen in einer Richtlinie verwenden, stellen Sie sicher, dass diese Richtlinieneinstellungen für das Bandbreitenlimit nicht eingeschlossen sind.

Bandbreitenlimit für die Audioumleitung

Mit dieser Einstellung geben Sie die maximal zulässige Bandbreite für die Wiedergabe oder die Aufnahme von Audio in einer Benutzersitzung in Kilobits pro Sekunde an.

Standardmäßig ist kein Maximalwert (Null) angegeben.

Wenn Sie für diese Einstellung und für die Einstellung Bandbreitenlimit für die Audioumleitung (Prozent) einen Wert angeben, wird die restriktivere Einstellung angewendet.

Bandbreitenlimit für die Audioumleitung (Prozent)

Mit dieser Einstellung geben Sie das maximal zulässige Bandbreitenlimit für die Wiedergabe oder die Aufnahme von Audio in als Prozentsatz der Gesamtsitzungsbandbreite an.

Standardmäßig ist kein Maximalwert (Null) angegeben.

Wenn Sie für diese Einstellung und für die Einstellung Bandbreitenlimit für die Audioumleitung einen Wert angeben, wird die restriktivere Einstellung angewendet.

Wenn Sie die Einstellung konfigurieren, müssen Sie auch die Einstellung Bandbreitenlimit für Sitzung insgesamt konfigurieren, mit der die Gesamtbandbreite definiert wird, die für Clientsitzungen verfügbar ist.

Bandbreitenlimit für Client-USB-Geräteumleitung

Mit dieser Einstellung geben Sie die maximal zulässige Bandbreite für die Umleitung von USB-Geräten zum und vom Client in Kilobit pro Sekunde an.

Standardmäßig ist kein Maximalwert (Null) angegeben.

Wenn Sie für diese Einstellung und für die Einstellung Bandbreitenlimit für Client-USB-Geräteumleitung (Prozent) einen Wert angeben, wird die restriktivere Einstellung angewendet.

Bandbreitenlimit für Client-USB-Geräteumleitung (Prozent)

Mit dieser Einstellung geben Sie die maximal zulässige Bandbreite für die Umleitung von USB-Geräten zum und vom Client als Prozentsatz der Gesamtsitzungsbandbreite an.

Standardmäßig ist kein Maximalwert (Null) angegeben.

Wenn Sie für diese Einstellung und für die Einstellung Bandbreitenlimit für Client-USB-Geräteumleitung einen Wert angeben, wird die restriktivere Einstellung angewendet.

Wenn Sie die Einstellung konfigurieren, müssen Sie auch die Einstellung Bandbreitenlimit für Sitzung insgesamt konfigurieren,

mit der die Gesamtbandbreite definiert wird, die für Clientsitzungen verfügbar ist.

Bandbreitenlimit für Zwischenablagenumleitung

Mit dieser Einstellung geben Sie die maximal zulässige Bandbreite in Kilobits pro Sekunde für Datenübertragungen zwischen einer Sitzung und der lokalen Zwischenablage an.

Standardmäßig ist kein Maximalwert (Null) angegeben.

Wenn Sie für diese Einstellung und für die Einstellung Bandbreitenlimit für Zwischenablagenumleitung (Prozent) einen Wert angeben, wird die restriktivere Einstellung angewendet.

Bandbreitenlimit für Zwischenablagenumleitung (Prozent)

Mit dieser Einstellung geben Sie die maximal zulässige Bandbreite für Datenübertragungen zwischen einer Sitzung und der lokalen Zwischenablage als Prozentsatz der Gesamtsitzungsbandbreite an.

Standardmäßig ist kein Maximalwert (Null) angegeben.

Wenn Sie für diese Einstellung und für die Einstellung Bandbreitenlimit für Zwischenablagenumleitung einen Wert angeben, wird die restriktivere Einstellung angewendet.

Wenn Sie die Einstellung konfigurieren, müssen Sie auch die Einstellung Bandbreitenlimit für Sitzung insgesamt konfigurieren, mit der die Gesamtbandbreite definiert wird, die für Clientsitzungen verfügbar ist.

Bandbreitenlimit für COM-Portumleitung

Hinweis: Konfigurieren Sie bei Virtual Delivery Agent 7.x 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 LPT-Portumleitung (Prozent) einen Wert angeben, wird die restriktivere Einstellung angewendet.

Bandbreitenlimit für COM-Portumleitung (Prozent)

Hinweis: Konfigurieren Sie bei Virtual Delivery Agent 7.x 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 auch für die Einstellung Bandbreitenlimit für LPT-Portumleitung einen Wert angeben, wird die restriktivere Einstellung angewendet.

Wenn Sie die Einstellung konfigurieren, müssen Sie auch die Einstellung Bandbreitenlimit für Sitzung insgesamt konfigurieren, mit der die Gesamtbandbreite definiert wird, die für Clientsitzungen verfügbar ist.

Bandbreitenlimit für Dateiumleitung

Mit dieser Einstellung geben Sie die maximal zulässige Bandbreite für den Zugriff auf Clientlaufwerke in einer Clientverbindung in Kilobits pro Sekunde an.

Standardmäßig ist kein Maximalwert (Null) angegeben.

Wenn Sie für diese Einstellung und für die Einstellung Bandbreitenlimit für Dateiumleitung (Prozent) einen Wert angeben, wird die restriktivere Einstellung (mit dem niedrigeren Wert) angewendet.

Bandbreitenlimit für Dateiumleitung (Prozent)

Mit dieser Einstellung geben Sie das maximal zulässige Bandbreitenlimit für den Zugriff auf Clientlaufwerke als Prozentsatz der Gesamtsitzungsbandbreite an

Standardmäßig ist kein Maximalwert (Null) angegeben.

Wenn Sie für diese Einstellung und für die Einstellung Bandbreitenlimit für Dateiumleitung einen Wert angeben, wird die restriktivere Einstellung angewendet.

Wenn Sie die Einstellung konfigurieren, müssen Sie auch die Einstellung Bandbreitenlimit für Sitzung insgesamt konfigurieren, mit der die Gesamtbandbreite definiert wird, die für Clientsitzungen verfügbar ist.

Bandbreitenlimit für HDX MediaStream-Multimediabeschleunigung

Mit dieser Einstellung geben Sie die maximal zulässige Bandbreite für die Bereitstellung von Streamingaudio und -video mit HDX MediaStream-Multimediabeschleunigung in Kilobit pro Sekunde an.

Standardmäßig ist kein Maximalwert (Null) angegeben.

Wenn Sie für diese Einstellung und für die Einstellung Bandbreitenlimit für HDX MediaStream-Multimediabeschleunigung (Prozent) einen Wert angeben, wird die restriktivere Einstellung angewendet.

Bandbreitenlimit für HDX MediaStream-Multimediabeschleunigung (Prozent)

Mit dieser Einstellung geben Sie die maximal zulässige Bandbreite für die Bereitstellung von Streamingaudio und -video mit HDX MediaStream-Multimediabeschleunigung als Prozentsatz der Gesamtsitzungsbandbreite an.

Standardmäßig ist kein Maximalwert (Null) angegeben.

Wenn Sie für diese Einstellung einen Wert angeben und auch für die Einstellung "Bandbreitenlimit für HDX MediaStream-Multimediabeschleunigung", wird die restriktivere Einstellung angewendet.

Wenn Sie die Einstellung konfigurieren, müssen Sie auch die Einstellung Bandbreitenlimit für Sitzung insgesamt konfigurieren, mit der die Gesamtbandbreite definiert wird, die für Clientsitzungen verfügbar ist.

Bandbreitenlimit für LPT-Portumleitung

Hinweis: Konfigurieren Sie bei Virtual Delivery Agent 7.x diese Einstellung über die Registrierung (siehe Konfigurieren von COM-Port- und LPT-Portumleitungseinstellungen in der Registrierung).
Mit dieser Einstellung geben Sie die maximal zulässige Bandbreite in Kilobits pro Sekunde an, die für Druckaufträge über den LPT-Port in einer Benutzersitzung verwendet werden kann.

Standardmäßig ist kein Maximalwert (Null) angegeben.

Wenn Sie für diese Einstellung und für die Einstellung Bandbreitenlimit für COM-Portumleitung (Prozent) einen Wert angeben, wird die restriktivere Einstellung angewendet.

Bandbreitenlimit für LPT-Portumleitung (Prozent)

Hinweis: Konfigurieren Sie bei Virtual Delivery Agent 7.x 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 COM-Portumleitung einen Wert angeben, wird die restriktivere Einstellung angewendet.

Wenn Sie die Einstellung konfigurieren, müssen Sie auch die Einstellung Bandbreitenlimit für Sitzung insgesamt konfigurieren, mit der die Gesamtbandbreite definiert wird, die für Clientsitzungen verfügbar ist.

Bandbreitenlimit für Sitzung insgesamt

Mit dieser Einstellung geben Sie Gesamtbandbreite in Kilobits pro Sekunde an, die für Benutzersitzungen verwendet werden kann.

Die maximal erzwingbare Bandbreitenbeschränkung ist 10 MBit/s (10.000 KBit/s). Standardmäßig ist kein Maximalwert (Null) angegeben.

Durch Beschränken der Bandbreite, die von einer Clientverbindung verbraucht wird, kann zu einer Leistungsverbesserung führen, wenn andere Anwendungen außerhalb der Clientverbindung auch auf die Bandbreite zugreifen.

Bandbreitenlimit für Druckerumleitung

Mit dieser Einstellung geben Sie die maximal zulässige Bandbreite für den Zugriff auf Clientdrucker in einer Benutzersitzung in Kilobits pro Sekunde an.

Standardmäßig ist kein Maximalwert (Null) angegeben.

Wenn Sie für diese Einstellung und für die Einstellung Bandbreitenlimit für Druckerumleitung (Prozent) einen Wert angeben, wird die restriktivere Einstellung angewendet.

Bandbreitenlimit für Druckerumleitung (Prozent)

Mit dieser Einstellung geben Sie die maximal zulässige Bandbreite für den Zugriff auf Clientdrucker als Prozentsatz der Gesamtsitzungsbandbreite an.

Standardmäßig ist kein Maximalwert (Null) angegeben.

Wenn Sie für diese Einstellung und für die Einstellung Bandbreitenlimit für Druckerumleitung einen Wert angeben, wird die restriktivere Einstellung angewendet.

Wenn Sie die Einstellung konfigurieren, müssen Sie auch die Einstellung Bandbreitenlimit für Sitzung insgesamt konfigurieren, mit der die Gesamtbandbreite definiert wird, die für Clientsitzungen verfügbar ist.

Bandbreitenlimit für TWAIN-Geräteumleitung

Mit dieser Einstellung geben Sie die maximal zulässige Bandbreite in Kilobits pro Sekunde für die Steuerung von TWAIN-Bildverarbeitungsgeräten in veröffentlichten Anwendungen an.

Standardmäßig ist kein Maximalwert (Null) angegeben.

Wenn Sie für diese Einstellung und für die Einstellung Bandbreitenlimit für TWAIN-Geräteumleitung (Prozent) einen Wert

angeben, wird die restriktivere Einstellung angewendet.

Bandbreitenlimit für TWAIN-Geräteumleitung (Prozent)

Mit dieser Einstellung geben Sie die maximal zulässige Bandbreite für die Steuerung von TWAIN-Bildverarbeitungsgeräten in veröffentlichten Anwendungen als Prozentsatz der Gesamtsitzungsbandbreite an.

Standardmäßig ist kein Maximalwert (Null) angegeben.

Wenn Sie für diese Einstellung und für die Einstellung Bandbreitenlimit für TWAIN-Geräteumleitung einen Wert angeben, wird die restriktivere Einstellung angewendet.

Wenn Sie die Einstellung konfigurieren, müssen Sie auch die Einstellung Bandbreitenlimit für Sitzung insgesamt konfigurieren, mit der die Gesamtbandbreite definiert wird, die für Clientsitzungen verfügbar ist.

Einstellungen der Richtlinie "Clientsensoren"

Feb 29, 2016

Der Abschnitt "Clientsensoren" enthält Richtlinieneinstellungen, mit denen gesteuert wird, wie Informationen über den Mobilgerätsensor in einer Benutzersitzung gehandhabt werden.

Anwendungen können den physischen Standort des Clientgeräts verwenden

Diese Einstellung legt fest, ob Anwendungen, die in einer Sitzung auf einem Mobilgerät ausgeführt werden, den physischen Standort des Benutzergeräts verwenden können.

In der Standardeinstellung ist die Verwendung von Standortinformationen nicht zugelassen.

Wenn diese Einstellung nicht zugelassen ist und eine Anwendung versucht, die Standortinformationen abzurufen, wird ein Wert von "Zugriff verweigert" zurückgegeben.

Wenn diese Einstellung nicht zugelassen ist, kann ein Benutzer die Verwendung von Standortinformationen verhindern und eine Citrix Receiver-Anforderung für den Zugriff auf den Standort ablehnen. Android- und iOS-Geräte senden am Anfang jeder Sitzung eine Anforderung für die Standortinformationen.

Berücksichtigen Sie beim Entwickeln von gehosteten Anwendungen, die die Einstellung Anwendungen können den physischen Standort des Clientgeräts verwenden enthalten Folgendes:

- Eine standortaktivierte Anwendung sollte sich aus den folgenden Gründen nicht darauf verlassen, dass Standortinformationen verfügbar sind:
  - Ein Benutzer gewährt möglicherweise keinen Zugriff auf die Standortinformationen.
  - Der Standort ist ggf. nicht verfügbar oder ändert sich, währen die Anwendung ausgeführt wird.
  - Ein Benutzer stellt möglicherweise eine Verbindung mit der Anwendungssitzung von einem anderen Gerät her, das keine Standortinformationen unterstützt.
- Anforderungen für eine standortaktivierte Anwendung:
  - Das Standortfeature muss in der Standardeinstellung deaktiviert sein.
  - Eine Benutzeroption für das Zulassen oder Ablehnen des Features muss bei Ausführung der Anwendung verfügbar sein.
  - Eine Benutzeroption muss verfügbar sein, mit der von der Anwendung zwischengespeicherte Standortdaten gelöscht werden. (Citrix Receiver speichert keine Standortdaten im Cache.)
- Eine standortaktivierte Anwendung muss die Granularität der Standortinformationen verwalten, damit die abgefragten Daten dem Zweck der Anwendung entsprechen und die entsprechenden Gesetze einhalten.
- Bei der Verwendung der Standortdienste sollte eine sichere Verbindung (zum Beispiel mit TLS oder einem VPN) erzwungen werden. Citrix Receiver sollte eine Verbindung mit vertrauenswürdigen Servern herstellen.
- Sie sollten eine Rechtsberatung hinsichtlich der Verwendung von Standortdiensten erwägen.

Einstellungen der Richtlinie "Desktopbenutzeroberfläche"

Feb 29, 2016

Der Abschnitt "Desktopbenutzeroberfläche" enthält Richtlinieneinstellungen für visuelle Effekte, wie Desktophintergrund, Menüanimationen und das Verhalten von Fensterinhalten beim Drag & Drop, um die für Clientverbindungen verbrauchte Bandbreite zu steuern. Die Anwendungsleistung über ein WAN lässt sich durch Beschränken des Bandbreitenverbrauchs verbessern.

Desktopgestaltungsumleitung

Mit dieser Einstellung geben Sie an, ob die Verarbeitung des Grafikprozessors (GPU) oder des integrierten Grafikprozessors (IGP) auf dem Benutzergerät für die lokale DirectX-Grafikwiedergabe verwendet werden soll, um eine nahtlosere Windows-Desktopdarstellung zu erzielen. Wenn die Desktopgestaltungsumleitung aktiviert ist, wird eine hoch reaktionsfähige Windows-Benutzererfahrung bei Beibehaltung einer hohen Skalierbarkeit auf dem Server gewährleistet.

Standardmäßig ist die Desktopgestaltungsumleitung aktiviert.

Um die Desktopgestaltungsumleitung auszuschalten und die für Benutzersitzungen erforderliche Bandbreite zu reduzieren, wählen Sie Deaktiviert aus, wenn Sie diese Einstellung einer Richtlinie hinzufügen.

Grafikqualität Desktopgestaltung

Mit dieser Einstellung wird die Qualität der für die Desktopgestaltungsumleitung verwendeten Grafiken angegeben.

Die Standardeinstellung ist "Hoch".

Wählen Sie die Qualität Hoch, Mittel, Niedrig oder Verlustfrei aus.

Desktophintergrund

Mit dieser Einstellung legen Sie fest, ob Hintergründe in Benutzersitzungen angezeigt werden.

Standardmäßig kann der Desktophintergrund in Benutzersitzungen angezeigt werden.

Um den Desktophintergrund auszuschalten und die für Benutzersitzungen erforderliche Bandbreite zu reduzieren, wählen Sie die Einstellung Nicht zugelassen, wenn Sie diese Einstellung einer Richtlinie hinzufügen.

Menüanimation

Mit dieser Einstellung legen Sie fest, ob Menüanimation in Benutzersitzungen zugelassen oder verhindert wird.

Standardmäßig ist Menüanimation zugelassen.

Menüanimation ist eine Microsoft-Einstellung für erleichterte Bedienung. Ist die Einstellung aktiviert, werden Menüs nach einer kurzen Verzögerung durch Bildlauf- oder Einblendeffekt angezeigt. Unten im Menü wird ein Pfeil angezeigt. Das Menü wird eingeblendet, wenn Sie mit der Maus auf diesen Pfeil zeigen.

Menüanimation ist auf einem Desktop aktiviert, wenn diese Richtlinieneinstellung auf Zugelassen festgelegt ist und die Microsoft-Einstellung für Menüanimation aktiviert ist.

Hinweis: Änderungen an der Microsoft-Einstellung für Menüanimation sind Desktopänderungen. Dies bedeutet, dass einem Benutzer, der Menüanimation in einer Sitzung aktiviert hat, in späteren Sitzungen auf dem Desktop keine Menüanimation zur Verfügung steht, wenn die Desktopeinstellungen so festgelegt sind, dass am Desktop vorgenommene Änderungen nach dem Beenden der Sitzung verworfen werden. Aktivieren Sie daher für Benutzer, die Menüanimation benötigen, die Microsoft-Einstellung im Masterimage für den Desktop oder stellen Sie sicher, dass der Desktop vom Benutzer vorgenommene Änderungen beibehält.

Fensterinhalt beim Verschieben anzeigen

Mit dieser Einstellung legen Sie fest, ob Fensterinhalte beim Verschieben des Fensters auf dem Bildschirm angezeigt werden.

Standardmäßig ist die Anzeige des Fensterinhalts beim Verschieben zugelassen.

Wenn Zugelassen ausgewählt ist, wird beim Verschieben das ganze Fenster angezeigt. Wenn Nicht zugelassen ausgewählt ist, wird bis zum Ablegen nur der Fensterrahmen beim Verschieben angezeigt.

Einstellungen der Richtlinie "Endbenutzerüberwachung"

Feb 29, 2016

Der Abschnitt "Endbenutzerüberwachung" enthält Richtlinien zum Messen von Sitzungsnetzwerkverkehr.

ICA-Roundtripberechnung

Mit dieser Einstellung legen Sie fest, ob ICA-Roundtripberechnungen für aktive Verbindungen durchgeführt werden.

Standardmäßig sind die Berechnungen für aktive Verbindungen aktiviert.

Standardmäßig wird die Initiierung des ICA-Roundtripmessung verzögert, bis Netzwerkverkehr auf eine Benutzeraktion hinweist. Diese Verzögerung kann eine unbestimmte Länge haben und verhindert, dass die ICA-Roundtripmessung der einzige Grund für den ICA-Verkehr ist

Intervall für ICA-Roundtripberechnung

Mit dieser Einstellung geben Sie die Häufigkeit an, in Sekunden, mit der ICA-Roundtripberechnungen durchgeführt werden

Standardmäßig wird der ICA-Roundtrip alle 15 Sekunden berechnet.

ICA-Roundtrip für Verbindungen im Leerlauf berechnen

Mit dieser Einstellung legen Sie fest, ob ICA-Roundtripberechnungen für Verbindungen im Leerlauf durchgeführt werden.

Standardmäßig werden Berechnungen nicht für Verbindungen im Leerlauf durchgeführt.

Standardmäßig wird die Initiierung des ICA-Roundtripmessung verzögert, bis Netzwerkverkehr auf eine Benutzeraktion hinweist. Diese Verzögerung kann eine unbestimmte Länge haben und verhindert, dass die ICA-Roundtripmessung der einzige Grund für den ICA-Verkehr ist

Richtlinieneinstellung für Enhanced Desktop Experience

Feb 29, 2016

Durch die Richtlinieneinstellung "Enhanced Desktop Experience" werden Sitzungen auf Serverbetriebssystemen so konfiguriert, dass sie wie lokale Windows 7-Desktops aussehen, damit Benutzer in den Genuss einer verbesserten Desktopdarstellung kommen.

Standardmäßig ist diese Einstellung zugelassen.

Wenn ein Benutzerprofil mit dem Design "Windows – klassisch" bereits auf dem virtuellen Desktop vorhanden ist, wird durch Aktivieren dieser Richtlinie nicht die verbesserte Desktopdarstellung für diesen Benutzer bereitgestellt. Wenn sich ein Benutzer, dessen Benutzerprofil mit einem Windows 7-Design konfiguriert ist, bei einem virtuellen Desktop unter Windows Server 2012 anmeldet, für den diese Richtlinie deaktiviert oder nicht konfiguriert ist, wird eine Fehlermeldung angezeigt, die angibt, dass das Design nicht angewendet werden kann.

In beiden Fällen kann das Problem durch Zurücksetzen des Benutzerprofils gelöst werden.

Wenn die Richtlinie auf einem virtuellen Desktop mit aktiven Benutzersitzungen deaktiviert wird, sind Aussehen und Verhalten von Sitzungen nicht mit der Desktopdarstellung von Windows 7 und Windows - klassisch konsistent. Wenn Sie dies vermeiden möchten, starten Sie den virtuellen Desktop neu, nachdem Sie die Richtlinieneinstellung geändert haben. Sie müssen auch sämtliche Roamingprofile auf dem virtuellen Desktop löschen. Citrix empfiehlt außerdem, alle anderen Benutzerprofile auf dem virtuellen Desktop zu löschen, um Inkonsistenzen zwischen Profilen zu vermeiden.

Wenn Sie Roamingbenutzerprofile in der Umgebung verwenden, stellen Sie sicher, dass das Feature "Enhanced Desktop Experience" für alle virtuellen Desktops, die sich ein Profil teilen, entweder aktiviert oder deaktiviert ist.

Citrix rät davon ab, Roamingprofile zwischen virtuellen Desktops, auf denen Serverbetriebssysteme und Clientbetriebssysteme ausgeführt werden, freizugeben. Die Profile für Client- und Serverbetriebssysteme sind unterschiedlich und das Freigeben von Roamingprofilen zwischen beiden Systemtypen kann zu Inkonsistenzen in den Profileigenschaften führen, wenn ein Benutzer zwischen den Systemen wechselt.

Einstellungen der Richtlinie "Dateiumleitung"

Feb 29, 2016

Der Abschnitt "Dateiumleitung" enthält Richtlinieneinstellungen für die Clientlaufwerkzuordnung und die Clientlaufwerkoptimierung.

Clientlaufwerke automatisch verbinden

Mit dieser Einstellung legen Sie fest, ob die automatische Verbindung von Clientlaufwerken bei der Benutzeranmeldung zugelassen ist.

In der Standardeinstellung ist die automatische Verbindung zugelassen.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, müssen Sie die Einstellungen für die Laufwerktypen aktivieren, die automatisch verbunden werden. Konfigurieren Sie beispielsweise Optische Clientlaufwerke, damit CD-Laufwerke auf dem Clientgerät automatisch verbunden werden.

Die folgenden Richtlinieneinstellungen hängen zusammen:

- Clientlaufwerkumleitung
- Clientdiskettenlaufwerke
- Optische Clientlaufwerke
- Lokale Clientfestplattenlaufwerke
- Clientnetzlaufwerke
- Clientwechsellaufwerke

Clientlaufwerkumleitung

Mit dieser Einstellung aktivieren oder deaktivieren Sie die Dateiumleitung von und zu Laufwerken auf dem Benutzergerät.

In der Standardeinstellung ist die Dateiumleitung aktiviert.

Wenn aktiviert, können Benutzer ihre Dateien auf allen Clientlaufwerken speichern. Wenn deaktiviert, wird jegliche Dateiumleitung verhindert, unabhängig von den Dateiumleitungseinstellungen für einzelne Laufwerkstypen, z. B. Clientdiskettenlaufwerke und Clientnetzlaufwerke.

Die folgenden Richtlinieneinstellungen hängen zusammen:

- Clientdiskettenlaufwerke
- Optische Clientlaufwerke
- Lokale Clientfestplattenlaufwerke
- Clientnetzlaufwerke
- Clientwechsellaufwerke

Lokale Clientfestplattenlaufwerke

Mit dieser Einstellung legen Sie fest, ob Benutzer auf die lokalen Festplattenlaufwerke des Benutzergeräts zugreifen oder Dateien darauf speichern können.

In der Standardeinstellung ist der Zugriff auf lokale Festplattenlaufwerke zugelassen.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, müssen Sie auch für die Einstellung Clientlaufwerkumleitung die Option Zugelassen wählen. Wenn diese Einstellungen deaktiviert sind, können lokale Festplattenlaufwerke nicht

zugeordnet werden und Benutzer können auch nicht manuell auf diese Laufwerke zugreifen – unabhängig von der Einstellung für Lokale Festplattenlaufwerke.

Konfigurieren Sie außerdem die Einstellung Clientlaufwerke automatisch verbinden, damit lokale Festplattenlaufwerke automatisch verbunden werden.

Clientdiskettenlaufwerke

Mit dieser Einstellung legen Sie fest, ob Benutzer auf die Diskettenlaufwerke des Benutzergeräts zugreifen oder Dateien darauf speichern können.

In der Standardeinstellung ist der Zugriff auf Diskettenlaufwerke zugelassen.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, müssen Sie auch für die Einstellung Clientlaufwerkumleitung die Option Zugelassen wählen. Wenn diese Einstellungen deaktiviert sind, können Diskettenlaufwerke nicht zugeordnet werden und Benutzer können auch nicht manuell auf diese Laufwerke zugreifen – unabhängig von der Einstellung für Clientdiskettenlaufwerke.

Konfigurieren Sie außerdem die Einstellung Clientlaufwerke automatisch verbinden, damit Diskettenlaufwerke automatisch verbunden werden.

Clientnetzlaufwerke

Mit dieser Einstellung legen Sie fest, ob Benutzer auf die (remoten) Netzlaufwerke des Benutzergeräts zugreifen oder Dateien speichern können.

In der Standardeinstellung ist der Zugriff auf Netzlaufwerke zugelassen.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, müssen Sie auch für die Einstellung Clientlaufwerkumleitung die Option Zugelassen wählen. Wenn diese Einstellungen deaktiviert sind, können Netzlaufwerke nicht zugeordnet werden und Benutzer können auch nicht manuell auf diese Laufwerke zugreifen – unabhängig von der Einstellung für Clientnetzlaufwerke.

Konfigurieren Sie außerdem die Einstellung Clientlaufwerke automatisch verbinden, damit Netzlaufwerke automatisch verbunden werden.

Optische Clientlaufwerke

Mit dieser Einstellung legen Sie fest, ob Benutzer auf CD-, DVD- und BD-Laufwerke des Clientgeräts zugreifen oder Dateien dort speichern können.

In der Standardeinstellung ist der Zugriff auf optische Clientlaufwerke zugelassen.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, müssen Sie auch für die Einstellung Clientlaufwerkumleitung die Option Zugelassen wählen. Wenn diese Einstellungen deaktiviert sind, können optische Clientlaufwerke nicht zugeordnet werden und Benutzer können auch nicht manuell auf diese Laufwerke zugreifen – unabhängig von der Einstellung für Optische Clientlaufwerke.

Konfigurieren Sie außerdem die Einstellung Clientlaufwerke automatisch verbinden, damit optische Clientlaufwerke automatisch verbunden werden.

Clientwechsellaufwerke

Mit dieser Einstellung legen Sie fest, ob Benutzer auf die USB-Laufwerke des Benutzergeräts zugreifen oder Dateien speichern können.

In der Standardeinstellung ist der Zugriff auf Clientwechsellaufwerke zugelassen.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, müssen Sie auch für die Einstellung Clientlaufwerkumleitung die Option Zugelassen wählen. Wenn diese Einstellungen deaktiviert sind, können Clientwechsellaufwerke nicht zugeordnet werden und Benutzer können auch nicht manuell auf diese Laufwerke zugreifen – unabhängig von der Einstellung für Clientwechsellaufwerke.

Konfigurieren Sie außerdem die Einstellung Clientlaufwerke automatisch verbinden, damit Clientwechsellaufwerke automatisch verbunden werden.

Host-zu-Client-Umleitung

Mit dieser Einstellung aktivieren oder deaktivieren Sie Dateitypzuordnungen für URLs und manche Medieninhalte, damit sie auf dem Clientgerät geöffnet werden. Wenn deaktiviert, werden Inhalte auf dem Server geöffnet.

In der Standardeinstellung ist die Dateitypzuordnung deaktiviert.

Diese Art von URLs werden lokal geöffnet, wenn Sie die Einstellung aktivieren:
- Hypertext Transfer Protocol (HTTP)
- Secure Hypertext Transfer Protocol (HTTPS)
- Real Player und QuickTime (RTSP)
- Real Player und QuickTime (RTSPU)
- Ältere Real Player-URLs (PNM)
- Microsoft Media Server (MMS)

Clientlaufwerksbuchstaben erhalten

Mit dieser Einstellung aktivieren oder deaktivieren Sie, ob die Clientlaufwerksbuchstaben erhalten bleiben.

In der Standardeinstellung bleiben die Clientlaufwerksbuchstaben nicht erhalten.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, müssen Sie auch für die Einstellung Clientlaufwerkumleitung die Option Zugelassen wählen.

Schreibgeschützter Zugriff auf Clientlaufwerke

Diese Einstellung erlaubt oder verhindert, dass Benutzer und Anwendungen Dateien oder Ordner auf zugeordneten Clientlaufwerken erstellen oder ändern.

Standardmäßig können Dateien und Ordner auf zugeordneten Clientlaufwerken geändert werden.

Wenn die Einstellung auf Aktiviert gesetzt wird, ist Lesezugriff auf die Dateien und Verzeichnisse möglich.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, müssen Sie auch für die Einstellung Clientlaufwerkumleitung die Option Zugelassen wählen.

Umleitung spezieller Ordner

Mit dieser Einstellung legen Sie fest, ob Benutzer von Citrix Receiver und dem Webinterface ihre lokalen speziellen Ordner in einer Sitzung sehen, z. B. "Dokumente" und "Desktop".

In der Standardeinstellung ist die Umleitung spezieller Ordner zugelassen.

Diese Einstellung verhindert, dass jegliche Objekte, die durch eine Richtlinie gefiltert werden, die Umleitung spezieller Ordner verwenden. Einstellungen an anderer Stelle werden nicht beachtet. Wenn diese Einstellung nicht zugelassen ist, werden verwandte Einstellungen im Webinterface, in StoreFront oder Citrix Receiver ignoriert.

Sie legen fest, welche Benutzer die Umleitung spezieller Ordner erhalten, indem Sie Zugelassen wählen und diese Einstellung in eine Richtlinie aufnehmen, die nach den Benutzern gefiltert wird, denen diese Funktion zur Verfügung stehen soll. Diese Einstellung überschreibt alle anderen Einstellungen für die Umleitung spezieller Ordner.

Die Umleitung spezieller Ordner interagiert mit dem Clientgerät. Daher verhindern Einstellungen, die den Benutzerzugriff auf lokale Festplatten untersagen, auch die Umleitung spezieller Ordner.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, müssen Sie auch für die Einstellung Lokale Clientfestplattenlaufwerke die Option Zugelassen wählen.

Asynchrones Schreiben verwenden

Mit dieser Einstellung aktivieren oder deaktivieren Sie asynchrones Schreiben auf Laufwerke.

Standardmäßig ist das asynchrone Schreiben deaktiviert.

Für Verbindungen über WANs, die normalerweise durch relativ hohe Bandbreite und hohe Latenz charakterisiert sind, können Sie durch asynchrone Schreibvorgänge die Dateiübertragungen und Schreibvorgänge auf Clientlaufwerke beschleunigen. Sollte jedoch ein Verbindungsfehler oder Datenträgerfehler auftreten, können die Clientdateien, die geschrieben werden, in einem nicht definierten Zustand enden. Dem Benutzer werden dann in einem Popupfenster die betroffenen Dateien angezeigt. Der Benutzer kann das Problem beheben, z. B. durch Neustart einer unterbrochenen Dateiübertragung bei der Wiederverbindung oder nach Beheben eines Datenträgerfehlers.

Citrix empfiehlt, dass asynchrone Schreibvorgänge auf Datenträgern nur für Benutzer implementiert werden, die eine Remoteverbindung mit guter Geschwindigkeit für die Dateiübertragungen benötigen, und die verlorene Dateien oder Daten problemlos wiederherstellen können, sollten Fehler bei der Verbindung oder dem Datenträger auftreten.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, müssen Sie auch für die Einstellung Clientlaufwerkumleitung die Option Zugelassen wählen. Wenn diese Einstellung deaktiviert ist, finden keine asynchronen Schreibvorgänge statt.

Einstellungen der Richtlinie "Flash-Umleitung"

Feb 29, 2016

Der Abschnitt "Flash-Umleitung" enthält Richtlinieneinstellungen für die Behandlung von Flash-Inhalten in Benutzersitzungen.

Flash-Beschleunigung

Aktiviert oder deaktiviert die Wiedergabe von Flash-Inhalten auf Benutzergeräten statt auf dem Server. Standardmäßig ist die clientseitige Wiedergabe von Flash-Inhalten aktiviert.

Hinweis: Diese Einstellung wird für die Legacy-Flash-Umleitung mit dem Citrix Online Plug-In 12.1 verwendet.
Wenn aktiviert, reduziert diese Einstellung die Netzwerk- und Serverlast, indem Flash-Inhalte auf dem Clientgerät wiedergegeben werden. Zusätzlich erreichen Sie mit der Einstellung Flash-URL-Kompatibilitätsliste, dass Flash-Inhalte von bestimmten Websites auf dem Server wiedergegeben werden.

Auf dem Benutzergerät muss die Einstellung HDX MediaStream Flash-Umleitung auf dem Benutzergerät aktivieren auch aktiviert sein.

Ist diese Einstellung deaktiviert, werden Flash-Inhalte von allen Websites, unabhängig von deren URLs, auf dem Server wiedergegeben. Damit nur die Flash-Inhalte bestimmter Websites auf dem Benutzergerät wiedergeben werden, konfigurieren Sie die Einstellung Flash-URL-Kompatibilitätsliste.

Flash-Hintergrundfarbenliste

Mit dieser Einstellung können Sie Schlüsselfarben für bestimmte URLs festlegen.

In der Standardeinstellung sind keine Schlüsselfarben angegeben.

Schlüsselfarben werden hinter clientseitig wiedergegebenem Flash angezeigt und unterstützen die visuelle Erkennung von Bereichen. Die angegebene Schlüsselfarbe sollte selten sein, sonst funktioniert die visuelle Bereichserkennung ggf. nicht richtig.

Gültige Eingaben bestehen aus einer URL (mit optionalen Platzhaltern am Anfang und Ende), der ein 24-Bit-RGB-Farbhexcode folgt. Zum Beispiel: http://citrix.com 000003.

Stellen Sie sicher, dass die angegebene URL die URL für den Flash-Inhalt ist. Sie weicht möglicherweise von der URL der Website ab.

Warnung

Die unsachgemäße Verwendung des Registrierungs-Editors kann zu schwerwiegenden Problemen führen, die nur durch eine Neuinstallation des Betriebssystems gelöst werden können. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine falsche Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.

Auf VDA-Maschinen, auf denen Windows 8 oder Windows 2012 ausgeführt wird, werden mit dieser Einstellung möglicherweise nicht die Schlüsselfarben für die URL festgelegt. Wenn dieses Problem auftritt, bearbeiten Sie die

Registrierung auf der VDA-Maschine.

Verwenden Sie bei 32-Bit-Maschinen die folgende Registrierungseinstellung:

[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer]
"ForceHDXFlashEnabled"=dword:00000001

Verwenden Sie bei 64-Bit-Maschinen die folgende Registrierungseinstellung:

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer]
"ForceHDXFlashEnabled"=dword:00000001

Flash-Abwärtskompatibilität

Mit dieser Einstellung aktivieren oder deaktivieren Sie die Verwendung von Originalfeatures für die Legacy-Flash-Umleitung mit älteren Versionen von Citrix Receiver (früher Citrix Online Plug-In).

Standardmäßig ist diese Einstellung aktiviert.

Auf dem Benutzergerät muss die Einstellung HDX MediaStream Flash-Umleitung auf dem Benutzergerät aktivieren auch aktiviert sein.

Flash-Umleitungsfeatures der zweiten Generation können mit Citrix Receiver 3.0 verwendet werden. Legacyumleitungsfeatures werden mit dem Citrix Online Plug-In 12.1 unterstützt. Um sicherzustellen, dass die Flash-Umleitungsfeatures der zweiten Generation verwendet werden, muss die Flash-Umleitung der zweiten Generation auf dem Server und dem Benutzergerät aktiviert sein. Wenn die Legacyumleitung entweder auf dem Server oder dem Benutzergerät aktiviert ist, werden die Legacyumleitungsfeatures verwendet.

Flash-Standardverhalten

Mit dieser Einstellung wird das Standardverhalten für die Flash-Beschleunigung der zweiten Generation festgelegt.

Standardmäßig ist die Flash-Beschleunigung aktiviert.

Wählen Sie für die Konfiguration dieser Einstellung eine der folgenden Optionen:

- Flash-Beschleunigung aktivieren: Flash-Umleitung wird verwendet.
- Flash Player blockieren: Flash-Umleitung sowie serverseitiges Rendering werden nicht verwendet. Der Benutzer kann keine Flash-Inhalte anzeigen.
- Flash-Beschleunigung deaktivieren: Flash-Umleitung wird nicht verwendet. Der Benutzer kann auf dem Server wiedergegebene Flash-Inhalte anzeigen, wenn ein mit den Inhalten kompatibler Adobe Flash Player für Windows Internet Explorer auf dem Server installiert ist.

Diese Einstellung kann für einzelne Webseiten und Flash-Instanzen basierend auf der Einstellung Flash-URL-Kompatibilitätsliste überschrieben werden. Außerdem muss auf dem Benutzergerät die Einstellung HDX MediaStream Flash-Umleitung auf dem Benutzergerät aktivieren aktiviert sein.

Flash-Ereignisprotokollierung

Mit dieser Einstellung aktivieren oder deaktivieren Sie die Aufzeichnung von Flash-Ereignissen im Windows-Anwendungsereignisprotokoll.

Standardmäßig ist die Protokollierung aktiviert.

Auf Computern unter Windows 7 oder Windows Vista wird ein spezielles Protokoll für die Flash-Umleitung im Knoten "Anwendungs- und Dienstprotokolle" angezeigt.

Flash - intelligentes Fallback

Mit dieser Einstellung aktivieren oder deaktivieren Sie automatische Versuche, das serverseitige Rendering für Flash Player-Instanzen zu verwenden, wenn das clientseitige Rendering entweder unnötig ist oder eine schlechte Benutzererfahrung ergibt.

Standardmäßig ist diese Einstellung aktiviert.

Flash-Latenzschwellenwert

Mit dieser Einstellung geben Sie einen Schwellenwert zwischen 0-30 Millisekunden an, um festzulegen, wo Adobe Flash-Inhalte wiedergegeben werden.

In der Standardeinstellung ist der Schwellenwert 30.

Beim Start wird die aktuelle Latenz zwischen Server und Benutzergerät von HDX MediaStream für Flash gemessen. Wenn die Latenz unter dem Schwellenwert liegt, werden Flash-Inhalte mit HDX MediaStream für Flash auf dem Benutzergerät wiedergegeben. Wenn die Latenz den Schwellenwert überschreitet, werden die Inhalte auf dem Netzwerkserver wiedergegeben, wenn Adobe Flash Player dort vorhanden ist.

Wenn Sie diese Einstellung aktivieren, muss die Einstellung Flash-Abwärtskompatibilität vorhanden und auf Zugelassen eingestellt sein.

Hinweis: Dies gilt nur, wenn HDX MediaStream Flash-Umleitung im Legacymodus verwendet wird.

Verhindern von Flash-Videofallback

Mit dieser Einstellung geben Sie an, ob und wie "kleine" Flash-Inhalte gerendert und angezeigt werden.

Standardmäßig ist diese Einstellung nicht konfiguriert.

Wählen Sie für die Konfiguration dieser Einstellung eine der folgenden Optionen:

- **Only small content:** Es werden nur Intelligentes-Fallback-Inhalte auf dem Server gerendert, andere Flash-Inhalte werden durch eine Fehler-SWF-Datei ersetzt.
- **Only small content with a supported client:** Es werden nur Intelligentes-Fallback-Inhalte auf dem Server gerendert, wenn der Client aktuell die Flash-Umleitung verwendet, andere Flash-Inhalte werden durch eine Fehler-SWF-Datei ersetzt.
- **No server side content:** Alle Inhalte auf dem Server werden durch eine Fehler-SWF-Datei ersetzt.

Zum Verwenden dieser Richtlinieneinstellung geben Sie eine Fehler-SWF-Datei an. Diese Fehler-SWF-Datei ersetzt alle Flash-Inhalte, die nicht auf dem VDA gerendert werden sollen.

Fehler beim Verhindern von Flash-Videofallback *.swf

Diese Einstellung legt die URL der Fehlermeldung fest, die anstelle von Flash-Instanzen angezeigt wird, wenn Server-Lastverwaltungsrichtlinien verwendet werden. Beispiel:

    http://domainName.tld/sample/path/error.swf

URL-Liste für serverseitigen Flash-Inhaltsabruf

Mit dieser Einstellung geben Sie die Websites an, deren Flash-Inhalte auf den Server heruntergeladen und dann auf das Benutzergerät zur Wiedergabe übertragen werden.

In der Standardeinstellung sind keine Sites angegeben.

Diese Einstellung wird verwendet, wenn das Benutzergerät keinen direkten Internetzugang hat; der Server stellt die Verbindung bereit. Auf dem Benutzergerät muss die Einstellung Serverseitigen Inhaltsabruf aktivieren auch aktiviert sein.

Die Flash-Umleitung der zweiten Generation enthält ein Fallback für den serverseitigen Flash-Inhaltsabruf für SWF-Dateien. Wenn ein Benutzergerät Flash-Inhalte nicht von einer Website abrufen kann, und die Website in der URL-Liste für serverseitigen Flash-Inhaltsabruf angegeben ist, erfolgt automatisch der serverseitige Inhaltsabruf.

Hinzufügen von URLs zur Liste:

- Fügen Sie die URL der Flash-Anwendung und nicht die HTML-Seite auf oberster Ebene hinzu, die Flash Player initiiert.
- Verwenden Sie ein Sternchen (*) am Anfang oder am Ende der URL als Platzhalterzeichen.
- Verwenden Sie den Platzhalter am Ende, um alle untergeordneten URLs zuzulassen (http://www.citrix.com/*).
- Die Präfixe http:// und https:// werden verwendet (falls vorhanden), sind jedoch für gültige Listeneinträge nicht vorgeschrieben.

Flash-URL-Kompatibilitätsliste

Mit dieser Einstellung geben Sie die Regeln an, die festlegen, ob die Wiedergabe von Flash-Inhalten auf bestimmten Websites auf dem Benutzergerät oder auf dem Server erfolgt oder ob sie blockiert wird.

In der Standardeinstellung sind keine Regeln angegeben.

Hinzufügen von URLs zur Liste:

- Sortieren Sie die Liste nach Priorität, sodass die wichtigsten URLs, Aktionen und Wiedergabeorte ganz oben stehen.
- Verwenden Sie ein Sternchen (*) am Anfang oder am Ende der URL als Platzhalterzeichen.
- Verwenden Sie den Platzhalter am Ende, um auf alle untergeordneten URLs zu verweisen (http://www.citrix.com/*).
- Die Präfixe http:// und https:// werden verwendet (falls vorhanden), sind jedoch für gültige Listeneinträge nicht vorgeschrieben.
- Fügen Sie der Liste Websites hinzu, deren Flash-Inhalte nicht richtig auf dem Benutzergerät wiedergegeben werden, und wählen Sie entweder die Optionen Auf Server rendern oder Blockieren.

Einstellungen der Richtlinie "Grafiken"

Feb 29, 2016

Der Abschnitt "Grafiken" enthält Richtlinieneinstellungen, mit denen Sie steuern, wie Bilder in Benutzersitzungen behandelt werden.

Anzeigespeicherlimit

Mit dieser Einstellung geben Sie die maximale Größe des Videopuffers (in Kilobytes) für die Sitzung an.

Das Standardlimit ist 65536 Kilobytes.

Für Verbindungen, die eine größere Farbtiefe und eine höhere Auflösung erfordern, erhöhen Sie den Grenzwert. Berechnen Sie den maximal erforderlichen Arbeitsspeicher mit dieser Formel:

Speicher in Byte = (Farbtiefe in Bits pro Pixel) / 8) * (vertikale Auflösung in Pixel)*(horizontale Auflösung in Pixel).

Beispiel: Bei einer Farbtiefe von 32, einer vertikalen Auflösung von 600 und einer horizontalen Auflösung von 800 ergibt dies einen maximal erforderlichen Arbeitsspeicher von (32 / 8) * (600) * (800) = 1920000 Byte, was ein Anzeigespeicherlimit von 1920 KB ergibt.

Andere Farbtiefen als 32 Bit sind nur verfügbar, wenn die Richtlinieneinstellung Legacygrafikmodus aktiviert ist.

HDX weist Benutzern nur den pro Sitzung erforderlichen Anzeigespeicher zu. Wenn also nur einige Benutzer mehr als den Standardspeicher benötigen, hat das Erhöhen des Anzeigespeicherlimits keine negativen Auswirkungen auf die Skalierbarkeit.

Herabsetzungspräferenz für Anzeigemodus

Hinweis: Bei Virtual Delivery Agent 7.x gilt diese Richtlinieneinstellung nur, wenn die Richtlinieneinstellung Legacygrafikmodus aktiviert ist.
Diese Einstellung gibt an, ob die Farbtiefe oder die Auflösung zuerst herabgesetzt werden soll, wenn das Speicherlimit für die Sitzung erreicht wird.

Standardmäßig wird die Farbtiefe zuerst herabgesetzt.

Wenn das Speicherlimit der Sitzung erreicht wird, können Sie die Bildqualität verringern, indem Sie erst die Farbtiefe oder erst die Auflösung herabsetzen. Wird erst die Farbtiefe herabgesetzt, werden Bilder mit weniger Farben dargestellt. Wird erst die Auflösung herabgesetzt, werden Bilder mit weniger Pixel pro Zoll angezeigt.

Wenn Benutzer in dem Fall benachrichtigt werden sollen, dass entweder die Farbtiefe oder die Auflösung herabgesetzt werden muss, konfigurieren Sie die Einstellung Benutzer beim Herabsetzen des Anzeigemodus benachrichtigen.

Dynamische Fenstervorschau

Mit dieser Einstellung kann die Anzeige von Seamlessfenster in den Fenstervorschaumodi Flip, Flip 3D, Taskleistenvorschau und Einsehen aktiviert bzw. deaktiviert werden.

Windows Aero-Vorschauoption	**Beschreibung**
Symbolleistenvorschau	Wenn der Benutzer auf das Symbol eines Fensters zeigt, wird ein Bild dieses Fensters über der

Windows Aero-Vorschauoption	Beschreibung
Fenstervorschau	Symbolleiste angezeigt. Wenn der Benutzer auf ein Symbolleistenvorschaubild zeigt, wird das Bild in voller Größe auf dem Bildschirm angezeigt.
Flip	Wenn der Benutzer Alt + Tab drückt, werden kleine Vorschausymbole für jedes geöffnete Fenster angezeigt.
Flip-3D	Wenn der Benutzer die Tabulator- und Windows-Tasten drückt, werden große Bilder der geöffneten Fenster überlappend auf dem Bildschirm angezeigt.

Standardmäßig ist diese Einstellung aktiviert.

Bildzwischenspeicherung

Hinweis: Bei Virtual Delivery Agent 7.x gilt diese Richtlinieneinstellung nur, wenn die Richtlinieneinstellung Legacygrafikmodus aktiviert ist.
Mit dieser Einstellung aktivieren oder deaktivieren Sie das Zwischenspeichern und Abrufen von Bildabschnitten in Sitzungen. Durch das Zwischenspeichern von Bildern in Abschnitten und das Abrufen dieser Abschnitte wird das Ruckeln beim Bildlauf verringert. Darüber hinaus werden weniger Daten über das Netzwerk übertragen und die Verarbeitung auf dem Benutzergerät wird reduziert.

Standardmäßig ist die Einstellung für die Bildzwischenspeicherung aktiviert.

Hinweis: Die Einstellung für die Bildzwischenspeicherung steuert, wie Bilder zwischengespeichert und abgerufen werden, jedoch nicht, ob sie zwischengespeichert werden. Wenn die Einstellung "Legacygrafikmodus" aktiviert ist, werden Bilder zwischengespeichert.

Legacygrafikmodus

Diese Einstellung deaktiviert die umfassende Grafikdarstellung und verwendet den Legacygrafikmodus, um die Skalierbarkeit über ein WAN oder eine mobile Verbindung zu verbessern.

Die Einstellung ist standardmäßig deaktiviert und die umfassende Grafikdarstellung wird verwendet.

Maximal zugelassene Farbtiefe

Hinweis: Bei Virtual Delivery Agent 7.x gilt diese Richtlinieneinstellung nur, wenn die Richtlinieneinstellung Legacygrafikmodus aktiviert ist.
Mit dieser Einstellung geben Sie die maximale Farbtiefe an, die für eine Sitzung zulässig ist.

Die Standardeinstellung für die maximal zulässige Farbtiefe ist 32 Bits pro Pixel.

Diese Einstellung gilt nur für ThinWire-Treiber und -Verbindungen. Sie gilt nicht für VDAs mit einem anderen Treiber als ThinWire für die primäre Anzeige, z. B. VDAs mit WDDM-Treiber (Windows Display Driver Model). Bei Desktopbetriebssystem-VDAs mit einem WDDM-Treiber als primären Anzeigetreiber, z. B. Windows 8, hat diese Einstellung keine Auswirkung. Bei Windows-Serverbetriebssystem-VDAs mit WDDM-Treiber, z. B. Windows Server 2012 R2, kann diese Einstellung verhindern, dass Benutzer eine Verbindung mit dem VDA herstellen.

Für eine hohe Farbtiefe ist mehr Speicher erforderlich. Damit die Farbtiefe herabgesetzt wird, wenn das Speicherlimit erreicht wurde, konfigurieren Sie die Einstellung Herabsetzungspräferenz für Anzeigemodus. Wird die Farbtiefe herabgesetzt, werden Bilder mit weniger Farben dargestellt.

Benutzer beim Herabsetzen des Anzeigemodus benachrichtigen

Hinweis: Bei Virtual Delivery Agent 7.x gilt diese Richtlinieneinstellung nur, wenn die Richtlinieneinstellung Legacygrafikmodus aktiviert ist.
Mit dieser Einstellung erzielen Sie, dass Benutzer eine kurze Erklärung erhalten, wenn die Farbtiefe oder die Auflösung herabgesetzt wird.

Standardmäßig werden Benutzer nicht benachrichtigt.

Warteschlange und Verwerfen

Hinweis: Bei Virtual Delivery Agent 7.x gilt diese Richtlinieneinstellung nur, wenn die Richtlinieneinstellung Legacygrafikmodus aktiviert ist.
Mit dieser Einstellung werden Bilder in der Warteschlange verworfen, die durch ein anderes Bild ersetzt wurden.

Standardmäßig ist diese Einstellung aktiviert.

Dies verbessert die Reaktionszeit, wenn Grafiken an das Benutzergerät gesendet werden. Wenn Sie diese Einstellung konfigurieren, ruckeln Animationen möglicherweise, weil Frames ausgelassen werden.

Einstellungen der Richtlinie "Zwischenspeichern"

Feb 29, 2016

Der Abschnitt "Zwischenspeichern" enthält Einstellungen, mit denen Bilddaten auf Benutzergeräten zwischengespeichert werden können, wenn Clientverbindungen eine beschränkte Bandbreite haben.

Schwellenwert für permanenten Cache

Hinweis: Bei Virtual Delivery Agent 7.x gilt diese Richtlinieneinstellung nur, wenn die Richtlinieneinstellung Legacygrafikmodus aktiviert ist.
Mit dieser Einstellung werden Bitmaps auf der Festplatte des Benutzergeräts zwischengespeichert. Dies ermöglicht eine Wiederverwendung von großen, oft verwendeten Bildern aus früheren Sitzungen.

Der Standardschwellenwert ist 3000000 Bits pro Sekunde.

Der Schwellenwert ist der Wert, unter dem das Feature "Permanentcache" angewendet wird. Beispielsweise werden mit dem Standardwert Bitmaps auf der Festplatte des Benutzergeräts zwischengespeichert, wenn die Bandbreite unter 3000000 Bit/s fällt.

Framehawk-Richtlinieneinstellungen

Feb 29, 2016

Der Abschnitt "Framehawk" enthält Richtlinieneinstellungen zum Aktivieren und Konfigurieren des Framehawk-Anzeigekanals auf dem Server.

Framehawk-Anzeigekanal

Wenn diese Option aktiviert ist, versucht der Server, den Framehawk-Anzeigekanal für die Grafiken und das Eingabe-Remoting der Benutzer zu verwenden. Bei diesem Anzeigekanal bietet durch UDP eine bessere Benutzererfahrung in Netzwerken mit hohem Verlust und hoher Latenz, er verbraucht jedoch u. U. mehr Serverressourcen und Bandbreite als andere Grafikmodi.

Standardmäßig ist der Framehawk-Anzeigekanal deaktiviert.

Portbereich für Framehawk-Anzeigekanal

Mit dieser Richtlinieneinstellung geben Sie den Bereich der Portnummern an (im Format *niedrigste Portnummer,höchste Portnummer*), die vom VDA zum Austausch von Framehawk-Anzeigekanaldaten mit dem Benutzergerät verwendet werden. Der VDA versucht die Verwendung eines Ports, beginnend bei dem Port mit der niedrigsten Nummer und geht dann ggf. zu dem Port mit der nächsthöheren Nummer über. Über den Port erfolgen eingehende und ausgehende Datenübertragungen.

Der Standardportbereich ist 3224,3324.

Einstellungen der Richtlinie "Keep-Alive"

Feb 29, 2016

Der Abschnitt "Keep-Alive" enthält Richtlinieneinstellungen für die Verwaltung der ICA-Keep-Alive-Meldungen.

ICA-Keep-Alive - Timeout

Mit dieser Einstellung geben Sie die Anzahl der Sekunden zwischen aufeinanderfolgenden ICA-Keep-Alive-Meldungen an.

Das Standardintervall zwischen Keep-Alive-Meldungen ist 60 Sekunden.

Geben Sie ein Intervall zwischen 1-3600 Sekunden an, in dem ICA-Keep-Alive-Meldungen gesendet werden. Konfigurieren Sie diese Einstellung nicht, wenn Sie eine Netzwerküberwachungssoftware zum Schließen inaktiver Verbindungen verwenden.

ICA-Keep-Alives

Mit dieser Einstellung legen Sie fest, ob ICA-Keep-Alive-Meldungen in regelmäßigen Abständen gesendet werden sollen.

Standardmäßig werden keine Keep-Alive-Meldungen gesendet.

Wenn Sie diese Einstellung aktivieren, wird verhindert, dass unterbrochene Verbindungen getrennt werden. Wenn der Server keine Aktivität feststellt, verhindert diese Einstellung, dass die Sitzung durch die Remotedesktopdienste getrennt wird. Der Server sendet alle paar Sekunden Keep-Alive-Meldungen, um zu ermitteln, ob die Sitzung aktiv ist. Wenn die Sitzung nicht mehr aktiv ist, wird die Sitzung vom Server als "Getrennt" gekennzeichnet.

ICA-Keep-Alive funktioniert nicht, wenn Sie die Sitzungszuverlässigkeit verwenden. Konfigurieren Sie daher ICA-Keep-Alive nur für Verbindungen, die die Sitzungszuverlässigkeit nicht verwenden.

Verwandte Richtlinieneinstellungen: Sitzungszuverlässigkeit - Verbindungen.

Einstellungen der Richtlinie "Lokaler App-Zugriff"

Feb 29, 2016

Der Abschnitt "Lokaler App-Zugriff" enthält Richtlinieneinstellungen, mit denen Sie die Integration lokal installierter Anwendungen mit gehosteten Anwendungen in einer gehosteten Desktopumgebung konfigurieren können.

Lokalen App-Zugriff zulassen

Mit dieser Einstellung legen Sie fest, ob die Integration lokal installierter Anwendungen mit gehosteten Anwendungen in einer gehosteten Desktopumgebung zugelassen oder verweigert werden soll.

Wenn ein Benutzer eine lokal installierte Anwendung startet, wirkt es so, als ob diese auf dem virtuellen Desktop des Benutzers ausgeführt würde, obwohl sie tatsächlich lokal ausgeführt wird.

Standardmäßig ist der lokale App-Zugriff nicht zulässig.

URL-Umleitungssperrliste

Mit dieser Einstellung geben Sie Websites an, die Ziel einer Weiterleitung sind und im lokalen Webbrowser gestartet werden sollen. Dies kann auch Websites umfassen, für die Gebietsschema-Informationen erforderlich sind (z. B. msn.com oder newsgoogle.com) oder Websites mit reichhaltigen Medieninhalten, die besser auf dem Benutzergerät wiedergegeben werden.

In der Standardeinstellung sind keine Sites angegeben.

URL-Umleitungspositivliste

Mit dieser Einstellung geben Sie die Websites an, die in der Umgebung, in der sie gestartet werden, wiedergegeben werden sollen.

In der Standardeinstellung sind keine Sites angegeben.

Einstellungen der Richtlinie "Mobilerfahrung"

Feb 29, 2016

Der Abschnitt "Mobilerfahrung" enthält Richtlinieneinstellungen für die Handhabung des Citrix Mobility Packs.

Automatische Anzeige der Tastatur

Diese Einstellung aktiviert oder deaktiviert die automatische Anzeige der Tastatur auf Bildschirmen von Mobilgeräten.

Standardmäßig ist die automatische Anzeige der Tastatur deaktiviert.

Für Fingereingabe optimierten Desktop starten

Diese Einstellung ist deaktiviert und für Windows 10-Maschinen nicht verfügbar.

Diese Einstellung bestimmt das allgemeine Verhalten der Citrix Receiver-Benutzeroberfläche, indem sie eine für die Fingereingabe optimierte Benutzeroberfläche zulässt oder verweigert, die für Tablet-Geräte optimiert ist.

Standardmäßig wird eine für die Fingereingabe optimierte Benutzeroberfläche verwendet.

Setzen Sie diese Richtlinie auf "Nicht zugelassen", um nur die Windows-Benutzeroberfläche zu verwenden.

Kombinationsfelder remoten

Diese Einstellung bestimmt die Typen von Kombinationsfeldern, die in Sitzungen auf mobilen Geräten angezeigt werden können. Stellen Sie diese Richtlinie auf Zugelassen ein, um das gerätenative Kombinationsfeld-Steuerelement anzuzeigen. Wenn diese Einstellung zugelassen ist, kann ein Benutzer eine Sitzungseinstellung in Citrix Receiver für iOS ändern und das Windows-Kombinationsfeld verwenden.

Standardmäßig wird die Funktion zum Remoten von Kombinationsfeldern verweigert.

Einstellungen der Richtlinie "Multimedia"

Feb 29, 2016

Der Abschnitt "Multimedia" enthält Richtlinieneinstellungen, mit denen Sie das Streaming von Audio und Video in Benutzersitzungen verwalten.

Videoqualität beschränken

Mit dieser Einstellung geben Sie die maximale Videoqualitätsstufe für eine HDX-Verbindung an. Wird die Einstellung konfiguriert, dann wird die Videoqualität auf den angegebenen Wert beschränkt, sodass die Dienstqualität für Multimedia in der Umgebung gewährleistet ist.

Standardmäßig ist diese Einstellung nicht konfiguriert.

Zum Festlegen der maximalen Qualität wählen Sie eine der folgenden Optionen:

- 1080p/8,5 MBit/s
- 720p/4,0 MBit/s
- 480p/720 KBit/s
- 380p/400 KBit/s
- 240p/200 KBit/s

Hinweis: Die gleichzeitige Wiedergabe mehrerer Videos auf einem Server verbraucht viele Ressourcen und kann die Skalierbarkeit des Servers beeinträchtigen.

Multimediakonferenzen

Mit dieser Einstellung legen Sie fest, ob die Unterstützung von Videokonferenzanwendungen zugelassen ist.

Standardmäßig ist die Unterstützung für Videokonferenzen zugelassen.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, muss die Einstellung Windows Media-Umleitung vorhanden und auf Zugelassen gesetzt sein.

Für Multimediakonferenzen müssen folgende Bedingungen erfüllt sein:

- Der Gerätetreiber des Herstellers für die in der Multimediakonferenz verwendete Webcam muss installiert sein.
- Die Webcam muss mit dem Clientgerät verbunden werden, bevor eine Videokonferenzsitzung initiiert wird. Der Server verwendet zu jedem Zeitpunkt nur eine installierte Webcam. Wenn mehrere Webcams auf dem Benutzergerät installiert sind, versucht der Server nacheinander jede Webcam zu verwenden, bis eine Videokonferenzsitzung steht.

Optimierung von Windows Media-Multimediaumleitung über WAN

Mit dieser Einstellung aktivieren Sie die Multimediatranscodierung in Echtzeit. Damit wird Audio- und Videostreaming für mobile Geräte ermöglicht und die Benutzererfahrung durch eine verbesserte Übermittlung von Windows Media-Inhalt über WAN optimiert.

Standardmäßig wird die Bereitstellung von Windows Media-Inhalt über das WAN optimiert.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, muss die Einstellung Windows Media-Umleitung vorhanden und auf Zugelassen gesetzt sein.

Wenn diese Einstellung aktiviert ist, wird die Multimediatranscodierung nach Bedarf automatisch bereitgestellt, sodass Audio- und Videostreaming zur Verbesserung der Benutzererfahrung auch bei schlechten Netzwerkbedingungen ermöglicht

wird.

GPU für die Optimierung von Windows Media-Multimediaumleitung über WAN verwenden

Mit dieser Einstellung wird die Transcodierung von Multimediainhalten in Echtzeit im Grafikprozessor (GPU) des Virtual Delivery Agent (VDA) ermöglicht, um die Serverskalierbarkeit zu verbessern. Die GPU-Transcodierung ist nur verfügbar, wenn der VDA eine unterstützte GPU für die Hardwarebeschleunigung hat. Andernfalls erfolgt die Transcodierung automatisch in der CPU.

Hinweis: GPU-Transcodierung wird nur von NVIDIA-GPUs unterstützt.
Standardmäßig ist die Verwendung der GPU auf dem VDA zum Optimieren der Bereitstellung von Windows Media-Inhalt über das WAN nicht zulässig.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, stellen Sie sicher, dass die Einstellungen Windows Media-Umleitung und Optimierung von Windows Media-Multimediaumleitung über WAN vorhanden und auf Zugelassen gesetzt sind.

Verhindern von Videofallback

Administratoren können über die Einstellung der Richtlinie "Verhindern von Videofallback" die Methoden für die Übertragung gestreamter Inhalte an Benutzer festlegen.

Standardmäßig ist diese Einstellung nicht konfiguriert. Dies ermöglicht ein Fallback vom clientseitigen Abruf auf RAVE und von dort auf den Server.

Wählen Sie für die Konfiguration dieser Einstellung eine der folgenden Optionen:

- **Serverseitiger Abruf - Serverseitige Wiedergabe**: ermöglicht ein Fallback vom clientseitigen Abruf auf RAVE und von dort auf den Server.
- **Serverseitiger Abruf - Clientseitige Wiedergabe**: ermöglicht ein Fallback vom clientseitigen Abruf auf RAVE, jedoch kein Fallback von RAVE auf den Server.
- **Clientseitiger Abruf - Clientseitige Wiedergabe**: lässt kein Fallback vom clientseitigen Abruf auf RAVE und von dort auf den Server zu.

Wird der Inhalt nicht wiedergegeben, wird im Playerfenster gemeldet, dass das Video wegen mangelnder Ressourcen blockiert wurde.

Clientseitiger Abruf von Windows Media-Inhalten

Diese Einstellung ermöglicht das Streamen von Multimediadateien anstatt über den Hostserver direkt vom Quellanbieter im Internet oder Intranet auf Benutzergeräte.

Standardmäßig ist das direkte Streaming von Multimediadateien vom Quellenanbieter auf Benutzergeräte zulässig.

Zulassen dieser Einstellung verbessert die Netzwerknutzung und Serverskalierbarkeit durch Verschieben der gesamten Medienverarbeitung vom Hostserver auf das Benutzergerät. Dadurch wird auch das Erfordernis der Installation eines erweiterten Multimedia-Frameworks, z. B. von Microsoft DirectShow oder Media Foundation, auf Benutzergeräten hinfällig. Diese müssen lediglich eine Datei von einer URL abspielen können.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, muss die Einstellung Windows Media-Umleitung vorhanden und auf Zugelassen gesetzt sein. Wenn diese Einstellung deaktiviert ist, ist das direkte Streaming von Multimediadateien auf Benutzergeräte ebenfalls deaktiviert.

Windows Media-Umleitung

Diese Einstellung steuert und optimiert die Art und Weise, mit der Streamingaudio und -video Benutzern von Servern bereitgestellt wird.

Standardmäßig ist das Streamen von Audio und Video für Benutzer zulässig.

Zulassen dieser Einstellung erhöht die Qualität von auf dem Server wiedergegebenem Audio und Video auf ein Niveau, das dem der lokalen Wiedergabe auf dem Benutzergerät entspricht. Der Server streamt Multimediainhalte komprimiert im Originalformat zum Client, Dekomprimierung und Wiedergabe der Medien übernimmt das Benutzergerät.

Die Windows Media-Umleitung optimiert Multimediadateien, die mit Codecs verschlüsselt sind, die den Standards von Microsoft DirectShow, DirectX Media Objects (DMO) und Media Foundation entsprechen. Um eine Multimediadatei wiederzugeben, muss ein mit dem Codierungsformat der Multimediadatei kompatibler Codec auf dem Benutzergerät vorhanden sein.

In der Standardeinstellung ist Audio auf Citrix Receiver deaktiviert. Wenn Benutzer Multimedia-Anwendungen in ICA-Sitzungen ausführen können, aktivieren Sie Audio oder geben Sie den Benutzern in der Citrix Receiver-Benutzeroberfläche die Berechtigung, Audio zu aktivieren.

Wählen Sie Verweigert nur, wenn die Wiedergabe von Medien mit der Windows Medienumleitung schlechter zu sein scheint, als mit der ICA-Komprimierung und regulärem Audio. Dies ist selten, kann aber mit geringer Bandbreite vorkommen, beispielsweise bei Medien, in denen die Schlüsselbilder (Keyframes) sehr weit auseinander liegen.

Windows Media-Umleitungspuffergröße

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

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 (5 Sekunden).

Einstellungen der Richtlinie "Multistreamverbindungen"

Feb 29, 2016

Im Abschnitt "Multistreamverbindungen" finden Sie Richtlinieneinstellungen zum Verwalten der Quality-of-Service-Priorität (QoS) für mehrere ICA-Verbindungen in einer Sitzung.

Audio über UDP

Mit dieser Einstellung legen Sie fest, ob Audio über UDP auf dem Server zugelassen wird.

Standardmäßig ist Audio über UDP auf dem Server zugelassen.

Wenn diese Einstellung aktiviert ist, wird ein UDP-Port auf dem Server geöffnet, sodass alle Verbindungen, die zur Verwendung von Audio über UDP - Real-time Transport konfiguriert sind, unterstützt werden.

Audio-UDP-Portbereich

Mit dieser Einstellung geben Sie den Bereich der Portnummern an (im Format niedrigste Portnummer,höchste Portnummer), die von Virtual Desktop Agent (VDA) zum Austausch von Audiopaketdaten mit dem Benutzergerät verwendet werden. Der VDA versucht, jedes UDP-Portpaar für den Austausch von Daten mit dem Benutzergerät zu verwenden. Dabei wird mit dem Port, der die niedrigste Nummer hat, begonnen und die Zahl für jeden folgenden Versuch um 2 erhöht. Alle Ports übernehmen eingehende und ausgehende Datenübertragungen.

Die Standardeinstellung ist 16500,16509.

Multiportrichtlinie

Mit dieser Einstellung geben Sie die TCP-Ports an, die für den ICA-Verkehr verwendet werden sollen, und legen eine Netzwerkpriorität für jeden Port fest.

Standardmäßig hat der primäre Port (2598) eine hohe Priorität.

Wenn Sie Ports konfigurieren, können Sie die folgenden Prioritäten zuweisen:

- Sehr hoch: für Echtzeitvorgänge, z. B. Webkonferenzen.
- Hoch: für interaktive Elemente, z. B. Bildschirm, Tastatur und Maus.
- Mittel: für Massenvorgänge, z. B. Clientlaufwerkzuordnung.
- Niedrig: für Hintergrundaufgaben, z. B. Drucken.

Jeder Port muss eine eindeutige Priorität haben. Sie können also nicht eine sehr hohe Priorität sowohl für CGP-Port 1 als auch für CGP-Port 3 zuweisen.

Wenn Sie für einen Port keine Priorität einstellen möchten, setzen Sie den Wert für den Port auf 0. Sie können den primären Port nicht entfernen und Sie können seine Prioritätsstufe nicht ändern.

Wenn Sie diese Einstellung konfigurieren, starten Sie den Server neu. Diese Einstellung wird nur angewendet, wenn die Richtlinie Multistreamcomputereinstellung aktiviert ist.

Multistreamcomputereinstellung

Mit dieser Einstellung aktivieren oder deaktivieren Sie Multistream auf dem Server.

Standardmäßig ist Multistream deaktiviert.

Wenn Sie Citrix Cloudbridge mit Multistream-Unterstützung in Ihrer Umgebung verwenden, müssen Sie diese Einstellung nicht konfigurieren. Konfigurieren Sie diese Richtlinieneinstellung, wenn Sie Router von Drittanbietern oder Legacy-Branch Repeater verwenden, um die gewünschte Quality of Service (QoS) zu erzielen.

Wenn Sie diese Einstellung konfigurieren, starten Sie den Server neu, um sicherzustellen, dass die Änderungen wirksam werden.
Wichtig: Das Verwenden dieser Richtlinieneinstellung mit den Richtlinieneinstellungen für das Bandbreitenlimit, wie beispielsweise Bandbreitenlimit für Sitzung insgesamt kann zu unerwarteten Ergebnissen führen. Wenn Sie diese Einstellung in eine Richtlinie aufnehmen, stellen Sie sicher, dass Sie keine Bandbreitenlimit-Einstellungen einschließen.

Multistreambenutzereinstellung

Mit dieser Einstellung aktivieren oder deaktivieren Sie Multistream auf dem Benutzergerät.

Standardmäßig ist Multistream für alle Benutzer deaktiviert.

Diese Einstellung wird nur auf Hosts angewendet, für die die Richtlinie Multistreamcomputereinstellung aktiviert ist.
Wichtig: Das Verwenden dieser Richtlinieneinstellung mit den Richtlinieneinstellungen für das Bandbreitenlimit, z. B. Bandbreitenlimit für Sitzung insgesamt, kann zu unerwarteten Ergebnissen führen. Wenn Sie diese Einstellung in eine Richtlinie aufnehmen, stellen Sie sicher, dass Sie keine Bandbreitenlimit-Einstellungen einschließen.

Einstellungen der Richtlinie "Portumleitung"

Feb 29, 2016

Der Abschnitt "Portumleitung" enthält Richtlinieneinstellungen für die LPT- und COM-Portzuordnung auf dem Client.

Hinweis: Konfigurieren Sie bei Virtual Delivery Agent 7.x diese Einstellungen über die Registrierung (siehe Konfigurieren von COM-Port- und LPT-Portumleitungseinstellungen in der Registrierung).

Client-COM-Ports automatisch verbinden

Mit dieser Einstellung aktivieren oder deaktivieren Sie die automatische Verbindung von COM-Ports auf dem Benutzergerät, wenn Benutzer sich bei der Site anmelden.

Standardmäßig werden COM-Ports nicht automatisch verbunden.

Client-LPT-Ports automatisch verbinden

Mit dieser Einstellung aktivieren oder deaktivieren Sie die automatische Verbindung von LPT-Ports auf dem Benutzergerät, wenn Benutzer sich bei der Site anmelden.

Standardmäßig werden LPT-Ports nicht automatisch verbunden.

Client-COM-Portumleitung

Mit dieser Einstellung legen Sie fest, ob der Zugriff auf COM-Ports des Benutzergeräts zulässig ist.

Standardmäßig ist die COM-Portumleitung nicht zugelassen.

Die folgenden Richtlinieneinstellungen hängen zusammen:

- Bandbreitenlimit für COM-Portumleitung
- Bandbreitenlimit für COM-Portumleitung (Prozent)

Client-LPT-Portumleitung

Mit dieser Einstellung legen Sie fest, ob der Zugriff auf LPT-Ports des Benutzergeräts zulässig ist.

Standardmäßig ist die LPT-Portumleitung nicht zugelassen.

LPT-Ports werden nur von Legacyanwendungen verwendet, die Druckaufträge an LPT-Ports senden und nicht an die Druckerobjekte auf dem Benutzergerät. Die meisten Geräte können heute Druckaufträge and Druckerobjekte senden. Diese Richtlinieneinstellung ist nur für Server erforderlich, auf denen Legacyanwendungen gehostet werden, die für das Drucken LPT-Ports verwenden.

Die folgenden Richtlinieneinstellungen hängen zusammen:

- Bandbreitenlimit für LPT-Portumleitung
- Bandbreitenlimit für LPT-Portumleitung (Prozent)

Einstellungen der Richtlinie "Drucken"

Feb 29, 2016

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).

Druckerzuweisungen

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 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.

- 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.

Ereignisprotokollpräferenz für die automatische Druckererstellung

Mit dieser Einstellung geben Sie an, welche Ereignisse bei der automatischen Druckererstellung protokolliert werden. Sie haben die Option, keine Fehler oder Warnungen, nur Fehler oder Fehler und Warnungen zu protokollieren.

Standardmäßig werden Fehler und Warnungen protokolliert.

Ein Beispiel für eine Warnung ist ein Ereignis, bei dem der native Druckertreiber für einen Drucker nicht installiert werden konnte und stattdessen der universelle Druckertreiber installiert wurde. Damit der universelle Druckertreiber in diesem Szenario verwendet werden kann, stellen Sie für Verwendung universeller Druckertreiber entweder Nur universelles Drucken verwenden oder Universelles Drucken nur verwenden, wenn angeforderter Treiber nicht verfügbar ist ein.

Sitzungsdrucker

Mit dieser Einstellung geben Sie die Netzwerkdrucker an, die in einer ICA-Sitzung automatisch erstellt werden sollen.

In der Standardeinstellung sind keine Drucker angegeben.

Um Drucker hinzuzufügen, geben Sie den UNC-Pfad des Druckers ein, der automatisch erstellt werden soll. Nach dem Hinzufügen des Druckers können Sie angepasste Einstellungen für die aktuelle Sitzung bei jeder Anmeldung anwenden.

Warten bis Drucker erstellt sind (Serverdesktop)

Mit dieser Einstellung legen Sie fest, ob es eine Verzögerung bei der Sitzungsverbindung geben soll, sodass Serverdesktopdrucker automatisch erstellt werden können.

Standardmäßig findet keine Verbindungsverzögerung statt.

Einstellungen der Richtlinie "Clientdrucker"

Feb 29, 2016

Der Abschnitt "Clientdrucker" enthält Richtlinieneinstellungen für Clientdrucker, einschließlich solcher zur automatischen Erstellung von Clientdruckern, zum Speichern von Druckereigenschaften und zum Verbinden mit Druckservern.

Clientdrucker automatisch erstellen

Mit dieser Einstellung geben Sie die Clientdrucker an, die automatisch erstellt werden. Diese Einstellung überschreibt die Standardeinstellungen für die automatische Clientdruckererstellung.

Standardmäßig werden alle Clientdrucker automatisch erstellt.

Diese Einstellung gilt nur, wenn die Einstellung Clientdruckerumleitung vorhanden und Zugelassen ist.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, wählen Sie eine der Optionen:

- Mit Alle Clientdrucker automatisch erstellen werden alle Drucker auf dem Clientgerät erstellt.
- Mit Nur Standarddrucker des Clients automatisch erstellen wird der Drucker automatisch erstellt, der auf dem Clientgerät als Standarddrucker angegeben wurde.
- Mit Nur lokale Clientdrucker (keine Netzwerkdrucker) automatisch erstellen werden nur die Drucker automatisch erstellt, die über einen LPT-, COM-, USB-, TCP/IP- oder anderen lokalen Port direkt mit dem Clientgerät verbunden sind.
- Mit Clientdrucker nicht automatisch erstellen wird die automatische Erstellung von Clientdruckern beim Anmelden der Benutzer deaktiviert. Die Remotedesktopdienste-Einstellungen für die automatische Erstellung von Clientdruckern überschreiben dann diese Einstellung in Richtlinien mit niedrigerer Priorität.

Generischen universellen Drucker automatisch erstellen

Hinweis: Hotfixes für Probleme aufgrund dieser Richtlinieneinstellung sind in den Knowledge Center-Artikeln CTX141565 und CTX141566 verfügbar.
Mit dieser Einstellung aktivieren oder deaktivieren Sie die automatische Erstellung des generischen universellen Citrix Druckerobjekts für Sitzungen, in denen ein Benutzergerät verwendet wird, das mit der universellen Drucklösung kompatibel ist.

Standardmäßig wird das generische universelle Druckerobjekt nicht automatisch erstellt.

Die folgenden Richtlinieneinstellungen hängen zusammen:

- Verwendung universeller Druckertreiber
- Priorität universeller Treiber

Clientdruckernamen

Mit dieser Einstellung legen Sie die Namenskonvention für automatisch erstellte Drucker fest.

Standardmäßig werden die Standardnamen der Drucker verwendet.

Wählen Sie Standarddruckernamen, um Druckernamen im Format "HPLaserJet 4 von Clientname in Sitzung 3" zu verwenden.

Wählen Sie Legacydruckernamen, um Clientdruckernamen im alten Stil zuzulassen und die Rückwärtskompatibilität für Benutzer oder Gruppen zu erhalten, die MetaFrame Presentation Server 3.0 oder früher verwenden. Ein Beispiel für einen Legacydruckernamen ist "Client/clientname#/HPLaserJet 4". Diese Option ist weniger sicher.
Hinweis: Diese Option wird nur für Abwärtskompatibilität mit älteren Versionen von XenApp und XenDesktop bereitgestellt.

Direkte Verbindungen zu Druckservern

Mit dieser Einstellung aktivieren oder deaktivieren Sie direkte Verbindungen vom virtuellen Desktop oder Server, auf dem Anwendungen gehostet werden, zu einem Druckserver für Clientdrucker in einer zugänglichen Netzwerkfreigabe.

Standardmäßig sind direkte Verbindungen aktiviert.

Aktivieren Sie direkte Verbindungen, wenn der Netzwerkdruckserver für virtuelle Desktops bzw. für Server, auf denen Anwendungen gehostet werden, nicht über ein WAN zugänglich ist. Direkte Verbindungen gestatten schnelleres Drucken, wenn der Netzwerkdruckserver und der virtuelle Desktop oder Anwendungsserver sich im gleichen LAN befinden.

Deaktivieren Sie direkte Verbindungen, wenn das Netzwerk über ein WAN verläuft oder hohe Latenz oder beschränkte Bandbreite aufweist. Druckaufträge werden durch das Benutzergerät und den Netzwerkdruckserver geleitet. Daten werden komprimiert an das Benutzergerät gesendet, es wird somit weniger Bandbreite bei der Übertragung der Daten über das WAN gebraucht.

Wenn zwei Netzwerkdrucker den gleichen Namen haben, wird der Drucker benutzt, der im gleichen Netzwerk ist wie der Client.

Druckertreiberzuordnung und -kompatibilität

Mit dieser Einstellung legen Sie Regeln für die Treiberersetzung bei automatisch erstellten Druckern fest.

In der Standardeinstellung sind keine Regeln angegeben.

Wenn Sie Regeln für die Treiberersetzung definieren, können Sie zulassen oder verhindern, dass Drucker mit dem angegebenen Treiber erstellt werden. Außerdem können Sie für erstellte Drucker nur universelle Druckertreiber zulassen. Bei der Treiberersetzung werden die Namen der Druckertreiber, die das Benutzergerät bereitstellt, überschrieben oder zugeordnet und ein äquivalenter Treiber auf dem Server wird ersetzt. So können Serveranwendungen auf Clientdrucker zuzugreifen, die denselben Treiber wie der Server, aber unterschiedliche Treibernamen verwenden.

Sie können eine Treiberzuordnung hinzufügen, eine bestehende Zuordnung bearbeiten, benutzerdefinierte Einstellungen für eine Zuordnung überschreiben oder die Reihenfolge der Treibereinträge in der Liste ändern. Um eine Zuordnung hinzuzufügen, geben Sie den Clientdruckertreibernamen an und wählen dann den Ersatztreiber auf dem Server aus.

Speicherung von Druckereigenschaften

Mit dieser Einstellung geben Sie an, ob die Druckereigenschaften gespeichert werden und wo.

Standardmäßig ermittelt das System, ob Druckereigenschaften auf dem Clientgerät (falls verfügbar) gespeichert werden oder im Benutzerprofil.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, wählen Sie eine der Optionen:

- Wählen Sie Nur auf dem Clientgerät speichern, wenn Sie ein vorgeschriebenes oder servergespeichertes Profil verwenden, das nicht gespeichert wird. Wählen Sie diese Option nur aus, wenn auf allen Servern in der Farm XenApp 5 oder höher ausgeführt wird und die Benutzer die Citrix Online Plug-In-Versionen 9 bis 12.x oder Citrix Receiver 3.x verwenden.
- Wählen Sie Nur im Benutzerprofil speichern, wenn das System durch die Bandbreite (diese Option reduziert den Datenverkehr im Netzwerk) und die Anmeldegeschwindigkeit begrenzt ist oder die Benutzer Legacy-Plug-Ins verwenden. Bei dieser Option werden die Druckereigenschaften im Benutzerprofil auf dem Server gespeichert. Die Eigenschaften werden nicht mit dem Clientgerät ausgetauscht. Verwenden Sie diese Option für MetaFrame Presentation Server 3.0 oder früher und MetaFrame Presentation Server Client 8.x oder früher. Dies gilt nur, wenn ein servergespeichertes Profil für Remotedesktopdienste (RDS) verwendet wird.

- Mit Nur im Profil speichern, wenn sie nicht auf dem Client gespeichert sind kann das System festlegen, wo die Druckereigenschaften gespeichert werden. Die Druckereigenschaften werden auf dem Clientgerät gespeichert, sofern es verfügbar ist, ansonsten im Benutzerprofil. Diese Option bietet zwar die größte Flexibilität, kann jedoch die Anmeldezeit verlangsamen und zusätzliche Bandbreite für die Systemprüfung verbrauchen.
- Druckereigenschaften nicht speichern verhindert das Speichern von Druckereigenschaften.

Gespeicherte und wiederhergestellte Clientdrucker

Mit dieser Einstellung aktivieren oder deaktivieren Sie das Speichern und Neuerstellen von Clientdruckern. Standardmäßig werden Clientdrucker automatisch gespeichert und automatisch wiederhergestellt.

Gespeicherte Drucker sind vom Benutzer erstellte Drucker, die beim Start der nächsten Sitzung wiederhergestellt werden. Wenn XenApp einen gespeicherten Drucker wiederhergestellt, werden alle Richtlinieneinstellungen außer Clientdrucker automatisch erstellen berücksichtigt.

Gespeicherte Drucker sind Drucker die von einem Administrator vollständig angepasst wurden und deren gespeicherter Zustand permanent mit einem Clientport verbunden ist.

Einstellungen der Richtlinie "Treiber"

Feb 29, 2016

Der Abschnitt "Treiber" enthält Richtlinieneinstellungen für Druckertreiber.

Automatische Installation von mitgelieferten Druckertreibern

Mit dieser Einstellung aktivieren oder deaktivieren Sie die automatische Installation von Druckertreibern vom standardmäßigen Windows-Treibersatz oder von Treiberpaketen, die auf dem Host mit pnputil.exe /a bereitgestellt wurden.

Standardmäßig werden diese Treiber bei Bedarf installiert.

Priorität universeller Treiber

Mit dieser Einstellung geben Sie an, in welcher Reihenfolge die universellen Druckertreiber verwendet werden, angefangen mit dem ersten Eintrag in der Liste.

Standardmäßig ist die Prioritätsreihenfolge wie folgt:

- EMF
- XPS
- PCL5c
- PCL4
- PS

Sie können Treiber hinzufügen, bearbeiten oder entfernen und die Reihenfolge der Treiber in der Liste ändern.

Verwendung universeller Druckertreiber

Mit dieser Einstellung geben Sie an, wann universelles Drucken verwendet wird.

Standardmäßig wird universelles Drucken nur verwendet, wenn der angeforderte Treiber nicht verfügbar ist.

Universelles Drucken verwendet allgemeine Druckertreiber statt modellspezifischer Standardtreiber; dies verringert potentiell den Aufwand für die Treiberverwaltung auf Hostcomputern. Die Verfügbarkeit universeller Druckertreiber hängt von den Funktionen des Benutzergeräts, des Hosts und der Druckserversoftware ab. In bestimmten Konfigurationen steht universelles Drucken möglicherweise nicht zur Verfügung.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, wählen Sie eine der Optionen:

- Mit Nur druckermodellspezifische Treiber verwenden verwendet der Clientdrucker nur die modellspezifischen Standardtreiber, die bei der Anmeldung automatisch erstellt wurden. Wenn der erforderliche Treiber nicht verfügbar ist, kann der Clientdrucker nicht automatisch erstellt werden.
- Nur universelles Drucken verwenden gibt an, dass keine modellspezifischen Standardtreiber verwendet werden. Nur universelle Druckertreiber werden zum Erstellen von Druckern verwendet.
- Mit Universelles Drucken nur verwenden, wenn angeforderter Treiber nicht verfügbar ist werden modellspezifische Standardtreiber für die Druckererstellung verwendet, wenn sie verfügbar sind. Wenn der Treiber auf dem Server nicht zur Verfügung steht, wird der Clientdrucker automatisch mit dem entsprechenden universellen Treiber erstellt.
- Mit Druckermodellspezifische Treiber nur verwenden, wenn universelles Drucken nicht verfügbar ist werden universelle Druckertreiber verwendet, wenn sie verfügbar sind. Wenn der Treiber auf dem Server nicht zur Verfügung steht, wird der Clientdrucker automatisch mit dem entsprechenden modellspezifischen Druckertreiber erstellt.

Einstellungen der Richtlinie "Universeller Druckserver"

Feb 29, 2016

Der Abschnitt "Universeller Druckserver" enthält Richtlinieneinstellungen für die Behandlung des universellen Druckservers.

Universellen Druckserver aktivieren

Diese Einstellung aktiviert oder deaktiviert das Feature "Universeller Druckserver" auf dem virtuellen Desktop oder dem Server, auf dem Anwendungen gehostet werden. Wenden Sie die Richtlinie auf Organisationseinheiten an, die den virtuellen Desktop oder Server enthalten, auf dem Anwendungen gehostet werden.

Standardmäßig ist das Feature deaktiviert.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, wählen Sie eine der folgenden Optionen:

- **Aktiviert mit Fallback auf systemeigenen Windows-Remotedruck**: Netzwerkdruckerverbindungen werden nach Möglichkeit vom universellen Druckserver bedient. Wenn dieser nicht verfügbar ist, wird der Windows-Druckanbieter verwendet. Der Windows-Druckanbieter handhabt weiterhin alle Drucker, die vorher mit dem Windows-Druckanbieter erstellt wurden.
- **Aktiviert ohne Fallback auf systemeigenen Windows-Remotedruck**: Netzwerkdruckerverbindungen werden ausschließlich vom universellen Druckserver bedient. Wenn dieser nicht verfügbar ist, schlägt die Netzwerkdruckerverbindung fehl. Mit dieser Einstellung wird der Netzwerkdruck über den Windows-Druckanbieter effektiv deaktiviert. Drucker, die vorher mit dem Windows-Druckanbieter erstellt wurden, werden nicht erstellt, solange eine Richtlinie mit dieser Einstellung aktiv ist.
- **Deaktiviert**: Das Feature "Universeller Druckserver" ist deaktiviert. Beim Herstellen einer Verbindung mit einem Netzwerkdrucker, der einen UNC-Namen hat, wird keine Verbindung mit dem universellen Druckserver versucht. Verbindungen mit Remotedruckern verwenden weiterhin den Windows-Remotedruck.

Port für Druckdatenstrom des universellen Druckservers (CGP)

Diese Einstellung gibt die Nummer des TCP-Ports an, die vom Druckdatenstrom-Listener (CGP) des universellen Druckservers verwendet wird. Wenden Sie diese Richtlinie nur für Organisationseinheiten an, die den Druckserver enthalten.

Die Standardeinstellung der Portnummer ist "7229".

Gültige Portnummern müssen im Bereich von 1 bis 65535 liegen.

Universeller Druckserver - Eingabebandbreitenlimit für Druckdatenstrom (KBit/s)

Diese Einstellung gibt das obere Limit (in Kilobit pro Sekunde) für die Übertragungsrate der Druckdaten an, die von jedem Druckauftrag mit CGP an den universellen Druckserver übergeben werden. Wenden Sie die Richtlinie auf Organisationseinheiten an, die den virtuellen Desktop oder Server enthalten, auf dem Anwendungen gehostet werden.

In der Standardeinstellung ist der Wert 0, was angibt, dass es kein oberes Limit gibt.

Port für universellen Druckserverwebdienst (HTTP/SOAP)

Diese Einstellung gibt die Nummer des TCP-Ports an, die vom HTTP/SOAP-Webdienstlistener des universellen Druckservers verwendet wird. Der universelle Druckserver ist eine optionale Komponente, mit der die Verwendung universeller Druckertreiber von Citrix für den Netzwerkdruck ermöglicht wird. Wird der universelle Druckserver verwendet, werden die Druckbefehle von den XenApp- und XenDesktop-Hosts mit SOAP über HTTP an den universellen Druckserver gesendet.

Durch diese Einstellung ändert sich die Nummer des Standard-TCP-Ports, der vom Webdienstlistener des universellen Druckservers für eingehende HTTP/SOAP-Anforderungen überwacht wird.

Sie müssen den gleichen HTTP- Port für Host und Druckserver konfigurieren. Wenn Sie nicht den gleichen Port konfigurieren, stellt die Hostsoftware keine Verbindung mit dem universellen Druckserver her. Durch diese Einstellung ändert sich der VDA unter XenApp und XenDesktop. Außerdem müssen Sie den Standardport auf dem Computer mit dem universellen Druckserver ändern.

Die Standardeinstellung der Portnummer ist "8080".

Gültige Portnummern müssen im Bereich von 0 bis 65535 liegen.

Einstellungen der Richtlinie "Universelles Drucken"

Feb 29, 2016

Der Abschnitt "Universelles Drucken"" enthält Richtlinieneinstellungen für die Verwaltung des universellen Drucks.

Universelles Drucken - EMF-Verarbeitungsmodus

Mit dieser Einstellung steuern Sie die Verarbeitungsmethode für die EMF-Spooldatei auf dem Windows-Benutzergerät.

Standardmäßig werden EMF-Datensätze direkt zum Drucker gespoolt.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, wählen Sie eine der Optionen:

- EMF-Datensätze für Drucker neu verarbeiten erzwingt die Neuverarbeitung der EMF-Spooldatei und sendet sie durch das GDI-Teilsystem auf dem Benutzergerät. Sie können diese Einstellung für Treiber verwenden, für die eine EMF-Neuverarbeitung erforderlich ist, die jedoch nicht unbedingt in der Sitzung automatisch ausgewählt werden.
- Wenn Direkt zum Drucker spoolen mit dem universellen Citrix Druckertreiber verwendet wird, werden die EMF-Datensätze garantiert gespoolt und an das Benutzergerät für die Verarbeitung übergeben. Diese EMF-Spooldateien werden normalerweise direkt in die Spoolwarteschlange des Clients gesetzt. Für Drucker und Treiber, die mit dem EMF-Format kompatibel sind, ist dies die schnellste Druckmethode.

Universelles Drucken - Bildkomprimierungslimit

Mit dieser Einstellung geben Sie die maximale Qualität und minimale Komprimierung für Bilder an, die mit dem universellen Citrix Druckertreiber gedruckt werden.

Das Limit für Bildkomprimierung ist standardmäßig auf Beste Qualität (verlustfreie Komprimierung) gesetzt.

Wenn Keine Komprimierung ausgewählt ist, wird die Komprimierung nur für den EMF-Druck deaktiviert.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, wählen Sie eine der Optionen:

- Keine Komprimierung
- Beste Qualität (verlustfreie Komprimierung)
- Hohe Qualität
- Standardqualität
- Geringere Qualität (maximale Komprimierung)

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, die auch die Einstellung "Universelles Drucken - Optimierungsstandards" enthält, achten Sie auf Folgendes:

- Wenn die Komprimierungsstufe in der Einstellung Universelles Drucken - Komprimierungslimit niedriger ist als die in der Einstellung Universelles Drucken - Optimierungsstandards werden Bilder basierend auf der Einstellung Universelles Drucken - Bildkomprimierungslimit komprimiert.
- Wenn die Komprimierung deaktiviert ist, haben die Optionen Gewünschte Bildqualität und Heavyweight-Komprimierung aktivieren in der Einstellung Universelles Drucken - Optimierungsstandards keine Auswirkung in der Richtlinie.

Universelles Drucken - Optimierungsstandards

Mit dieser Einstellung geben Sie die Standardwerte für die Druckoptimierung an, wenn der universelle Druckertreiber für eine Sitzung erstellt wurde.

- Mit Gewünschte Bildqualität geben Sie das standardmäßige Bildkomprimierungslimit an, das auf universelles Drucken angewendet wird. In der Standardeinstellung ist Standardqualität aktiviert, d. h. Benutzer können Bilder nur mit der

Standardqualitäts- oder geringeren Qualitätskomprimierung drucken.
- Mit Heavyweight-Komprimierung aktivieren aktivieren oder deaktivieren Sie das Verringern der Bandbreite unter den Komprimierungsgrad, der von Gewünschte Bildqualität festgelegt ist; Bildqualität geht nicht verloren. Standardmäßig ist die Heavyweight-Komprimierung deaktiviert.
- Mit den Einstellungen Zwischenspeichern von Bildern und Schriftarten legen Sie fest, ob Bilder und Schriftarten, die mehrmals im Druckdatenstrom vorhanden sind, zwischengespeichert werden. Sie stellen damit sicher, dass jedes eindeutige Bild oder jede Schriftart nur einmal zum Drucker gesendet wird. Standardmäßig werden eingebettete Bilder und Schriftarten zwischengespeichert. Hinweis: Diese Einstellungen gelten nur, wenn das Benutzergerät dieses Verhalten unterstützt.
- Mit Nicht-Administratoren können diese Einstellungen ändern legen Sie fest, ob Benutzer die Standardeinstellungen für die Druckoptimierung in einer Sitzung ändern können. Standardmäßig können Benutzer die Standardeinstellungen für die Druckoptimierung nicht ändern.

Hinweis: Alle diese Optionen werden für den EMF-Druck unterstützt. Für XPS-Druck wird nur die Option Gewünschte Bildqualität unterstützt.
Wenn Sie diese Einstellung einer Richtlinie hinzufügen, die auch die Einstellung "Universelles Drucken - Optimierungsstandards" enthält, achten Sie auf Folgendes:
- Wenn die Komprimierungsstufe in der Einstellung Universelles Drucken - Komprimierungslimit niedriger ist als die in der Einstellung Universelles Drucken - Optimierungsstandards werden Bilder basierend auf der Einstellung Universelles Drucken - Bildkomprimierungslimit komprimiert.
- Wenn die Komprimierung deaktiviert ist, haben die Optionen Gewünschte Bildqualität und Heavyweight-Komprimierung aktivieren in der Einstellung Universelles Drucken - Optimierungsstandards keine Auswirkung in der Richtlinie.

Universelles Drucken - Vorschaueinstellung

Mit dieser Einstellung geben Sie an, ob die Druckvorschau für automatisch erstellte oder universelle Drucker verwendet werden soll.

Standardmäßig wird die Druckvorschau für automatisch erstellte oder generische universelle Drucker nicht verwendet.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, wählen Sie eine der Optionen:
- Druckvorschau für automatisch erstellte oder generische universelle Drucker nicht verwenden
- Druckervorschau nur für automatisch erstellte Drucker verwenden
- Druckvorschau nur für generische universelle Drucker verwenden
- Druckvorschau für automatisch erstellte und generische universelle Drucker verwenden

Universelles Drucken - Druckqualitätslimit

Diese Einstellung legt den Höchstwert für Punkte pro Zoll (dpi) zum Erstellen von Ausdrucken in einer Sitzung fest.

Standardmäßig ist Kein Limit aktiviert, d. h. Benutzer können die höchste Druckqualität auswählen, die vom Drucker zugelassen wird, mit dem sie eine Verbindung herstellen.

Wenn diese Einstellung konfiguriert ist, wird die maximale Druckqualität, die Benutzern zur Verfügung steht, hinsichtlich Ausgabeauflösung beschränkt. Sowohl die Druckqualität und die Druckqualitätsmerkmale des Druckers, mit dem sich die Benutzer verbinden, werden auf die konfigurierte Einstellung beschränkt. Beispiel: Wenn Mittlere Auflösung (600 dpi) konfiguriert ist, können Benutzer eine Ausgabe nur mit einer maximalen Qualität von 600 drucken, und die Einstellung "Druckqualität" auf der Registerkarte "Erweitert" im Dialogfeld "Universeller Drucker" enthält nur Auflösungseinstellungen bis zu "Mittlere Qualität (600 dpi).

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, wählen Sie eine der Optionen:

- Entwurf (150 dpi)
- Niedrige Auflösung (300 dpi)
- Mittlere Auflösung (600 dpi)
- Hohe Auflösung (1200 dpi)
- Kein Limit

Einstellungen der Richtlinie "Sicherheit"

Feb 29, 2016

Der Abschnitt "Sicherheit" enthält die Richtlinieneinstellung zum Konfigurieren der Sitzungsverschlüsselung und der Anmeldedatenverschlüsselung.

SecureICA-Mindestverschlüsselungsgrad

Mit dieser Einstellung geben Sie das Minimum für den Verschlüsselungsgrad der Sitzungsdaten an, die zwischen dem Server und einem Clientgerät ausgetauscht werden.

Wichtig: Bei Virtual Delivery Agent 7.x kann mit dieser Richtlinieneinstellung nur die Anmeldedatenverschlüsselung mit RC5 128-Bit-Verschlüsselung aktiviert werden. Die anderen Einstellungen werden nur für Abwärtskompatibilität mit älteren Versionen von XenApp und XenDesktop bereitgestellt.

Bei VDA 7.x wird die Sitzungsdatenverschlüsselung mit den Grundeinstellungen der Bereitstellungsgruppe des VDAs festgelegt. Wenn für die Bereitstellungsgruppe die Option "Secure ICA aktivieren" ausgewählt ist, werden Sitzungsdaten mit der RC5-Verschlüsselung (128 Bit) verschlüsselt. Wenn die Option "Secure ICA aktivieren" für die Bereitstellungsgruppe nicht ausgewählt ist, werden Sitzungsdaten mit der Basic-Verschlüsselung verschlüsselt.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, wählen Sie eine der Optionen:

- Basic verschlüsselt die Clientverbindung mit einem nicht RC5-konformen Algorithmus. Mit diesem Verschlüsselungsverfahren kann der Datenstrom zwar vor direktem Lesen geschützt werden, ein Entschlüsseln ist aber möglich. Standardmäßig verwendet der Server für den Client-Server-Netzwerkverkehr den Verschlüsselungsgrad "Basic".
- RC5 (128 Bit) nur Anmeldung verschlüsselt die Anmeldedaten mit der RC5-128-Bit-Verschlüsselung und die Clientverbindung mit dem Verschlüsselungsgrad "Basic".
- RC5 (40 Bit) verschlüsselt die Verbindung mit der RC5-40-Bit-Verschlüsselung.
- RC5 (56 Bit) verschlüsselt die Verbindung mit der RC5-56-Bit-Verschlüsselung.
- RC5 (128 Bit) verschlüsselt die Verbindung mit der RC5-128-Bit-Verschlüsselung.

Die Einstellungen, die Sie für die Verschlüsselung zwischen Client und Server festlegen, können mit Verschlüsselungseinstellungen des Windows-Betriebssystems interagieren. Wenn ein höherer Verschlüsselungsgrad auf dem Server oder Benutzergerät eingestellt ist, können Einstellungen überschrieben werden, die Sie für veröffentlichte Ressourcen angegeben haben.

Sie können den Verschlüsselungsgrad erhöhen, um die Kommunikation und Datenintegrität für bestimmte Benutzer stärker zu sichern. Wenn für eine Richtlinie ein höherer Verschlüsselungsgrad erforderlich ist, wird Citrix Receivern mit einem niedrigeren Verschlüsselungsgrad die Verbindung verweigert.

SecureICA führt keine Authentifizierung durch und prüft auch nicht die Datenintegrität. Verwenden Sie SecureICA mit TLS-Verschlüsselung, um eine vollständige Verschlüsselung für die Site bereitzustellen.

SecureICA verwendet nicht FIPS-konforme Algorithmen. Wenn dies ein Problem ist, konfigurieren Sie den Server und Citrix Receiver, um zu verhindern, dass SecureICA verwendet wird.

Einstellungen der Richtlinie "Serverlimits"

Feb 29, 2016

Der Abschnitt "Serverlimits" enthält die Richtlinieneinstellung zum Steuern von Sitzungen im Leerlauf.

Serverleerlauf-Zeitintervall

Mit dieser Einstellung geben Sie in Millisekunden an, wie lange eine ununterbrochene Benutzersitzung erhalten bleibt, wenn keine Benutzereingaben stattfinden.

Standardmäßig werden Leerlaufsitzungen nicht getrennt (Serverleerlaufzeitintervall = 0)

> ## 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. Dies ist ein MicrosoftDialogfeld, das nicht von Citrix Richtlinieneinstellungen gesteuert wird. Weitere Informationen finden Sie unter http://support.citrix.com/article/CTX118618.

Einstellungen der Richtlinie "Sitzungslimits"

Feb 29, 2016

Der Abschnitt "Sitzungslimits" enthält Richtlinieneinstellungen, mit denen Sie die Dauer der Sitzungen festlegen können, bevor diese getrennt werden.

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.

Standardmäßig werden getrennte Sitzungen nicht abgemeldet.

Getrennte Sitzungen - Timerintervall

Mit dieser Einstellung legen Sie fest, wie viele Minuten ein getrennter, gesperrter Desktop gesperrt bleibt, bevor die Sitzung abgemeldet wird.

Standardmäßig sind es 1440 Minuten (24 Stunden).

Sitzungsverbindungstimer

Mit dieser Einstellung aktivieren oder deaktivieren Sie einen Timer, mit dem die maximale Dauer einer ununterbrochenen Sitzung zwischen einem Benutzergerät und einem Desktop festgelegt wird.

Standardmäßig ist dieser Timer aktiviert.

Sitzungsverbindung - Timerintervall

Diese Einstellung legt die Höchstdauer einer ununterbrochenen Verbindung zwischen einem Benutzergerät und einem Desktop in Minuten fest.

Standardmäßig ist die maximale Dauer 1440 Minuten (24 Stunden).

Sitzungsleerlauftimer

Mit dieser Einstellung aktivieren oder deaktivieren Sie einen Timer, der angibt, wie lange eine ununterbrochene Benutzergeräteverbindung mit einem Desktop erhalten bleibt, wenn keine Benutzereingaben stattfinden.

Standardmäßig ist dieser Timer deaktiviert.

Sitzungsleerlauf - Timerintervall

Diese Einstellung legt fest, wie viele Minuten eine ununterbrochene Verbindung zwischen einem Benutzergerät und einem Desktop aufrechterhalten wird, wenn keine Eingabe vom Benutzer erfolgt.

Standardmäßig bleiben Leerlaufsitzungen 1440 Minuten (24 Stunden) erhalten.

Einstellungen der Richtlinie "Sitzungszuverlässigkeit"

Feb 29, 2016

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.

Standardmäßig ist die Sitzungszuverlässigkeit zugelassen.

Durch die Sitzungszuverlässigkeit bleiben Sitzungen aktiv und auf dem Bildschirm des Benutzers, wenn die Netzwerkverbindung unterbrochen wird. Die Benutzer sehen so lange weiterhin die Anwendung, die sie verwenden, bis die Netzwerkkonnektivität wiederhergestellt ist.

Mit der Sitzungszuverlässigkeit bleibt die Sitzung auf dem Server aktiv. Wenn die Netzwerkverbindung unterbrochen ist, friert der Bildschirm auf dem Client ein und der Mauszeiger wird als Sanduhr angezeigt, bis die Verbindung 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. Wenn Sie möchten, dass Benutzer eine Verbindung zu unterbrochenen Sitzungen nur mit einer Neuauthentifizierung wiederherstellen können, stellen Sie Authentifizierung bei automatischer Wiederverbindung von Clients entsprechend ein. Benutzer werden dann aufgefordert, sich neu zu authentifizieren, wenn sie sich mit der unterbrochenen Sitzung wiederverbinden.

Wenn Sie sowohl Sitzungszuverlässigkeit als auch die Funktion zur automatischen Wiederverbindung verwenden, werden beide Funktionen nacheinander ausgeführt. Die Sitzungszuverlässigkeit beendet oder trennt die Benutzersitzung, nachdem der mit der Option Sitzungszuverlässigkeit - Timeout festgelegte Zeitraum abgelaufen ist. Anschließend werden die Richtlinieneinstellungen für die automatische Wiederverbindung von Clients wirksam und es wird versucht, eine Verbindung mit der unterbrochenen Sitzung wiederherzustellen.

Sitzungszuverlässigkeit - Portnummer

Mit dieser Einstellung geben Sie die TCP-Portnummer für eingehende Sitzungszuverlässigkeitsverbindungen an.

Die Standardeinstellung der Portnummer ist "2598".

Sitzungszuverlässigkeit - Timeout

Mit dieser Einstellung legen Sie fest, wie viele Sekunden der Sitzungszuverlässigkeitsproxy auf die Wiederverbindung der Sitzung wartet, bevor die Sitzung getrennt wird.

Die Standardeinstellung ist 180 Sekunden (3 Minuten).

Sie können zwar eine Sitzung länger offen lassen, beachten Sie jedoch, dass Benutzer nicht zu einer Neuauthentifizierung auffordert werden, um den Bedienungskomfort zu erhöhen. Je länger eine Sitzung offen gelassen wird, desto höher ist das Risiko, dass der Benutzer abgelenkt wird und das Benutzergerät verlässt. Benutzer ohne Berechtigung hätten in dem Fall möglicherweise Zugriff auf die Sitzung.

Einstellungen der Richtlinie "Zeitzonensteuerung"

Feb 29, 2016

Der Abschnitt "Zeitzonensteuerung" enthält Richtlinieneinstellungen für die Zeitzone in Sitzungen.

Lokale Zeitzone für Legacyclients schätzen

Mit dieser Einstellung aktivieren oder deaktivieren Sie das Schätzen der lokalen Zeitzone auf Clientgeräten, die falsche Zeitzoneninformationen an den Server senden.

Standardmäßig schätzt der Server die lokale Zeitzone, wenn erforderlich.

Diese Einstellung ist für die Verwendung mit älteren Citrix Receiver-Versionen oder ICA- Clients vorgesehen, die keine detaillierten Zeitzoneninformationen an den Server senden. Bei Verwendung mit Citrix Receiver-Versionen, die detaillierte Zeitzoneninformationen an den Server senden, beispielsweise die unterstützten Versionen von Citrix Receiver für Windows, hat diese Einstellung keine Auswirkung.

Lokale Zeit des Clients verwenden

Mit dieser Einstellung legen Sie die Zeitzoneneinstellung der Benutzersitzung fest. Dies kann entweder die Zeitzone der Sitzung des Benutzers oder die des Benutzergeräts sein.

Standardmäßig wird die Zeitzone der Sitzung des Benutzers verwendet.

Damit diese Einstellung wirksam wird, aktivieren Sie die Einstellung Zeitzonenumleitung zulassen im Gruppenrichtlinien-Editor (Benutzerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Remotedesktopdienste > Remotedesktop-Sitzungshost > Remotesitzungsumgebung > Geräte- und Ressourcenumleitung).

Einstellungen der Richtlinie "TWAIN-Geräte"

Feb 29, 2016

Der Abschnitt "TWAIN-Geräte" enthält Richtlinieneinstellungen für die Zuordnung von TWAIN-Geräten, wie Digitalkameras oder Scanner, und für das Optimieren der Bildübertragung vom Server zum Client.

> **Hinweis**
>
> TWAIN 2.0 wird zurzeit nicht unterstützt.

TWAIN-Geräteumleitung für Client

Mit dieser Einstellung legen Sie fest, ob Benutzer auf TWAIN-Geräte auf dem Benutzergerät aus Bildverarbeitungsanwendungen auf Servern zugreifen können. Standardmäßig ist die TWAIN-Geräteumleitung zugelassen.

Die folgenden Richtlinieneinstellungen hängen zusammen:

- TWAIN-Komprimierungsgrad
- Bandbreitenlimit für TWAIN-Geräteumleitung
- Bandbreitenlimit für TWAIN-Geräteumleitung (Prozent)

TWAIN-Komprimierungsgrad

Mit dieser Einstellung geben Sie den Komprimierungsgrad für Bildübertragungen vom Client zum Server an. Verwenden Sie Gering für die beste Bildqualität, Mittel für eine gute Bilderqualität und Hoch für eine geringe Bildqualität. Standardmäßig wird die mittlere Komprimierung angewendet.

Einstellungen der Richtlinie "USB-Geräte"

Feb 29, 2016

Der Abschnitt "USB-Geräte" enthält Richtlinieneinstellungen für die Verwaltung der Dateiumleitung bei USB-Geräten.

Regeln für die Client-USB-Geräteoptimierung

Regeln für die Client-USB-Geräteoptimierung können auf Geräte angewendet werden, um die Optimierung zu deaktivieren oder den Optimierungsmodus zu ändern.

Wenn ein Benutzer ein USB-Gerät anschließt, prüft der Host, ob das Gerät gemäß den USB-Richtlinieneinstellungen zulässig ist. Ist das Gerät zulässig, prüft der Host die **Regeln für die Client-USB-Geräteoptimierung** für das Gerät. Wenn keine Regel angegeben ist, wird das Gerät im interaktiven Modus behandelt (02). Aufnahmemodus (04) ist der empfohlene Modus für Signaturgeräte. Eine Beschreibung der Modi finden Sie unten.

Gut zu wissen

- Für die Verwendung von Wacom Signatur-Tablets empfiehlt Citrix, dass Sie den Bildschirmschoner deaktivieren. Anweisungen hierzu finden Sie am Ende dieses Abschnitts.
- Unterstützung für die Optimierung von Wacom-Signatur-Tablets der STU-Reihe ist in der Installation von Richtlinien bei XenApp und XenDesktop vorkonfiguriert.
- Signaturgeräte funktionieren lückenlos in XenApp und XenDesktop und erfordern zur Verwendung als Signaturgerät keine Treiber. Wacom bietet zusätzliche Software an, die zur weiteren Anpassung des Geräts installiert werden kann. Informationen finden Sie unter http://www.wacom.com/.
- Grafiktablets: Bestimmte Grafik-Eingabegeräte werden als HID-Gerät an einem PCI/ACPI-Bus präsentiert und nicht unterstützt. Diese Geräte müssen an einen USB-Hostcontroller auf dem Client angeschlossen werden, damit sie innerhalb der XenDesktop-Sitzung umgeleitet werden.

Richtlinienregeln haben das Format von durch Leerzeichen getrennten Tag=Wert-Ausdrücken. Die folgenden Tags werden unterstützt:

Tagname	Beschreibung
Modus	Der Optimierungsmodus wird für Eingabegeräte der Klasse 3 (class=**03**) unterstützt. Unterstützte Modi: 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 vom Gerätedeskriptor
PID	Produkt-ID vom Gerätedeskriptor

REL	Release-ID vom Gerätedeskriptor
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=1230 PID=1230 class=03 (Eingabegerät im Erfassungsmodus)

Mode=00000002 VID=1230 PID=1230 class=03 (Eingabegerät im interaktiven Modus, Standardeinstellung)

Mode=00000001 VID=1230 PID=1230 class=03 (Eingabegerät ohne Optimierung)

Mode=00000100 VID=1230 PID=1230 (Setupoptimierung deaktiviert, Standardeinstellung)

Mode=00000200 VID=1230 PID=1230 (Setupoptimierung aktiviert)

Deaktivieren des Optimierungsmodus mittels einer Einstellung in der Registrierung

Der Optimierungsmodus kann systemweit über folgendes Registrierungskennzeichen deaktiviert werden:

HKLM\System\CurrentControlSet\Services\Icausbb\Parameters

DisableInputOptimization DWORD – Wert auf **1** festlegen

Es ist ein Systemneustart erforderlich, damit diese Änderung wirksam wird.

Deaktivieren des Bildschirmschoners für Wacom-Signatur-Tablets

Für die Verwendung von Wacom Signatur-Tablets sollten Sie den Bildschirmschoner wie folgt deaktivieren:

1. Installieren Sie den Wacom-STU-Treiber nach der Umleitung des Geräts.
2. Installieren Sie das Wacom-STU-Display-MSI, um Zugriff auf die Systemsteuerung des Signatur-Tablets zu erhalten.
3. Navigieren Sie zu **Control Panel > Wacom STU Display > STU430** oder **STU530** und wählen Sie die Registerkarte für das jeweilige Modell aus.
4. Klicken Sie auf **Change** und wählen Sie **Yes**, wenn das 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, kann das Gerät remote auf dem virtuellen Desktop verwendet werden. Ist es eine Verweigern-Regel, 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 einem Schnittstellendeskriptor
SubClass	Unterklasse vom Gerätedeskriptor oder ein Schnittstellendeskriptor
Prot	Protokoll vom Gerätedeskriptor oder ein Schnittstellendeskriptor

Wenn Sie neue Richtlinienregeln erstellen, beachten Sie Folgendes:

- Bei Regeln wird die Groß- und Kleinschreibung nicht berücksichtigt.
- Regeln können optional von einen Kommentar gefolgt werden, der mit # eingeleitet wird.
- Leere Zeilen und Kommentare werden ignoriert.
- Tags müssen den Übereinstimmungsoperator = verwenden, z. B. VID=1230.
- 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=1230 PID=0007 # Weitere Industrie, 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.

Einstellungen der Richtlinie "Visuelle Anzeige"

Feb 29, 2016

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

Ermöglicht die Verringerung der Farbtiefe für das Senden einfacher Grafiken auf **16 Bit pro Pixel**, was potenziell unter geringen Einbußen bei der Bildqualität die Reaktion bei Verbindungen mit geringer Bandbreite verbessert. Diese Option wird nur unterstützt, wenn kein Videocodec zum Komprimieren von Grafiken verwendet wird.

Die Standardeinstellung ist 24 Bit pro Pixel.

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.

Verwenden von Videocodec für die Komprimierung

Ermöglicht die Verwendung eines Videocodecs zum Komprimieren von Grafiken, wenn am Endpunkt eine Videodecodierung verfügbar ist. Ist am Endpunkt keine Videodecodierung verfügbar oder wenn Sie festlegen, dass kein Videocodec verwendet werden soll, wird eine Kombination aus Standbildkomprimierung und Bitmapcaching verwendet.

Die Standardeinstellung ist "Verwenden von Videocodec wenn verfügbar".

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**
- **Mittel**: bietet die beste Leistung und Bandbreiteneffizienz in den meisten Anwendungsfällen.
- **Hoch**: empfiehlt sich, wenn visuell verlustfreie Bildqualität gewünscht wird.
- **Zu verlustfrei verbessern**: sendet verlustreiche Bilder in Zeiträumen mit hoher Netzwerkaktivität und verlustfreie Bilder bei verringerter Netzwerkaktivität an das Benutzergerät. Mit dieser Einstellung wird die Leistung bei Netzwerkverbindungen mit beschränkter Bandbreite verbessert.
- **Immer verlustfrei**: In Situationen, in denen kein Qualitätsverlust akzeptabel ist (z. B. bei der Anzeige von Röntgenbildern), wählen Sie Immer verlustfrei, um sicherzustellen, dass keine verlustreichen Daten an das Benutzergerät gesendet werden.

Wenn die Einstellung **Legacygrafikmodus** aktiviert ist, hat die Einstellung **Bildqualität** keine Auswirkungen in der Richtlinie.

Einstellungen der Richtlinie "Bewegtbilder"

Feb 29, 2016

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 Diashows auf der Grundlage der verfügbaren Bandbreite automatisch an. Bei aktiviertem adaptivem Bildschirm werden Benutzern gleichmäßig ausgeführte Präsentationen ohne Qualitätseinbußen angezeigt. Standardmäßig ist der adaptive Bildschirm aktiviert.

Bei VDAs der Version 7.0 bis 7.6 gilt diese Einstellung nur, wenn der Legacygrafikmodus aktiviert ist. Bei VDAs ab Version 7.6 FP1 gilt diese Einstellung, wenn der Legacygrafikmodus aktiviert ist oder wenn der Legacygrafikmodus deaktiviert ist und kein Videocodec zum Komprimieren von Grafiken verwendet wird.

Wenn der Legacygrafikmodus aktiviert ist, muss die Sitzung neu gestartet werden, damit die Richtlinienänderungen wirksam werden. Adaptive Anzeige und progressive Anzeige schließen einander aus, d. h. durch Aktivieren der adaptiven Anzeige wird die progressive Anzeige deaktiviert und umgekehrt. Allerdings können progressive und adaptive Anzeige zur gleichen Zeit deaktiviert sein. Die progressive Anzeige wird als Legacyfeature für XenApp und XenDesktop nicht empfohlen. Durch Festlegen des Schwellenwerts für die progressive Komprimierung wird die adaptive Anzeige deaktiviert.

Grad der progressiven Komprimierung

Hinweis: Bei Virtual Delivery Agent 7.x gilt diese Richtlinieneinstellung nur, wenn die Richtlinieneinstellung Legacygrafikmodus aktiviert ist.
Mit dieser Einstellung wird zuerst ein weniger detailliertes Bild angezeigt, das dafür aber schneller dargestellt werden kann.

In der Standardeinstellung wird keine progressive Komprimierung angewendet.

Sobald es verfügbar ist, wird ein detailreicheres Bild anzeigt, das die normale Einstellung für verlustreiche Komprimierung verwendet. Verwenden Sie sehr hohe oder ultrahohe Komprimierung für die verbesserte Anzeige von bandbreitenintensiven Grafiken, wie etwa Fotografien.

Die progressive Komprimierung ist nur wirksam, wenn der Komprimierungsgrad höher ist als die Einstellung für Grad der verlustreichen Komprimierung.
Hinweis: Der stärkere Komprimierungsgrad für die progressive Komprimierung verbessert auch die Interaktivität von dynamischen Bildern über Clientverbindungen. Die Qualität eines dynamischen Bilds, z. B. ein sich drehendes dreidimensionales Modell, wird temporär verringert, bis das Bild stehen bleibt. Zu dem Zeitpunkt wird dann die reguläre

Einstellung der verlustreichen Komprimierung angewendet.
Die folgenden Richtlinieneinstellungen hängen zusammen:

- Schwellenwert für progressive Komprimierung
- Progressive Heavyweight-Komprimierung

Schwellenwert für progressive Komprimierung

Hinweis: Bei Virtual Delivery Agent 7.x gilt diese Richtlinieneinstellung nur, wenn die Richtlinieneinstellung Legacygrafikmodus aktiviert ist.
Mit dieser Einstellung geben Sie die maximale Bandbreite in Kilobits pro Sekunde für eine Verbindung an, auf die progressive Komprimierung angewendet wird. Die Komprimierung wird nur für Clientverbindungen unter diesem Bandbreitenwert verwendet.

Der Standardschwellenwert ist 2147483647 Kilobits pro Sekunde.

Die folgenden Richtlinieneinstellungen hängen zusammen:

- Schwellenwert für progressive Komprimierung
- Progressive Heavyweight-Komprimierung

Mindestframeratesollwert

Mit dieser Einstellung wird die Framerate pro Sekunde eingestellt, die das System für dynamische Bilder in Netzwerken mit geringer Bandbreite versucht beizubehalten.
Die Standardeinstellung für diesen Parameter ist 10 F/s.

Bei VDAs der Version 7.0 bis 7.6 gilt diese Einstellung nur, wenn der Legacygrafikmodus aktiviert ist. Bei VDAs ab Version 7.6 FP1 gilt diese Einstellung, wenn der Legacygrafikmodus deaktiviert oder aktiviert ist.

Einstellungen der Richtlinie "Standbilder"

Feb 29, 2016

Der Abschnitt "Standbilder" enthält Einstellungen, mit denen Sie die Komprimierung für statische Bilder entfernen oder ändern können.

Zusätzliche Farbkomprimierung

Mit dieser Einstellung aktivieren oder deaktivieren Sie die Verwendung der zusätzlichen Farbkomprimierung für Bilder, die über Clientverbindungen mit beschränkter Bandbreite bereitgestellt werden; dies verbessert die Reaktionszeit, da die Bilder in geringerer Qualität angezeigt werden.
Standardmäßig ist die zusätzliche Farbkomprimierung deaktiviert.

Bei Aktivierung wird die zusätzliche Farbkomprimierung nur angewendet, wenn die Bandbreite der Clientverbindung unter dem für Schwellenwert für zusätzliche Farbkomprimierung festgelegten Wert liegt. Wenn die Bandbreite der Clientverbindung über dem Schwellenwert liegt oder Deaktiviert ausgewählt ist, wird die zusätzliche Farbkomprimierung nicht angewendet.

Schwellenwert für zusätzliche Farbkomprimierung

Hinweis: Bei Virtual Delivery Agent 7.x gilt diese Richtlinieneinstellung nur, wenn die Richtlinieneinstellung Legacygrafikmodus aktiviert ist.
Mit dieser Einstellung geben Sie die maximale Bandbreite in Kilobits pro Sekunde für eine Verbindung an, unter der die zusätzliche Farbkomprimierung angewendet wird. Wenn die Bandbreite der Clientverbindung unter den eingestellten Wert abfällt, wird die zusätzliche Farbkomprimierung (falls aktiviert) angewendet.

Der Standardschwellenwert ist 8192 Kilobits pro Sekunde.

Heavyweight-Komprimierung

Hinweis: Bei Virtual Delivery Agent 7.x gilt diese Richtlinieneinstellung nur, wenn die Richtlinieneinstellung Legacygrafikmodus aktiviert ist.
Mit dieser Einstellung reduzieren Sie die erforderliche Bandbreite noch stärker als mit der progressiven Komprimierung, ohne dabei an Bildqualität zu verlieren, indem ein verbesserter grafischer Algorithmus verwendet wird, der aber mehr CPU beansprucht.

Standardmäßig ist die Heavyweight-Komprimierung deaktiviert.

Wenn die Heavyweight-Komprimierung aktiviert ist, gilt sie für alle verlustreichen Komprimierungen. Diese Einstellung wird von Citrix Receiver unterstützt, hat aber keine Auswirkung auf andere Plug-Ins.

Die folgenden Richtlinieneinstellungen hängen zusammen:
- Grad der progressiven Komprimierung
- Schwellenwert für progressive Komprimierung

Grad der verlustreichen Komprimierung

Hinweis: Bei Virtual Delivery Agent 7.x gilt diese Richtlinieneinstellung nur, wenn die Richtlinieneinstellung Legacygrafikmodus aktiviert ist.
Mit dieser Einstellung steuern Sie den Grad der verlustreichen Komprimierung, der für Grafiken verwendet wird, die über Clientverbindungen mit beschränkter Bandbreite bereitgestellt werden. In solchen Fällen kann die Anzeige von Bildern ohne

Komprimierung sehr langsam sein.

Standardmäßig wird eine mittlere Komprimierung ausgewählt.

Bessere Reaktionszeiten bei bandbreitenintensiven Bildern erzielen Sie mit hoher Komprimierung. In Fällen, in denen die Bilddaten erhalten bleiben müssen, beispielsweise bei der Anzeige von Röntgenbildern, wo kein Qualitätsverlust akzeptabel ist, sollten Sie die verlustreiche Komprimierung nicht einsetzen.

Verwandte Richtlinieneinstellung: Schwellenwert für verlustreiche Komprimierung

Schwellenwert für verlustreiche Komprimierung

Hinweis: Bei Virtual Delivery Agent 7.x gilt diese Richtlinieneinstellung nur, wenn die Richtlinieneinstellung Legacygrafikmodus aktiviert ist.
Mit dieser Einstellung geben Sie die maximale Bandbreite in Kilobits pro Sekunde für eine Verbindung an, auf die die verlustreiche Komprimierung angewendet wird.

Der Standardschwellenwert ist 2147483647 Kilobits pro Sekunde.

Wenn Sie die Einstellung Grad der verlustreichen Komprimierung einer Richtlinie hinzufügen, ohne einen Schwellenwert anzugeben, kann sich dadurch die Anzeigegeschwindigkeit für detailreiche Bitmaps, wie Fotografien, über ein LAN verbessern.

Verwandte Richtlinieneinstellung: Grad der verlustreichen Komprimierung

Einstellungen der Richtlinie "WebSockets"

Feb 29, 2016

Der Abschnitt "WebSockets" enthält Richtlinieneinstellungen für den Zugriff auf virtuelle Desktops und gehostete Anwendungen mit Citrix Receiver für HTML5. Das Feature WebSockets erhöht die Sicherheit und verringert die Last durch bidirektionale Kommunikation zwischen browserbasierten Anwendungen und Servern ohne Öffnen von mehreren HTTP-Verbindungen.

WebSockets-Verbindungen

Diese Einstellung lässt WebSockets-Verbindungen zu oder lehnt sie ab.

Standardmäßig sind WebSocket-Verbindungen nicht zulässig.

WebSockets-Portnummer

Mit dieser Einstellung wird der Port für eingehende WebSocket-Verbindungen festgelegt.

In der Standardeinstellung ist der Wert 8008.

Vertrauenswürdige WebSockets-Ursprungsserverliste

Diese Einstellung bietet eine durch Trennzeichen getrennte Liste der vertrauenswürdigen Ursprungsserver, normalerweise Citrix Receiver für Web, in Form von URLs. Nur WebSockets-Verbindungen, die von einer dieser Adressen stammen, werden vom Server akzeptiert.

Standardmäßig wird der Platzhalter * verwendet. Damit wird allen Citrix Receiver für Web-URLs vertraut.

Wenn Sie eine Adresse in die Liste eingeben möchten, verwenden Sie folgende Syntax:

<Protokoll>://<Vollqualifizierter Domänenname des Hosts>:[Port]

Das Protokoll muss HTTP oder HTTPS sein. Wenn der Port nicht angegeben wird, wird Port 80 für HTTP und Port 443 für HTTPS verwendet.

Der Platzhalter * kann innerhalb der URL verwendet werden, außer als Teil einer IP-Adresse (10.105. *. *).

Einstellungen der Richtlinie "Lastverwaltung"

Feb 29, 2016

Der Abschnitt "Lastverwaltung" enthält Richtlinieneinstellungen für das Aktivieren und Konfigurieren des Lastausgleichs zwischen Servern, über die Windows Server-Betriebssystemmaschinen bereitgestellt werden.

Weitere Informationen zum Berechnen des Lastauswertungsindex finden Sie unter CTX202150.

Toleranzwert für gleichzeitige Anmeldungen

Mit dieser Einstellung geben Sie die maximal zulässige Anzahl gleichzeitiger Anmeldungen bei einem Server an.

Die Standardeinstellung ist 2.

CPU-Nutzung

Mit dieser Einstellung geben Sie den Prozentsatz der CPU-Nutzung an, bei dem der Server Volllast meldet. Ist diese Einstellung aktiviert, beträgt der Standardwert, bei dem der Server Volllast meldet, 90 %.

Standardmäßig ist diese Einstellung deaktiviert und die CPU-Nutzung wird bei der Lastberechnung nicht berücksichtigt.

CPU-Nutzung ausschließlich Prozesspriorität

Mit dieser Einstellung geben Sie die Prioritätsstufe an, bei der die Prozess-CPU-Auslastung vom Lastindex der CPU-Nutzung ausgeschlossen wird.

Die Standardeinstellung ist "Unter normal oder niedrig".

Datenträgernutzung

Mit dieser Einstellung geben Sie die Länge der Datenträgerwarteschlange an, zu der der Server 75 % Volllast meldet. Der Standardwert dieser Einstellung ist 8.

Standardmäßig ist diese Einstellung deaktiviert und die Datenträgernutzung wird bei der Lastberechnung nicht berücksichtigt.

Sitzungshöchstanzahl

Mit dieser Einstellung geben Sie die maximale Anzahl von Sitzungen an, die von einem Server gehostet werden können. Ist die Einstellung aktiviert, beträgt der Standardwert für die maximale Anzahl Sitzungen an, die von einem Server gehostet werden können, 250.

Standardmäßig ist diese Einstellung aktiviert.

Speichernutzung

Mit dieser Einstellung geben Sie den Prozentsatz der Speichernutzung an, bei dem der Server Volllast meldet. Ist diese Einstellung aktiviert, beträgt der Standardwert, bei dem der Server Volllast meldet, 90 %.

Standardmäßig ist diese Einstellung deaktiviert und die Speichernutzung wird bei der Lastberechnung nicht berücksichtigt.

Speichernutzung - Ausgangslast

Mit dieser Einstellung geben Sie einen Näherungswert der Speichernutzung durch das Basisbetriebssystem in MB an, unterhalb dessen die Speichernutzung bei einem Server als Nulllast interpretiert wird.

Der Standardwert dieser Einstellung ist 768 MB.

Einstellungen der Richtlinie "Profilverwaltung"

Feb 29, 2016

Der Abschnitt "Profilverwaltung" enthält Richtlinieneinstellungen zum Aktivieren der Profilverwaltung und zum Konfigurieren der Gruppen, die in die Verarbeitung der Profilverwaltung eingeschlossen bzw. ausgeschlossen werden sollen.

Weitere Informationen, wie die Namen der entsprechenden INI-Dateieinstellungen und die für eine Richtlinieneinstellung erforderliche Version der Profilverwaltung, finden Sie unter Profilverwaltungsrichtlinien.

Einstellungen der Richtlinie "Erweitert"

Feb 29, 2016

Der Abschnitt "Erweitert" enthält Richtlinieneinstellungen für die erweiterte Konfiguration der Profilverwaltung.

Automatische Konfiguration deaktivieren

Mit dieser Einstellung legen Sie fest, dass die Umgebung von der Profilverwaltung untersucht werden kann, z. B., um zu überprüfen, ob persönliche vDisks vorhanden sind, und um die Gruppenrichtlinie entsprechend zu konfigurieren. Nur Richtlinien für die Profilverwaltung mit dem Status "Nicht konfiguriert" werden angepasst, sodass alle zuvor vorgenommenen Anpassungen beibehalten werden. Dieses Feature beschleunigt die Bereitstellung und vereinfacht die Optimierung. Es ist keine Konfiguration des Features ist erforderlich aber Sie können die automatische Konfiguration bei Upgrades (zum Beibehalten der Einstellungen von früheren Versionen) oder bei der Problembehandlung deaktivieren. Die automatische Konfiguration funktioniert in XenApp oder anderen Umgebungen nicht.

In der Standardeinstellung ist die automatische Konfiguration zugelassen.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, wird die automatische Konfiguration aktiviert. Einstellungen der Profilverwaltung können sich dann möglicherweise ändern, wenn sich die Umgebung ändert.

Benutzer bei Problem abmelden

Mit dieser Einstellung wird eine Abmeldung eines Benutzers durch die Profilverwaltung ermöglicht, wenn ein Problem auftritt, z. B. wenn der Benutzerspeicher nicht verfügbar ist. Wenn diese Einstellung aktiviert ist, wird dem Benutzer eine Fehlermeldung angezeigt, bevor er abgemeldet wird. Wenn diese Einstellung deaktiviert ist, erhalten Benutzer ein temporäres Profil.

Standardmäßig ist diese Einstellung deaktiviert und Benutzer erhalten ein temporäres Profil, wenn ein Problem auftritt.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, wird ein temporäres Profil bereitgestellt.

Anzahl Wiederholungen beim Zugriff auf gesperrte Dateien

Mit dieser Einstellung geben Sie die Anzahl der Zugriffsversuche auf gesperrte Dateien durch die Profilverwaltung an.

Der Standardwert dieser Einstellung ist fünf Versuche.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, wird der Standardwert verwendet.

Internet-Cookiedateien bei Abmeldung verarbeiten

Mit dieser Einstellung legen Sie fest, dass die Datei index.dat beim Abmelden von der Profilverwaltung verarbeitet werden kann, damit Internet-Cookies im Dateisystem nach längerem Browsen entfernt werden. Auf diese Weise wird eine Aufblähung von Profilen vermieden. Eine Aktivierung der Einstellung verlängert die Abmeldezeiten. Aktivieren Sie sie daher nur, wenn das entsprechende Problem bei Ihnen auftritt.

Standardmäßig ist diese Einstellung deaktiviert und die Profilverwaltung verarbeitet die Datei index.dat beim Abmelden nicht.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, wird Index.dat nicht verarbeitet.

Grundlegende Richtlinieneinstellungen

Feb 29, 2016

Der Abschnitt "Grundlegend" enthält Richtlinieneinstellungen für die grundlegende Konfiguration der Profilverwaltung.

Aktiv zurückschreiben

Mit dieser Einstellung können geänderte Dateien und Ordner (aber keine Registrierungseinträge) während einer Sitzung mit dem Benutzerspeicher synchronisiert werden bevor die Abmeldung erfolgt.

Standardmäßig ist die Synchronisierung mit dem Benutzerspeicher während laufender Sitzungen deaktiviert.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, ist sie aktiviert.

Profilverwaltung aktivieren

Mit dieser Einstellung wird die Profilverwaltung zur Verarbeitung von An- und Abmeldungen aktiviert.

Standardmäßig ist diese Einstellung deaktiviert, um die Bereitstellung zu vereinfachen.

Wichtig: Citrix empfiehlt, eine Aktivierung der Profilverwaltung erst dann durchzuführen, wenn alle anderen Setupaufgaben ausgeführt wurden und getestet wurde, wie sich Citrix Benutzerprofile in der Umgebung verhalten.
Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, verarbeitet die Profilverwaltung keine Windows-Benutzerprofile.

Ausgeschlossene Gruppen

Mit dieser Einstellung geben Sie an, welche lokalen Computergruppen und welche Domänengruppen (lokale, globale und universelle) nicht von der Profilverwaltung verarbeitet werden sollen.

Wenn diese Option aktiviert ist, verarbeitet die Profilverwaltung keine Mitglieder der angegebenen Benutzergruppen.

Standardmäßig ist diese Einstellung deaktiviert und Mitglieder aller Benutzergruppen werden verarbeitet.

Geben Sie Domänengruppen im Format <DOMÄNENNAME>\<GRUPPENNAME> an.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden Mitglieder aller Benutzergruppen verarbeitet.

Unterstützung von Offlineprofilen

Mit dieser Einstellung wird die Unterstützung von Offlineprofilen aktiviert, durch die Profile nach einer Unterbrechung der Verbindung mit dem Netzwerk zum frühestmöglichen Zeitpunkt mit dem Benutzerspeicher synchronisiert werden.

Standardmäßig ist die Unterstützung von Offlineprofilen deaktiviert.

Diese Einstellung gilt für Benutzer von Laptops und mobile Benutzer im Roamingmodus. Wenn die Verbindung zum

Netzwerk unterbrochen wird, bleiben die Profile auf dem Laptop oder Gerät intakt, selbst wenn das Gerät neu gestartet wird oder im Ruhezustand gewesen ist. Während mobile Benutzer arbeiten, werden ihre Profile lokal aktualisiert und am Ende mit dem Benutzerspeicher synchronisiert, wenn die Netzwerkverbindung wiederhergestellt ist.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, ist die Unterstützung von Offlineprofilen deaktiviert.

Pfad zum Benutzerspeicher

Mit dieser Einstellung geben Sie den Pfad zu dem Verzeichnis (Benutzerspeicher) an, in dem Benutzereinstellungen, z. B. Registrierungseinstellungen und synchronisierte Dateien, gespeichert werden.

Standardmäßig wird das Windows-Verzeichnis auf dem Basislaufwerk verwendet.

Wenn diese Einstellung deaktiviert ist, werden die Benutzereinstellungen im Windows-Unterverzeichnis des Basisverzeichnisses gespeichert.

Mögliche Pfade:
- **Relativer Pfad**: Dieser Pfad muss relativ zum Basisverzeichnis sein. Dieses ist normalerweise mit dem Attribut #homeDirectory# für einen Benutzer in Active Directory konfiguriert.
- **Absoluter UNC-Pfad**: Hiermit wird üblicherweise eine Serverfreigabe oder ein DFS-Namespace angegeben.
- **Deaktiviert oder nicht konfiguriert**: In diesem Fall wird als Wert #homeDirectory#\Windows angenommen.

Verwenden Sie die folgenden Variablentypen beim Konfigurieren dieser Richtlinieneinstellung:
- Systemumgebungsvariablen in Prozentzeichen (z. B. %ProfVer%). Beachten Sie, dass Systemumgebungsvariablen normalerweise weitere Einrichtung erfordern.
- Attribute des Active Directory-Benutzerobjekts in Rauten (z. B. #sAMAccountName#).
- Profilverwaltungsvariablen. Weitere Informationen finden Sie in der Dokumentation zur Profilverwaltung.

Sie können auch mit den Benutzerumgebungsvariablen %username% und %userdomain% benutzerdefinierte Attribute erstellen, um Organisationsvariablen wie Standort und Benutzer vollständig zu definieren. Bei Attributen muss Groß- und Kleinschreibung beachtet werden.

Beispiele:
- \\Server\Freigabe\#sAMAccountName# speichert die Benutzereinstellungen unter dem UNC-Pfad \\Server\Freigabe\KurtMeier (wenn #sAMAccountName# zu Kurt Meier als aktuellem Benutzer aufgelöst wird).
- \\server\profiles$\%USERNAME%.%USERDOMAIN%\!CTX_PROFILEVER!!CTX_OSBITNESS! kann erweitert werden zu \\server\profiles$\JohnSmith.DOMAINCONTROLLER1\v2x64

Wichtig: Unabhängig davon, welche Attribute oder Variablen Sie verwenden, müssen Sie sicherstellen, dass diese Einstellung zu einem Ordner über dem Ordner, der NTUSER.DAT enthält, aufgelöst wird. Wenn sich diese Datei z. B. in \\Server\profiles$\KurtMeier.BuHa\v2x64\UPM_Profile befindet, geben Sie den Pfad zum Benutzerspeicher als \\Server\profiles$\KurtMeier.BuHa\v2x64 an (ohne den Unterordner \UPM_Profile) an.
Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, wird das Windows-Verzeichnis auf dem Basislaufwerk verwendet.

Anmeldungen lokaler Administratoren verarbeiten

Mit dieser Einstellung wird angegeben, ob Anmeldungen von Mitgliedern der Gruppe "BUILTIN\Administrators" verarbeitet

werden. Dies ermöglicht es Domänenbenutzern mit lokalen Administratorrechten, d. h. normalerweise Benutzer mit zugewiesenen virtuellen Desktops, die Verarbeitung zu umgehen, sich anzumelden und Probleme mit der Profilverwaltung bei einem Desktop zu behandeln.

Wenn diese Einstellung unter Serverbetriebssystemen deaktiviert oder nicht konfiguriert ist, nimmt die Profilverwaltung an, dass Anmeldungen von Domänenbenutzern, aber nicht von lokalen Administratoren, verarbeitet werden müssen. Unter Desktopbetriebssystemen werden Anmeldungen lokaler Administratoren verarbeitet.

Diese Einstellung ist standardmäßig deaktiviert und Anmeldungen lokaler Administratoren werden nicht verarbeitet.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden Anmeldungen lokaler Administratoren nicht verarbeitet.

Verarbeitete Gruppen

Mit dieser Einstellung geben Sie an, welche lokalen Computergruppen und welche Domänengruppen (lokale, globale und universelle) von der Profilverwaltung verarbeitet werden sollen.

Wenn diese Option aktiviert ist, verarbeitet die Profilverwaltung nur Mitglieder der angegebenen Benutzergruppen.

Standardmäßig ist diese Einstellung deaktiviert und Mitglieder aller Benutzergruppen werden verarbeitet.

Geben Sie Domänengruppen im Format <DOMÄNENNAME>\<GRUPPENNAME> an.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden Mitglieder aller Benutzergruppen verarbeitet.

Plattformübergreifende Richtlinieneinstellungen

Feb 29, 2016

Der Abschnitt "Plattformübergreifende Einstellungen" enthält Richtlinieneinstellungen für die Konfiguration der plattformübergreifenden Einstellungen der Profilverwaltung.

Benutzergruppen für plattformübergreifende Einstellungen

Mit dieser Einstellung geben Sie die Benutzergruppen an, deren Profile verarbeitet werden sollen, wenn das Feature für plattformübergreifende Einstellungen aktiviert ist.

Standardmäßig ist diese Einstellung deaktiviert und alle Benutzergruppen in der Richtlinieneinstellung Verarbeitete Gruppen werden verarbeitet.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden alle Benutzergruppen verarbeitet.

Plattformübergreifende Einstellungen aktivieren

Mit dieser Einstellung aktivieren oder deaktivieren Sie das Feature "Plattformübergreifende Einstellungen". Dieses ermöglicht das Migrieren und Roamen von Benutzerprofilen, wenn ein Benutzer eine Verbindung mit einer Anwendung herstellt, die unter mehreren Betriebssystemen ausgeführt wird.

Standardmäßig ist das Feature "Plattformübergreifende Einstellungen" deaktiviert.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden keine plattformübergreifenden Einstellungen angewendet.

Pfad zu plattformübergreifenden Definitionen

Mit dieser Einstellung geben Sie in Form eines UNC-Pfads den Netzwerkspeicherort an, der die aus dem Downloadpaket kopierten Definitionsdateien enthält.

Hinweis: Benutzer benötigen Lesezugriff und Administratoren Schreibzugriff auf diesen Speicherort, bei dem es sich entweder um eine Server Message Block-Dateifreigabe (SMB) oder eine Common Internet File System-Dateifreigabe (CIFS) handeln muss.
In der Standardeinstellung ist kein Pfad angegeben.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden keine plattformübergreifenden Einstellungen angewendet.

Pfad zum Speicher für plattformübergreifende Einstellungen

Diese Einstellung gibt den Pfad zum Speicher für plattformübergreifende Einstellungen an. Hier werden die plattformübergreifenden Einstellungen der Benutzer gespeichert. Der Pfad kann ein UNC-Pfad oder ein relativer Pfad zum Basisverzeichnis sein.

Hinweis: Benutzer müssen über Schreibzugriff auf den Speicher für plattformübergreifende Einstellungen verfügen. Standardmäßig ist diese Einstellung deaktiviert und der Pfad "Windows\PM_CP" wird verwendet.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, wird der Standardwert verwendet.

Quelle für plattformübergreifende Einstellungen

Mit dieser Einstellung legen Sie eine Plattform als Basisplattform fest, wenn die entsprechende Einstellung für die Organisationseinheit der Plattform aktiviert ist. Daten von den Profilen der Basisplattform werden in den Speicher für plattformübergreifende Einstellungen migriert.

Die Profile jeder Plattform werden in einer separaten Organisationseinheit gespeichert. Dies bedeutet, dass Sie die Plattform auswählen müssen, deren Profildaten zum Füllen des Speichers für plattformübergreifende Einstellungen verwendet werden sollen. Dies wird als Basisplattform bezeichnet.

Wenn diese Option aktiviert ist, migriert die Profilverwaltung die Daten des Einzelplattformprofils in den Speicher, wenn der Speicher für plattformübergreifende Einstellungen eine Definitionsdatei ohne Daten enthält oder die zwischengespeicherten Daten eines Einzelplattformprofils neuer sind als die Definitionsdaten im Speicher.

Wichtig: Wenn diese Einstellung in mehreren Organisationseinheiten für mehrere Benutzer oder Maschinenobjekte aktiviert ist, wird die Plattform, bei der sich der erste Benutzer anmeldet, zum Basisprofil.
Standardmäßig ist diese Einstellung deaktiviert und die Profilverwaltung migriert die Daten des Einzelplattformprofils nicht in den Speicher.

Einstellungen der Richtlinie "Dateisystem"

Feb 29, 2016

Der Abschnitt "Dateisystem" enthält Richtlinieneinstellungen zum Angeben der Dateien und Verzeichnisse in einem Benutzerprofil, die zwischen dem System, auf dem das Profil installiert ist, und dem Benutzerspeicher synchronisiert werden sollen.

Einstellungen der Richtlinie "Ausschlüsse"

Feb 29, 2016

Der Abschnitt "Ausschlüsse" enthält Richtlinieneinstellungen zum Konfigurieren der Dateien und Verzeichnisse in einem Benutzerprofil, die von der Synchronisierung ausgeschlossen werden sollen.

Ausschlussliste - Verzeichnisse

Mit dieser Einstellung geben Sie eine Liste der Ordner im Benutzerprofil an, die bei der Synchronisierung ignoriert werden sollen.

Geben Sie die Ordnernamen als Pfad relativ zum Benutzerprofil (% USERPROFILE%) an.

Standardmäßig ist diese Einstellung deaktiviert und alle Ordner in Benutzerprofilen werden synchronisiert.

Beispiel: Desktop ignoriert den Ordner "Desktop" im Benutzerprofil.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden alle Ordner im Benutzerprofil synchronisiert.

Ausschlussliste - Dateien

Mit dieser Einstellung geben Sie eine Liste der Dateien im Benutzerprofil an, die bei der Synchronisierung ignoriert werden sollen.

Standardmäßig ist diese Einstellung deaktiviert und alle Dateien in Benutzerprofilen werden synchronisiert.

Geben Sie die Dateinamen als Pfad relativ zum Benutzerprofil (% USERPROFILE%) an. Hinweis: Platzhalter sind zulässig und werden rekursiv angewendet.

Beispiel: "Desktop\Desktop.ini" ignoriert die Datei Desktop.ini im Verzeichnis "Desktop".

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden alle Dateien im Benutzerprofil synchronisiert.

Einstellungen der Richtlinie "Synchronisierung"

Feb 29, 2016

Der Abschnitt "Synchronisierung" enthält Richtlinieneinstellungen für die Angabe, welche Dateien und Ordner in einem Benutzerprofil zwischen dem System, auf dem das Profil installiert ist, und dem Benutzerspeicher synchronisiert werden.

Zu synchronisierende Verzeichnisse

Diese Einstellung gibt die Dateien an, die sich in ausgeschlossenen Ordnern befinden und von der Profilverwaltung in die Synchronisierung eingeschlossen werden sollen. Standardmäßig synchronisiert die Profilverwaltung alle Elemente im Benutzerprofil. Es ist nicht erforderlich, Unterordner des Benutzerprofils einzuschließen, indem Sie sie dieser Liste hinzufügen. Weitere Informationen finden Sie unter Aufnehmen und Ausschließen von Objekten.

Pfade in dieser Liste müssen relativ zum Benutzerprofil sein.

Beispiel: "Desktop\ausschließen\aufnehmen" stellt sicher, dass der Unterordner "aufnehmen" synchronisiert wird, selbst wenn das Verzeichnis "Desktop\ausschließen" nicht synchronisiert wird.

Standardmäßig ist diese Einstellung deaktiviert und keine Ordner sind angegeben.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden nur nicht ausgeschlossene Ordner im Benutzerprofil synchronisiert.

Zu synchronisierende Dateien

Diese Einstellung gibt die Dateien an, die sich in ausgeschlossenen Ordnern befinden und von der Profilverwaltung in die Synchronisierung eingeschlossen werden sollen. Standardmäßig synchronisiert die Profilverwaltung alle Elemente im Benutzerprofil. Es ist nicht erforderlich, Dateien in dem Benutzerprofil einzuschließen, indem Sie sie dieser Liste hinzufügen. Weitere Informationen finden Sie unter Aufnehmen und Ausschließen von Objekten.

Pfade in dieser Liste müssen relativ zum Benutzerprofil sein. Relative Pfade werden als relativ zum Benutzerprofil interpretiert. Platzhalter können nur für Dateinamen verwendet werden. Platzhalter können nicht verschachtelt werden und werden rekursiv angewendet.

Beispiele:

- Anwendungsdaten\Lokal\Microsoft\Office\Access.qat gibt eine Datei unter einem Ordner an, der in der Standardkonfiguration ausgeschlossen wurde.
- Anwendungsdaten\Lokal\Anwendungen*.cfg gibt alle Dateien mit der Erweiterung .cfg im Profilordner Anwendungsdaten\Lokal\Anwendungen und dessen Unterordnern an.

Standardmäßig ist diese Einstellung deaktiviert und keine Dateien sind angegeben.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden nur nicht ausgeschlossene Dateien im Benutzerprofil synchronisiert.

Zu spiegelnde Ordner

Mit dieser Einstellung geben Sie an, welche Ordner relativ zum Stammordner eines Benutzerprofils gespiegelt werden sollen. Diese Richtlinie kann beim Lösen von Problemen bei Transaktionsordnern (auch "Referenzordner" genannt) helfen. Dies sind Ordner, die voneinander abhängige Dateien enthalten, wobei eine Datei Verweise auf andere Dateien enthält.

Durch das Spiegeln von Ordnern kann die Profilverwaltung einen Transaktionsordner und seinen Inhalt als eine Entität verarbeiten. So wird das Aufblähen von Profilen verhindert. Beachten Sie, dass in solchen Situationen der "letzte Schreibvorgang Priorität hat", d. h. dass Dateien in gespiegelten Ordnern, die in mehr als einer Sitzung geändert wurden, von der letzten Aktualisierung überschrieben werden. Hierdurch gehen Profiländerungen verloren.

Sie können z. B. den Cookies-Ordner von Internet Explorer spiegeln, damit Index.dat mit den Cookies synchronisiert wird, auf die die Datei verweist.

Wenn ein Benutzer zwei Internet Explorer-Sitzungen auf unterschiedlichen Servern hat und er in jeder Sitzung auf andere Websites zugreift, werden Cookies dieser Sites auf dem entsprechenden Server hinzugefügt. Wenn sich der Benutzer von der ersten Sitzung abmeldet (oder auch mitten in der Sitzung, wenn das Feature für aktives Zurückschreiben konfiguriert ist), sollten die Cookies der zweiten Sitzung die Cookies der ersten Sitzung ersetzen. Stattdessen werden sie jedoch zusammengeführt und die Verweise auf die Cookies in Index.dat sind infolgedessen veraltet. Weiteres Browsen in neuen Sitzungen kann zum wiederholten Zusammenführen und einem aufgeblähten Cookie-Ordner führen.

Durch Spiegeln des Cookie-Ordners wird dieses Problem gelöst, indem Cookies, jedes Mal wenn der Benutzer sich abmeldet, mit denen der letzten Sitzung überschrieben werden. So bleibt Index.dat aktuell.

Standardmäßig ist diese Einstellung deaktiviert und es werden keine Ordner gespiegelt.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Richtlinie weder hier noch in der INI-Datei konfiguriert ist, werden keine Ordner gespiegelt.

Einstellungen der Richtlinie "Ordnerumleitung"

Feb 29, 2016

Der Abschnitt "Ordnerumleitung" enthält Richtlinieneinstellungen für die Angabe, ob häufig in Profilen erscheinende Ordner an einen freigegebenen Speicherort im Netzwerk umgeleitet werden sollen.

Administratorzugriff gewähren

Diese Einstellung ermöglicht einem Administrator den Zugriff auf den Inhalt von umgeleiteten Ordnern der Benutzer.

Diese Einstellung ist standardmäßig deaktiviert und es haben ausschließlich Benutzer Zugriff auf den Inhalt ihrer umgeleiteten Ordner.

Domänennamen einschließen

Diese Einstellung ermöglicht die Verwendung der Umgebungsvariablen %userdomain% als Teil des für umgeleitete Ordner angegebenen UNC-Pfads.

Standardmäßig ist diese Einstellung deaktiviert und die Umgebungsvariable %userdomain% ist nicht Teil der UNC-Pfad-Angabe für umgeleitete Ordner.

Einstellungen der Richtlinie "AppData(Roaming)"

Feb 29, 2016

Der Abschnitt "AppData(Roaming)" enthält Richtlinieneinstellungen für die Angabe, ob der Inhalt des Ordners "AppData(Roaming)" an einen freigegebenen Speicherort im Netzwerk umgeleitet werden soll.

AppData(Roaming)-Pfad

Mit dieser Einstellung geben Sie den Netzwerkspeicherort an, zu dem der Inhalt des Ordners "AppData(Roaming)" umgeleitet werden soll.

Standardmäßig ist diese Einstellung deaktiviert und kein Speicherort wird angegeben.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

Umleitungseinstellungen für AppData(Roaming)

Mit dieser Einstellung geben Sie an, wie der Inhalt des Ordners "AppData(Roaming)" umgeleitet werden soll.

Standardmäßig erfolgt die Umleitung an einen UNC-Pfad.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

Einstellungen der Richtlinie "Kontakte"

Feb 29, 2016

Der Abschnitt "Kontakte" enthält Richtlinieneinstellungen für die Angabe, ob der Inhalt des Ordners "Kontakte" an einen freigegebenen Speicherort im Netzwerk umgeleitet werden soll.

'Kontakte'-Pfad

Mit dieser Einstellung geben Sie den Netzwerkspeicherort an, zu dem der Inhalt des Ordners "Kontakte" umgeleitet werden soll.

Standardmäßig ist diese Einstellung deaktiviert und kein Speicherort wird angegeben.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

Umleitungseinstellungen für 'Kontakte'

Mit dieser Einstellung geben Sie an, wie der Inhalt des Ordners "Kontakte" umgeleitet werden soll.

Standardmäßig erfolgt die Umleitung an einen UNC-Pfad.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

Einstellungen der Richtlinie "Desktop"

Feb 29, 2016

Der Abschnitt "Desktop" enthält Richtlinieneinstellungen für die Angabe, ob der Inhalt des Ordners "Desktop" an einen freigegebenen Speicherort im Netzwerk umgeleitet werden soll.

'Desktop'-Pfad

Mit dieser Einstellung geben Sie den Netzwerkspeicherort an, zu dem der Inhalt des Ordners "Desktop" umgeleitet werden soll.

Standardmäßig ist diese Einstellung deaktiviert und kein Speicherort wird angegeben.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

Umleitungseinstellungen für 'Desktop'

Mit dieser Einstellung geben Sie an, wie der Inhalt des Ordners "Desktop" umgeleitet werden soll.

Standardmäßig erfolgt die Umleitung an einen UNC-Pfad.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

Einstellungen der Richtlinie "Dokumente"

Feb 29, 2016

Der Abschnitt "Dokumente" enthält Richtlinieneinstellungen für die Angabe, ob der Inhalt des Ordners "Dokumente" an einen freigegebenen Speicherort im Netzwerk umgeleitet werden soll.

'Dokumente'-Pfad

Mit dieser Einstellung geben Sie den Netzwerkspeicherort an, zu dem die Dateien im Ordner "Dokumente" umgeleitet werden sollen.

Standardmäßig ist diese Einstellung deaktiviert und kein Speicherort wird angegeben.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

Die Einstellung 'Dokumente'-Pfad muss aktiviert sein, damit Dateien sowohl in den Ordner "Dokumente" als auch in die Ordner "Bilder", "Musik" und "Videos" umgeleitet werden.

Umleitungseinstellungen für 'Dokumente'

Mit dieser Einstellung geben Sie an, wie der Inhalt des Ordners "Dokumente" umgeleitet werden soll.

Standardmäßig erfolgt die Umleitung an einen UNC-Pfad.

Wählen Sie eine der folgenden Optionen, um zu steuern, wie der Inhalt des Ordners "Dokumente" umgeleitet werden soll:

- Zum folgenden UNC-Pfad umleiten: leitet den Inhalt zu dem in der Richtlinieneinstellung 'Dokumente'-Pfad angegebenen UNC-Pfad.
- Zum Basisverzeichnis des Benutzers umleiten: leitet den Inhalt zu dem Basisverzeichnis des Benutzers. Dieses ist normalerweise mit dem Attribut #homeDirectory# für einen Benutzer in Active Directory konfiguriert.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

Einstellungen der Richtlinie "Downloads"

Feb 29, 2016

Der Abschnitt "Downloads" enthält Richtlinieneinstellungen für die Angabe, ob der Inhalt des Ordners "Downloads" an einen freigegebenen Speicherort im Netzwerk umgeleitet werden soll.

'Downloads'-Pfad

Mit dieser Einstellung geben Sie den Netzwerkspeicherort an, zu dem die Dateien im Ordner "Downloads" umgeleitet werden.

Standardmäßig ist diese Einstellung deaktiviert und kein Speicherort wird angegeben.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

Umleitungseinstellungen für 'Downloads'

Mit dieser Einstellung geben Sie an, wie der Inhalt des Ordners "Downloads" umgeleitet werden soll.

Standardmäßig erfolgt die Umleitung an einen UNC-Pfad.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

Einstellungen der Richtlinie "Favoriten"

Feb 29, 2016

Der Abschnitt "Favoriten" enthält Richtlinieneinstellungen für die Angabe, ob der Inhalt des Ordners "Favoriten" an einen freigegebenen Speicherort im Netzwerk umgeleitet werden soll.

'Favoriten'-Pfad

Mit dieser Einstellung geben Sie die Netzwerkfreigabe an, zu der der Inhalt des Ordners "Favoriten" umgeleitet werden soll.

Standardmäßig ist diese Einstellung deaktiviert und kein Speicherort wird angegeben.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

Umleitungseinstellungen für 'Favoriten'

Mit dieser Einstellung geben Sie an, wie der Inhalt des Ordners "Favoriten" umgeleitet werden soll.

Standardmäßig erfolgt die Umleitung an einen UNC-Pfad.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

Einstellungen der Richtlinie "Links"

Feb 29, 2016

Der Abschnitt "Links" enthält Richtlinieneinstellungen für die Angabe, ob der Inhalt des Ordners "Links" an einen freigegebenen Speicherort im Netzwerk umgeleitet werden soll.

'Links'-Pfad

Mit dieser Einstellung geben Sie die Netzwerkfreigabe an, zu der der Inhalt des Ordners "Links" umgeleitet werden soll.

Standardmäßig ist diese Einstellung deaktiviert und kein Speicherort wird angegeben.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

Umleitungseinstellungen für 'Links'

Mit dieser Einstellung geben Sie an, wie der Inhalt des Ordners "Links" umgeleitet werden soll.

Standardmäßig erfolgt die Umleitung an einen UNC-Pfad.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

Einstellungen der Richtlinie "Musik"

Feb 29, 2016

Der Abschnitt "Musik" enthält Richtlinieneinstellungen für die Angabe, ob der Inhalt des Ordners "Musik" an einen freigegebenen Speicherort im Netzwerk umgeleitet werden soll.

'Musik'-Pfad

Mit dieser Einstellung geben Sie die Netzwerkfreigabe an, zu der der Inhalt des Ordners "Musik" umgeleitet werden soll.

Standardmäßig ist diese Einstellung deaktiviert und kein Speicherort wird angegeben.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

Umleitungseinstellungen für 'Musik'

Mit dieser Einstellung geben Sie an, wie der Inhalt des Ordners "Musik" umgeleitet werden soll.

Standardmäßig erfolgt die Umleitung an einen UNC-Pfad.

Wählen Sie eine der folgenden Optionen, um zu steuern, wie der Inhalt des Ordners "Musik" umgeleitet werden soll:

- Zum folgenden UNC-Pfad umleiten: Leitet den Inhalt zu dem in der Richtlinieneinstellung 'Musik'-Pfad angegebenen UNC-Pfad.
- Relativ zum Ordner 'Dokumente' umleiten: Leitet den Inhalt in einen Ordner relativ zu dem Ordner "Dokumente" um.

Damit Inhalte in einen Ordner relativ zum Ordner "Dokumente" umgeleitet werden, muss die Einstellung 'Dokumente'-Pfad aktiviert sein.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

Einstellungen der Richtlinie "Bilder"

Feb 29, 2016

Der Abschnitt "Bilder" enthält Richtlinieneinstellungen für die Angabe, ob der Inhalt des Ordners "Bilder" an einen freigegebenen Speicherort im Netzwerk umgeleitet werden soll.

'Bilder'-Pfad

Mit dieser Einstellung geben Sie die Netzwerkfreigabe an, zu der der Inhalt des Ordners "Bilder" umgeleitet werden soll.

Standardmäßig ist diese Einstellung deaktiviert und kein Speicherort wird angegeben.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

Umleitungseinstellungen für 'Bilder'

Mit dieser Einstellung geben Sie an, wie der Inhalt des Ordners "Bilder" umgeleitet werden soll.

Standardmäßig erfolgt die Umleitung an einen UNC-Pfad.

Wählen Sie eine der folgenden Optionen, um zu steuern, wie der Inhalt des Ordners "Bilder" umgeleitet werden soll:

- Zum folgenden UNC-Pfad umleiten: Leitet den Inhalt zu dem in der Richtlinieneinstellung 'Bilder'-Pfad angegebenen UNC-Pfad.
- Relativ zum Ordner 'Dokumente' umleiten: Leitet den Inhalt in einen Ordner relativ zu dem Ordner "Dokumente" um.

Damit Inhalte in einen Ordner relativ zum Ordner "Dokumente" umgeleitet werden, muss die Einstellung 'Dokumente'-Pfad aktiviert sein.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

Einstellungen der Richtlinie "Gespeicherte Spiele"

Feb 29, 2016

Der Abschnitt "Gespeicherte Spiele" enthält Richtlinieneinstellungen für die Angabe, ob der Inhalt des Ordners "Gespeicherte Spiele" an einen freigegebenen Speicherort im Netzwerk umgeleitet werden soll.

Umleitungseinstellungen für 'Gespeicherte Spiele'

Mit dieser Einstellung geben Sie an, wie der Inhalt des Ordners "Gespeicherte Spiele" umgeleitet werden soll.

Standardmäßig erfolgt die Umleitung an einen UNC-Pfad.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

'Gespeicherte Spiele'-Pfad

Mit dieser Einstellung geben Sie die Netzwerkfreigabe an, zu der der Inhalt des Ordners "Gespeicherte Spiele" umgeleitet werden soll.

Standardmäßig ist diese Einstellung deaktiviert und kein Speicherort wird angegeben.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

Einstellungen der Richtlinie "Suchen"

Feb 29, 2016

Der Abschnitt "Suchen" enthält Richtlinieneinstellungen für die Angabe, ob der Inhalt des Ordners "Suchen" an einen freigegebenen Speicherort im Netzwerk umgeleitet werden soll.

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.

Mit dieser Einstellung geben Sie die Netzwerkfreigabe an, zu der der Inhalt des Ordners "Suchen" umgeleitet werden soll.

Standardmäßig ist diese Einstellung deaktiviert und kein Speicherort wird angegeben.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

Einstellungen der Richtlinie "Startmenü"

Feb 29, 2016

Der Abschnitt "Startmenü" enthält Richtlinieneinstellungen für die Angabe, ob der Inhalt des Ordners "Startmenü" an einen freigegebenen Speicherort im Netzwerk umgeleitet werden soll.

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.

Mit dieser Einstellung geben Sie die Netzwerkfreigabe an, zu der der Inhalt des Ordners "Startmenü" umgeleitet werden soll.

Standardmäßig ist diese Einstellung deaktiviert und kein Speicherort wird angegeben.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

Einstellungen der Richtlinie "Videos"

Feb 29, 2016

Der Abschnitt "Videos" enthält Richtlinieneinstellungen für die Angabe, ob der Inhalt des Ordners "Videos" an einen freigegebenen Speicherort im Netzwerk umgeleitet werden soll.

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.

Mit dieser Einstellung geben Sie die Netzwerkfreigabe an, zu der der Inhalt des Ordners "Videos" umgeleitet werden soll.

Standardmäßig ist diese Einstellung deaktiviert und kein Speicherort wird angegeben.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

Einstellungen der Richtlinie "Protokollierung"

Feb 29, 2016

Der Abschnitt "Protokollierung" enthält Richtlinieneinstellungen zum Konfigurieren der Protokollierung der Profilverwaltung.

Mit dieser Einstellung aktivieren oder deaktivieren Sie die ausführliche Protokollierung der in Active Directory ausgeführten Aktionen.

Diese Einstellung ist standardmäßig deaktiviert.

Wenn Sie diese Einstellung aktivieren, stellen Sie sicher, dass die Einstellung Protokollierung aktivieren auch aktiviert ist.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden Fehler und allgemeine Informationen protokolliert.

Mit dieser Einstellung aktivieren oder deaktivieren Sie die ausführliche Protokollierung allgemeiner Informationen.

Diese Einstellung ist standardmäßig deaktiviert.

Wenn Sie diese Einstellung aktivieren, stellen Sie sicher, dass die Einstellung Protokollierung aktivieren auch aktiviert ist.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden Fehler und allgemeine Informationen protokolliert.

Mit dieser Einstellung aktivieren oder deaktivieren Sie die ausführliche Protokollierung allgemeiner Warnungen.

Diese Einstellung ist standardmäßig deaktiviert.

Wenn Sie diese Einstellung aktivieren, stellen Sie sicher, dass die Einstellung Protokollierung aktivieren auch aktiviert ist.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden Fehler und allgemeine Informationen protokolliert.

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.

Mit dieser Einstellung aktivieren oder deaktivieren Sie die ausführliche Protokollierung der im Dateisystem ausgeführten Aktionen.

Diese Einstellung ist standardmäßig deaktiviert.

Wenn Sie diese Einstellung aktivieren, stellen Sie sicher, dass die Einstellung Protokollierung aktivieren auch aktiviert ist.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden Fehler und allgemeine Informationen protokolliert.

Mit dieser Einstellung aktivieren oder deaktivieren Sie die ausführliche Protokollierung von Dateisystembenachrichtigungen.

Diese Einstellung ist standardmäßig deaktiviert.

Wenn Sie diese Einstellung aktivieren, stellen Sie sicher, dass die Einstellung Protokollierung aktivieren auch aktiviert ist.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden Fehler und allgemeine Informationen protokolliert.

Mit dieser Einstellung aktivieren oder deaktivieren Sie die ausführliche Protokollierung von Benutzerabmeldungen.

Diese Einstellung ist standardmäßig deaktiviert.

Wenn Sie diese Einstellung aktivieren, stellen Sie sicher, dass die Einstellung Protokollierung aktivieren auch aktiviert ist.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden Fehler und allgemeine Informationen protokolliert.

Mit dieser Einstellung aktivieren oder deaktivieren Sie die ausführliche Protokollierung von Benutzeranmeldungen.

Diese Einstellung ist standardmäßig deaktiviert.

Wenn Sie diese Einstellung aktivieren, stellen Sie sicher, dass die Einstellung Protokollierung aktivieren auch aktiviert ist.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden Fehler und allgemeine Informationen protokolliert.

Mit dieser Einstellung geben Sie die maximal zulässige Größe für die Protokolldatei der Profilverwaltung in Bytes an.

Der Standardwert dieser Einstellung ist 1048576 Bytes (1 MB).

Citrix empfiehlt, dass die Größe dieser Datei auf 5 MB oder mehr erhöht wird, sofern Sie ausreichend Speicherplatz auf dem Datenträger haben. Wenn die Protokolldatei die maximale Größe überschreitet, wird eine vorhandene Sicherungskopie der Datei (.bak) gelöscht, die Protokolldatei erhält die Erweiterung .bak und eine neue Protokolldatei wird erstellt.

Die Protokolldatei wird unter "%SystemRoot%\System32\Logfiles\UserProfileManager" erstellt.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, wird der Standardwert verwendet.

Mit dieser Einstellung geben Sie einen alternativen Pfad an, der zum Speichern der Protokolldatei der Profilverwaltung verwendet wird.

Standardmäßig ist diese Einstellung deaktiviert und Protokolldateien werden im Standardspeicherort %SystemRoot%\System32\Logfiles\UserProfileManager gespeichert.

Der Pfad kann zu einem lokalen Laufwerk oder einem Remotelaufwerk im Netzwerk (UNC-Pfad) führen. Remotepfade können in großen, verteilten Umgebungen von Nutzen sein, können aber zu erheblichem Netzwerkverkehr führen, was für Protokolldateien unangebracht ist. Geben Sie für bereitgestellte virtuelle Maschinen mit einer beständigen Festplatte einen lokalen Pfad zu diesem Laufwerk an. Hierdurch wird sichergestellt, dass Protokolldateien beim Neustart der Maschine beibehalten werden. Geben Sie für virtuelle Maschinen ohne eine beständige Festplatte einen UNC-Pfad an. So werden Protokolldateien beibehalten. Das Systemkonto für die Maschinen muss aber Schreibzugriff auf die UNC-Freigabe haben. Verwenden Sie für Laptops, die vom Feature für Offlineprofile verwaltet werden, einen lokalen Pfad.

Wenn für Protokolldateien ein UNC-Pfad verwendet wird, empfiehlt Citrix, entsprechende Zugriffssteuerungslisten auf den Ordner mit den Protokolldateien anzuwenden, um sicherzustellen, dass nur autorisierte Benutzer- oder Computerkonten auf die gespeicherten Dateien zugreifen können.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, wird der Standardspeicherort "%SystemRoot%\System32\Logfiles\UserProfileManager" verwendet.

Mit dieser Einstellung aktivieren oder deaktivieren Sie die ausführliche Protokollierung persönlicher Benutzerinformationen.

Diese Einstellung ist standardmäßig deaktiviert.

Wenn Sie diese Einstellung aktivieren, stellen Sie sicher, dass die Einstellung Protokollierung aktivieren auch aktiviert ist.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden Fehler und allgemeine Informationen protokolliert.

Mit dieser Einstellung aktivieren oder deaktivieren Sie ausführliche Protokollierung der Richtlinienwerte beim An- und Abmelden von Benutzern.

Diese Einstellung ist standardmäßig deaktiviert.

Wenn Sie diese Einstellung aktivieren, stellen Sie sicher, dass die Einstellung Protokollierung aktivieren auch aktiviert ist.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden Fehler und allgemeine Informationen protokolliert.

Mit dieser Einstellung aktivieren oder deaktivieren Sie die ausführliche Protokollierung der in der Registrierung ausgeführten Aktionen.

Diese Einstellung ist standardmäßig deaktiviert.

Wenn Sie diese Einstellung aktivieren, stellen Sie sicher, dass die Einstellung Protokollierung aktivieren auch aktiviert ist.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden Fehler und allgemeine Informationen protokolliert.

Mit dieser Einstellung aktivieren oder deaktivieren Sie ausführliche Protokollierung aller Registrierungsunterschiede bei der Abmeldung von Benutzern.

Diese Einstellung ist standardmäßig deaktiviert.

Wenn Sie diese Einstellung aktivieren, stellen Sie sicher, dass die Einstellung Protokollierung aktivieren auch aktiviert ist.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden Fehler und allgemeine Informationen protokolliert.

Einstellungen der Richtlinie "Profilverarbeitung"

Feb 29, 2016

Der Abschnitt "Profilverarbeitung" enthält Richtlinieneinstellungen zum Konfigurieren, wie die Profilverwaltung Benutzerprofile verarbeitet.

Mit dieser Einstellung geben Sie optional eine Verlängerung für die Verzögerung (in Minuten) ein, nach der die Profilverwaltung lokal zwischengespeicherte Profile bei der Abmeldung löscht.

Bei einem Wert von 0 werden die Profile am Ende der Abmeldung sofort gelöscht. Die Profilverwaltung prüft jede Minute auf Abmeldungen, sodass ein Wert von 60 sicherstellt, dass Profile zwischen einer und zwei Minuten (je nachdem, wann die letzte Überprüfung stattgefunden hat) nach dem Abmelden gelöscht werden. Das Erweitern der Verzögerung ist nützlich, wenn Sie wissen, dass ein Prozess Dateien oder die Registrierungsstruktur während der Abmeldung geöffnet hält. Bei großen Profilen kann dies auch den Abmeldungsvorgang beschleunigen.

Die Standardeinstellung ist 0, lokal zwischengespeicherte Profile werden von der Profilverwaltung sofort gelöscht.

Wenn Sie diese Einstellung aktivieren, müssen Sie sicherstellen, dass die Einstellung Lokal zwischengespeicherte Profile nach Abmeldung löschen auch aktiviert ist.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden die Profile sofort gelöscht.

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.

Mit dieser Einstellung wird konfiguriert, wie die Profilverwaltung verfährt, wenn ein Benutzerprofil sowohl im Benutzerspeicher als auch als lokales Windows-Benutzerprofil (kein Citrix Benutzerprofil) vorhanden ist.

Standardmäßig verwendet die Profilverwaltung lokale Windows-Profile, ohne diese jedoch zu ändern.

Zum Steuern, wie die Profilverwaltung verfahren soll, wählen Sie eine der folgenden Optionen:

- Lokales Profil verwenden: Die Profilverwaltung verwendet lokale Windows-Profile, ohne diese jedoch zu ändern.
- Lokales Profil löschen: Die Profilverwaltung löscht das lokale Windows-Benutzerprofil und importiert dann das Citrix

Benutzerprofil aus dem Benutzerspeicher.
- Lokales Profil umbenennen: Die Profilverwaltung benennt das lokale Windows-Benutzerprofil um (als Sicherungskopie) und importiert dann das Citrix Benutzerprofil aus dem Benutzerspeicher.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden vorhandene lokale Profile verwendet.

Mit dieser Einstellung geben Sie den Typ des Profils an, das bei der Anmeldung eines Benutzers in den Benutzerspeicher migriert wird, wenn der Speicher kein aktuelles Profil für den Benutzer enthält.

Die Profilverwaltung kann vorhandene Profile während der Anmeldung spontan migrieren, wenn der Benutzer kein Profil im Benutzerspeicher hat. Anschließend verwendet die Profilverwaltung das Profil im Benutzerspeicher in der aktuellen Sitzung und in allen künftigen Sitzungen, die mit dem Pfad zu demselben Benutzerspeicher konfiguriert sind.

Standardmäßig werden lokale Profile und Roamingprofile während der Anmeldung in den Benutzerspeicher migriert.

Um anzugeben welche Profiltypen bei der Anmeldung in den Benutzerspeicher migriert werden sollen, wählen Sie eine der folgenden Optionen:
- Lokal und Roaming
- Lokal
- Roaming
- Keine (deaktiviert)

Wenn Sie Keine auswählen, wird der vorhandene Windows-Mechanismus für die Erstellung neuer Profile verwendet, genau wie in einer Umgebung, in der die Profilverwaltung nicht installiert ist.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden vorhandene lokale und servergespeicherte Profile migriert.

Mit dieser Einstellung geben Sie den Pfad zu dem Profil an, das die Profilverwaltung als Vorlage zum Erstellen neuer Benutzerprofile verwenden soll.

Dies muss der vollständige Pfad zu dem Ordner sein, der die Registrierungsdatei NTUSER.DAT und sämtliche anderen für das Vorlagenprofil erforderlichen Dateien und Ordner enthält.
Hinweis: Geben Sie mit dem Pfad nicht NTUSER.DAT ein. Geben Sie für die Datei \\Server\Profile\Vorlage\ntuser.dat den Speicherort als \\Server\Profile\Vorlage an.
Verwenden Sie einen absoluten Pfad (entweder einen UNC-Pfad oder einen Pfad auf dem lokalen Computer). Sie können einen lokalen Pfad verwenden, um z. B. ein Vorlagenprofil auf einem Citrix Provisioning Services-Image dauerhaft anzugeben. Relative Pfade werden nicht unterstützt.

Hinweis: Beachten Sie, dass diese Richtlinie nicht die Erweiterung von Active Directory-Attributen, Systemumgebungsvariablen oder der Variablen %USERNAME% und %USERDOMAIN% unterstützt.
Standardmäßig ist diese Einstellung deaktiviert und neue Benutzerprofile werden auf der Basis des Standardbenutzerprofils auf dem Gerät, auf dem sich der Benutzer als erstes anmeldet, erstellt.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden keine Vorlagen verwendet.

Diese Einstellung ermöglicht eine Überschreibung des lokalen Profils durch das Vorlagenprofil bei der Erstellung neuer Benutzerprofile.

Wenn ein Benutzer kein Citrix Benutzerprofil hat, aber ein lokales Windows-Benutzerprofil vorhanden ist, wird standardmäßig das lokale Profil verwendet (und in den Benutzerspeicher migriert, wenn diese Option nicht deaktiviert ist). Durch Aktivieren dieser Einstellung kann das Vorlagenprofil das lokale Profil bei der Erstellung neuer Benutzerprofile überschreiben.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden keine Vorlagen verwendet.

Diese Einstellung ermöglicht eine Überschreibung eines Roamingprofils durch das Vorlagenprofil bei der Erstellung neuer Benutzerprofile.

Wenn ein Benutzer kein Citrix Benutzerprofil hat aber ein lokales Windows-Benutzerprofil vorhanden ist, wird standardmäßig das Roamingprofil verwendet (und in den Benutzerspeicher migriert, wenn diese Option nicht deaktiviert ist). Durch Aktivieren dieser Einstellung kann das Vorlagenprofil das Roamingprofil bei der Erstellung neuer Benutzerprofile überschreiben.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden keine Vorlagen verwendet.

Bei Auswahl dieser Einstellung verwendet die Profilverwaltung das Vorlagenprofil als Standardprofil bei der Erstellung aller neuen Benutzerprofile.

Standardmäßig ist diese Einstellung deaktiviert und neue Benutzerprofile werden auf der Basis des Standardbenutzerprofils auf dem Gerät, auf dem sich der Benutzer als erstes anmeldet, erstellt.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden keine Vorlagen verwendet.

Einstellungen der Richtlinie "Registrierung"

Feb 29, 2016

Der Abschnitt "Registrierung" enthält Richtlinieneinstellungen, mit denen Sie festlegen können, welche Registrierungsschlüssel bei der Verarbeitung der Profilverwaltung berücksichtigt und welche ausgeschlossen werden sollen.

Mit dieser Einstellung geben Sie die Liste der Registrierungsschlüssel in der HKCU-Struktur an, die nicht von der Profilverwaltung verarbeitet werden sollen, wenn sich ein Benutzer abmeldet.

Wenn diese Option aktiviert ist, werden die in dieser Liste aufgeführten Schlüssel von der Verarbeitung ausgeschlossen, wenn sich ein Benutzer abmeldet.

Standardmäßig ist diese Einstellung deaktiviert, und alle Registrierungsschlüssel in der HKCU-Struktur werden verarbeitet.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden keine Registrierungsschlüssel von der Verarbeitung ausgeschlossen.

Mit dieser Einstellung geben Sie die Liste der Registrierungsschlüssel in der HKCU-Struktur an, die von der Profilverwaltung verarbeitet werden sollen, wenn sich ein Benutzer abmeldet.

Wenn diese Option aktiviert ist, werden die in dieser Liste aufgeführten Schlüssel in die Verarbeitung eingeschlossen, wenn sich ein Benutzer abmeldet.

Standardmäßig ist diese Einstellung deaktiviert, und alle Registrierungsschlüssel in der HKCU-Struktur werden verarbeitet.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, wird die gesamte HKCU-Struktur verarbeitet.

Einstellungen der Richtlinie "Gestreamte Benutzerprofile"

Feb 29, 2016

Der Abschnitt "Gestreamte Benutzerprofile" enthält Richtlinieneinstellungen zum Konfigurieren, wie die Profilverwaltung Benutzerprofile verarbeitet.

Mit dieser Einstellung geben Sie an, ob die Profilverwaltung gestreamte Dateien so bald wie möglich zwischenspeichern soll, wenn sich ein Benutzer anmeldet. Durch das Zwischenspeichern von Dateien, nachdem sich ein Benutzer anmeldet, wird Netzwerkbandbreite gespart und die Benutzererfahrung optimiert.

Verwenden Sie diese Einstellung mit der Einstellung Profilstreaming.

Standardmäßig ist diese Einstellung deaktiviert und gestreamte Dateien werden nicht so schnell wie möglich zwischengespeichert, wenn sich ein Benutzer anmeldet.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, ist sie deaktiviert.

Mit dieser Einstellung geben Sie eine Untergrenze (in Megabytes) für die Größe der Dateien an, die gestreamt werden. Die Profilverwaltung speichert Dateien dieser Größe bzw. größere Dateien so bald wie möglich zwischen, wenn ein Benutzer sich anmeldet.

Die Standardeinstellung ist 0 (null) und die Funktion zum Zwischenspeichern des gesamten Profils wird verwendet. Wenn das Feature zum Zwischenspeichern des gesamten Profils aktiviert ist, ruft die Profilverwaltung den gesamten Inhalt des Profils im Benutzerspeicher als Hintergrundaufgabe ab, nachdem sich ein Benutzer anmeldet.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, ist sie deaktiviert.

Diese Einstellung aktiviert oder deaktiviert das Feature für gestreamte Citrix Benutzerprofile. Wenn diese Option aktiviert ist, werden Dateien und Ordner in einem Profil nur dann aus dem Benutzerspeicher auf den lokalen Computer abgerufen, wenn auf sie von Benutzern nach der Anmeldung zugegriffen wird. Registrierungseinträge und Dateien im Bereich für ausstehende Dateien werden sofort abgerufen.

Standardmäßig ist das Profilstreaming ist deaktiviert.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, ist sie deaktiviert.

Mit dieser Einstellung geben Sie die Benutzerprofile in einer Organisationseinheit gestreamt werden, basierend auf Windows Benutzergruppen.

Wenn diese Option aktiviert ist, werden nur die Benutzerprofile in den angegebenen Benutzergruppen gestreamt. Alle anderen Benutzerprofile werden normal verarbeitet.

Standardmäßig ist diese Einstellung deaktiviert und alle Dateien in Benutzerprofilen werden normal verarbeitet.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden alle Benutzergruppen verarbeitet.

Mit dieser Einstellung geben Sie einen Zeitraum (in Tagen) an, nach dem Dateien der Benutzer aus dem Bereich für ausstehende Dateien in den Benutzerspeicher zurückgeschrieben werden, wenn ein Server nicht mehr reagiert und der Benutzerspeicher gesperrt bleibt. Dies verhindert ein Aufblähen des ausstehenden Bereichs und stellt sicher, dass der Benutzerstore immer die aktuellen Dateien enthält.

Die Standardeinstellung ist 1 Tag.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, wird der Standardwert verwendet.

Einstellungen der Richtlinie "Receiver"

Feb 29, 2016

Hinweis: Wenn nicht anders angegeben, bezieht sich "Receiver" auf Citrix Receiver.

Der Abschnitt "Receiver" enthält Richtlinieneinstellungen zum Angeben einer Liste von StoreFront-Adressen, die für auf dem virtuellen Desktop ausgeführte Windows-Betriebssysteme per Push an Citrix Receiver für Windows übertragen werden sollen.

Mit dieser Einstellung geben Sie eine Liste der StoreFront-Stores an, die Administratoren für die Übertragung per Push an Citrix Receiver für Windows auswählen können. Beim Erstellen einer Bereitstellungsgruppe können Administratoren auswählen, welche Stores für Citrix Receiver für Windows auf virtuellen Desktops, die in dieser Gruppe ausgeführt werden, per Push übertragen werden sollen.

In der Standardeinstellung sind keine Stores angegeben.

Geben Sie für jeden Store die folgenden Informationen in Form eines durch Semikolons getrennten Eintrags an:

- Storename: der Name des Stores wie er Benutzern angezeigt wird.
- Store-URL: die URL des Stores.
- Storeaktivierungszustand: Ob der Store für Benutzer verfügbar ist. Dies ist entweder ein oder aus.
- Store-Beschreibung: die Beschreibung des Stores, die Benutzern angezeigt wird.

Beispiel: Vertriebsstore;https://sales.mycompany.com/Citrix/Store/discovery;On;Store für Vertriebsmitarbeiter

Einstellungen der Richtlinie "Virtual Delivery Agent"

Feb 29, 2016

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

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.

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".

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.

Verwenden Sie diese Einstellung nur, wenn die Einstellung Automatische Controllerupdates aktivieren deaktiviert ist.

Mit dieser Einstellung geben Sie eine durch Leerzeichen getrennte Liste von vollständig qualifizierten Domänennamen

(FQDN) für Controller an, die der VDA für die Registrierung bei einem Controller verwendet, wenn die registrierungsbasierte Registrierung verwendet wird. Dies ist eine optionale Einstellung, die mit der Einstellung "Controller-SIDs" verwendet werden kann.

Diese Einstellung ist standardmäßig leer.

Mit dieser Einstellung ist eine automatische Registrierung des VDAs bei einem Controller nach der Installation möglich.

Nach der Registrierung wird von dem Controller, bei dem der VDA registriert ist, eine Liste der aktuellen Controller-FQDNs und -SIDs an den VDA gesendet. Diese Liste wird in den persistenten Speicher des VDAs geschrieben. Jeder Controller prüft die Datenbank alle 90 Minuten auf Controllerinformationen. Wurde seit der letzten Prüfung ein Controller hinzugefügt oder entfernt oder ist eine Richtlinienänderung erfolgt, sendet der Controller eine aktualisierte Liste an die bei ihm registrierten VDAs. Der VDA nimmt alle Verbindungen von allen Controllern in der aktuellen Liste an.

Standardmäßig ist diese Einstellung aktiviert.

Diese Einstellung steuert die Form der Adresse, die vom VDA für die Registrierung beim Controller verwendet wird:

- Bei aktivierter Einstellung wird der VDA mit der IPv6-Adresse der Maschine für die Kommunikation 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).
- Bei deaktivierter Einstellung wird der VDA mit der IPv4-Adresse der Maschine für die Kommunikation beim Controller registriert.

Diese Einstellung ist standardmäßig deaktiviert.

Verwenden Sie diese Einstellung nur, wenn die Einstellung Automatische Controllerupdates aktivieren deaktiviert ist.

Diese Einstellung gibt den Globally Unique Identifier (GUID) der Site an, den der VDA für die Registrierung bei einem Controller verwendet, wenn die Active Directory-basierte Registrierung verwendet wird.

Diese Einstellung ist standardmäßig leer.

Einstellungen der Richtlinie "HDX 3D Pro"

Feb 29, 2016

Der Bereich "HDX 3D Pro" enthält Richtlinieneinstellungen, mit denen Sie das Tool zum Konfigurieren der Bildqualität für Benutzer aktivieren und konfigurieren können. Mit dem Tool können Benutzer die Verwendung der verfügbaren Bandbreite durch Anpassen des Verhältnisses zwischen Bildqualität und Reaktionszeit in Echtzeit optimieren.

Mit dieser Einstellung wird angegeben, ob Benutzer verlustfreie Komprimierung mit dem Tool zum Konfigurieren der Bildqualität aktivieren oder deaktivieren können. In der Standardeinstellung wird den Benutzern die Möglichkeit zum Aktivieren der verlustfreien Komprimierung nicht eingeräumt.

Aktiviert ein Benutzer die verlustfreie Komprimierung, wird die Bildqualität automatisch auf den höchsten Wert eingestellt, der im Bildkonfigurationstool verfügbar ist. Standardmäßig kann je nach Leistungsfähigkeit des Benutzergeräts und des Hostcomputers entweder die GPU-basierte oder die CPU-basierte Komprimierung verwendet werden.

Mit dieser Einstellung geben Sie den Mindest- und den Höchstwert an, mit denen der Bildqualitätsanpassungsbereich, der den Benutzern im Tool zum Konfigurieren der Bildqualität zur Verfügung steht, festgelegt wird.

Geben Sie für die Bildqualität Werte zwischen 0 und 100 an. Der Höchstwert muss größer oder gleich dem Mindestwert sein.

Einstellungen der Richtlinie "Virtuelle IP"

Feb 29, 2016

Der Abschnitt "Virtuelle IP" enthält Richtlinieneinstellungen für die Angabe, ob Sitzungen eine eigene virtuelle Loopbackadresse haben.

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.

Mit dieser Einstellung geben Sie die ausführbaren Dateien der Anwendungen an, die virtuelle Loopbackadressen verwenden können. Wenn Sie der Liste Programme hinzufügen, geben Sie nur den Namen der ausführbaren Datei an. Sie müssen nicht den gesamten Pfad angeben.

In der Standardeinstellung sind keine ausführbaren Dateien angegeben.

Konfigurieren von COM-Port- und LPT-Portumleitungseinstellungen in der Registrierung

Feb 29, 2016

Richtlinieneinstellungen für COM-Port- und LPT-Portumleitung befinden sich unter HKLM\Software\Citrix\GroupPolicy\Defaults\Deprecated 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. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.

Registrierungsschlüssel	Beschreibung	Zulässige Werte
AllowComPortRedirection	Zulassen oder Verhindern der COM-Portumleitung	1 (Zulassen) oder 0 (Verhindern)
LimitComBw	Bandbreitenlimit für COM-Portumleitungskanal	Numerischer Wert
LimitComBWPercent	Bandbreitenlimit für COM-Portumleitungskanal als Prozentsatz der Gesamtsitzungsbandbreite	Numerischer Wert zwischen 0 und 100
AutoConnectClientComPorts	Automatische Verbindung von COM-Ports auf dem Benutzergerät	1 (Zulassen) oder 0 (Verhindern)
AllowLptPortRedirection	Zulassen oder Verhindern der LPT-Portumleitung	1 (Zulassen) oder 0 (Verhindern)
LimitLptBw	Bandbreitenlimit für LPT-Portumleitungskanal	Numerischer Wert
LimitLptBwPercent	Bandbreitenlimit für LPT-Portumleitungskanal als Prozentsatz der Gesamtsitzungsbandbreite	Numerischer Wert zwischen 0 und 100
AutoConnectClientLptPorts	Automatische Verbindung von LPT-Ports auf dem Benutzergerät	1 (Zulassen) oder 0 (Verhindern)

Nach dem Konfigurieren dieser Einstellungen ändern Sie die Maschinenkataloge, damit sie das neue Masterimage oder die aktualisierte physische Maschine verwenden. Wenn sich die Benutzer das nächste Mal abmelden, werden die Desktops mit den neuen Einstellungen aktualisiert.

Richtlinieneinstellungen für Connector für Configuration Manager 2012

Feb 29, 2016

Der Abschnitt "Connector für Configuration Manager 2012" enthält Richtlinieneinstellungen zum Konfigurieren des Citrix Connector 7.5-Agents.

Wichtig: Richtlinien für Warnungs-, Abmeldungs- und Neustartmeldungen gelten nur für Bereitstellungen für Serverbetriebssystemmaschinenkataloge, die manuell oder über Provisioning Services verwaltetet werden. Bei solchen Maschinenkatalogen benachrichtigt der Connector-Dienst Benutzer über ausstehende Anwendungsinstallationen oder Softwareupdates.
Verwenden Sie bei über MCS verwalteten Katalogen Studio zur Benachrichtigung der Benutzer. Verwenden Sie bei manuell verwalteten Maschinenkatalogen mit Desktopbetriebssystemmaschinen Configuration Manager zur Benachrichtigung der Benutzer. Verwenden Sie bei mit Provisioning Services verwalteten Maschinenkatalogen mit Desktopbetriebssystemmaschinen Provisioning Services zur Benachrichtigung der Benutzer.

Diese Einstellung gibt das Intervall an, mit dem Benutzern Vorabmeldungen angezeigt werden.

Intervalle werden im Format ttt.hh:mm:ss festgelegt. Dabei gilt Folgendes:
- ttt steht für die Tage. Dieser Parameter ist optional und kann Werte von 0 bis 999 annehmen.
- hh steht für die Stunden und kann Werte von 0 bis 23 annehmen.
- mm steht für Minuten und kann Werte von 0 bis 59 annehmen.
- ss steht für Sekunden und kann Werte von 0 bis 59 annehmen.

Das Standardintervall ist 1 Stunde (01:00:00).

Diese Einstellung enthält den editierbaren Text für die Vorabmeldung, die Benutzer vor anstehenden Softwareupdates oder Wartungsaufgaben erhalten, für die sie sich abmelden müssen.

Die Standardmeldung lautet: {TIMESTAMP} Please save your work. The server will go offline for maintenance in {TIMELEFT}

Diese Einstellung enthält den editierbaren Titel für die Titelleiste der Vorabmeldung, die Benutzer erhalten.

Der Standardtitel ist: Upcoming Maintenance

Diese Einstellung definiert, wie lange vor Wartungsaufgaben die Vorabwarnmeldung zum ersten Mal angezeigt wird.

Der Zeitraum wird im Format ttt.hh:mm:ss angegeben, mit den folgenden Variablen:
- ttt steht für die Tage. Dieser Parameter ist optional und kann Werte von 0 bis 999 annehmen.
- hh steht für die Stunden und kann Werte von 0 bis 23 annehmen.
- mm steht für Minuten und kann Werte von 0 bis 59 annehmen.

- ss steht für Sekunden und kann Werte von 0 bis 59 annehmen.

In der Standardeinstellung ist der Wert 16 Stunden (16:00:00), d. h. dass die erste Vorabwarnmeldung ca. 16 Stunden vor der Wartung angezeigt wird.

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

Diese Einstellung enthält den editierbaren Titel für die Titelleiste der letzten Meldung für Abmeldung erzwingen.

Der Standardtitel lautet: Notification From IT Staff

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.

Diese Einstellung enthält den editierbaren Text für die letzte Warnmeldung, die Benutzer auffordert, ihre Arbeit zu speichern und sich vor der erzwungenen Abmeldung abzumelden.

Die Standardmeldung enthält den folgenden Text: "{TIMESTAMP} Please save your work and log off. The server will go offline for maintenance in {TIMELEFT}

Diese Einstellung enthält den editierbaren Text für die Titelleiste der Meldung für Abmeldung erzwingen.

Der Standardtitel lautet: Notification From IT Staff

Der Connector-Agent erkennt automatisch, wenn er auf einem von Provisioning Services oder MCS verwalteten Maschinenklon ausgeführt wird. Der Agent blockiert Configuration Manager-Updates auf imageverwalteten Klonen und installiert die Updates automatisch auf dem Masterimage des Katalogs.

Nachdem ein Masterimage aktualisiert wurde, verwenden Sie Studio zum Orchestrieren des Neustarts der MCS-Klone. Der Connector-Agent orchestriert automatisch den Neustart von PVS-Katalogklonen während der Configuration Manager-Wartung. Zur Außerkraftsetzung dieses Verhaltens, damit Software auf Katalogklonen von Configuration Manager

installiert wird, ändern Sie den Modus von "Imageverwaltet" in Deaktiviert.

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

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 fünf Minuten (00:05:00) festgelegt.

Verwaltung

Feb 29, 2016

Die Verwaltung einer XenApp- oder XenDesktop-Site hat vielfältige Aspekte.

Lizenzierung

Eine gültige Verbindung mit dem Citrix Lizenzserver ist zum Erstellen einer Site erforderlich. Anschließend können Sie Aufgaben wie das Hinzufügen von Lizenzen, das Ändern von Lizenztyp oder -modell und das Verwalten von Lizenzadministratoren über Studio erledigen. Über Studio können Sie auch auf die License Administration Console zugreifen.

Zonen

In geografisch verteilten Bereitstellungen führen Sie Anwendungen und Desktops mithilfe von Zonen näher am Benutzer, um die Leistung zu verbessern. Beim Installieren und Konfigurieren einer Site sind alle Controller, Maschinenkataloge und Hostverbindungen in der primären Zone. Später können Sie mit Studio Satellitenzonen für diese Elemente erstellen. Wenn Sie mehrere Zonen haben, können Sie angeben, in welcher Zone neu erstellte Maschinenkataloge, Hostverbindungen und Controller hinzugefügt werden sollen. Sie können Elemente auch zwischen Zonen verschieben.

Verbindungen und Ressourcen

Wenn die Maschinen, über die Anwendungen und Desktops für Benutzer bereitgestellt werden, von einem Hypervisor oder Clouddienst gehostet werden, richten Sie die erste Verbindung beim Erstellen einer Site mit dem Hypervisor bzw. Clouddienst ein. Die Speicher- und Netzwerkdetails dieser Verbindung sind ihre *Ressourcen*. Später können Sie die Verbindung und ihre Ressourcen ändern und neue Verbindungen erstellen. Sie können auch die Maschinen verwalten, die eine konfigurierte Verbindung verwenden.

Verbindungsleasing

Das Verbindungsleasing ergänzt die bewährten Methoden zur hohen Verfügbarkeit bei SQL Server, da es Benutzern die Wiederverbindung mit den zuletzt verwendeten Anwendungen und Desktops ermöglicht, selbst wenn die Sitedatenbank nicht verfügbar ist. Das Verbindungsleasing kann zwar die Verbindungsresilienz und die Produktivität der Benutzer verbessern, in diesem Artikel werden jedoch Überlegungen im Hinblick auf Verfügbarkeit, Betrieb und Leistung anderer Funktionen für Controller mit geleaster Verbindung behandelt.

Virtuelle IP-Adressen und virtuelles Loopback

Die Microsoft virtuelle IP-Adresse stellt einer veröffentlichten Anwendung eine eindeutige dynamisch zugeordnete IP-Adresse für jede Sitzung bereit. Mit dem Citrix Feature des virtuellen Loopbacks können Sie Anwendungen, die mit dem lokalen Host (localhost) kommunizieren (normalerweise 127.0.0.1), so konfigurieren, dass sie eine eindeutige virtuelle Loopbackadresse im Bereich des lokalen Hosts verwenden (127.*).

Delivery Controller

Bevor ein VDA die Bereitstellung von Anwendungen und Desktops unterstützen kann, muss er bei einem Controller zum Aufbau der Kommunikation registriert werden. Controlleradressen können bei der Installation eines VDAs, über Citrix Richtlinieneinstellungen oder Registrierungseinstellungen und auf andere Weise angegeben werden. Es ist wichtig, dass die VDAs beim Hinzufügen, Verschieben und Entfernen von Controllern immer aktualisierte Informationen erhalten. In diesem Abschnitt wird beschrieben, wie und wann VDAs registriert werden, wie die Controllerinformationen aktualisiert werden und wie Controller hinzugefügt, verschoben und entfernt werden.

Sitzungen

Das Erhalten der Sitzungsaktivität ist wichtig, um eine optimale Benutzererfahrung zu gewährleisten. Mit diversen Features können Sie die Sitzungszuverlässigkeit optimieren und damit das Risiko von Problemen, Ausfallzeiten und Produktivitätsverlusten verringern.

- Sitzungszuverlässigkeit
- Automatische Wiederverbindung von Clients
- ICA-Keep-Alive
- Workspace Control
- Sitzungsroaming

Durchführung einer Suche in Studio

Zum Anzeigen von Informationen zu Maschinen, Sitzungen, Maschinenkatalogen, Anwendungen und Bereitstellungsgruppen in Studio steht ein flexibles Suchfeature zur Verfügung.

IPv4/ipv6

Dieses Release von XenApp und XenDesktop unterstützt reines IPv4, reines IPv6a und Bereitstellungen mit dualem Stapel, bei denen überlappende IPv4- und IPv6-Netzwerke verwendet werden. In diesem Abschnitt werden solche Bereitstellungen beschrieben. Außerdem werden die Citrix Richtlinieneinstellungen vorgestellt, mit denen die Verwendung von IPv4 bzw. IPv6 gesteuert wird.

Clientordnerumleitung

Durch die Clientordnerumleitung ändert sich der Zugriff auf clientseitige Dateien bei der hostseitigen Sitzung. Wird auf dem Server nur die Clientlaufwerkzuordnung aktiviert, werden die clientseitigen vollständigen Volumes den Sitzungen automatisch als UNC-Link (Universal Naming Convention) zugeordnet. Wenn Sie die Clientordnerumleitung auf dem Server aktivieren und der Benutzer sie auf dem Windows-Desktopgerät konfiguriert, wird der Teil des vom lokalen Benutzer angegebenen lokalen Volumes umgeleitet.

Benutzerprofile

Standardmäßig wird die Citrix Profilverwaltung automatisch zusammen mit einem VDA installiert. Wenn Sie diese Lösung verwenden, lesen Sie diesen Artikel mit allgemeinen Hinweisen und die Dokumentation zur Profilverwaltung mit umfassenden Informationen.

Lizenzierung

Feb 29, 2016

Sie können die Lizenzierung in Studio verwalten und nachverfolgen, wenn der Lizenzserver in derselben Domäne wie Studio oder in einer vertrauenswürdigen Domäne ist. Informationen zu anderen Lizenzierungsaufgaben finden Sie in der Dokumentation zur Lizenzierung.

Sie müssen für die nachfolgend beschriebenen Aufgaben Volladministrator für die Lizenzierung sein, außer um die Lizenzinformationen anzuzeigen. Zum Anzeigen der Lizenzinformationen in Studio muss der Administrator mindestens Lesezugriff als delegierter Administrator für die Lizenzierung haben. Die integrierten Rollen des Volladministrators und des Administrators mit Leserechten haben diese Berechtigung.

In der folgenden Tabelle werden die unterstützten Editionen und Lizenzierungsmodelle aufgeführt:

Produkte	Editionen	Lizenzmodelle
XenApp	• Platinum • Enterprise • Advanced	CCU
XenDesktop	• Platinum • Enterprise • App • VDI	• Benutzer/Gerät • CCU

Zum Anzeigen der Lizenzinformationen wählen Sie **Konfiguration > Lizenzierung** im Studio-Navigationsbereich. Eine Zusammenfassung der Lizenzverwendung sowie Einstellungen für die Site werden zusammen mit einer Liste aller Lizenzen angezeigt, die aktuell auf dem angegebenen Lizenzserver installiert sind.

Herunterladen einer Lizenz von Citrix:

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Lizenzierung**.
2. Wählen Sie im Aktionsbereich **Lizenzen zuteilen**.
3. Geben Sie den Lizenzzugangscode an, der per E-Mail von Citrix bereitgestellt wird.
4. Wählen Sie ein Produkt und klicken Sie auf **Lizenzen zuteilen**. Alle Lizenzen, die für das Produkt verfügbar sind, sind zugeteilt und heruntergeladen. Wenn Sie alle Lizenzen für einen bestimmten Lizenzzugangscode zuteilen und herunterladen, können Sie den Lizenzzugangscode nicht erneut verwenden. Zum Durchführen weiterer Transaktionen mit diesem Code melden Sie sich bei My Account an.

Hinzufügen von Lizenzen, die auf dem lokalen Computer oder im Netzwerk gespeichert sind:

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Lizenzierung**.
2. Wählen Sie im Aktionsbereich **Lizenzen hinzufügen**.
3. Navigieren Sie zu einer Lizenzdatei und fügen Sie sie dem Lizenzserver hinzu.

Ändern des Lizenzservers:

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Lizenzierung**.

2. Wählen Sie im Aktionsbereich **Lizenzserver ändern**.
3. Geben Sie die Adresse des Lizenzservers im Format name:port an ("name" = DNS-, NetBIOS- oder IP-Adresse). Wenn Sie keine Portnummer angeben, wird der Standardport (27000) verwendet.

Auswählen des Lizenztyps:

- Beim Konfigurieren der Site werden Sie nach Angabe des Lizenzservers aufgefordert, den zu verwendenden Lizenztyp auszuwählen. Stehen auf dem Server keine Lizenzen zur Verfügung, wird automatisch die Option zur Verwendung des Produkts während einer 30-tägigen Testphase ohne Lizenz ausgewählt.
- Stehen auf dem Server Lizenzen zur Verfügung, werden die entsprechenden Informationen angezeigt. Der Benutzer kann dann die gewünschte Lizenz auswählen. Alternativ können Sie dem Server eine Lizenzdatei hinzufügen und diese dann auswählen.

Ändern von Produktedition und Lizenzierungsmodell:

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Lizenzierung**.
2. Wählen Sie im Aktionsbereich **Produktedition bearbeiten**.
3. Aktualisieren Sie die entsprechenden Optionen.

Zum Öffnen der License Administration Console wählen Sie im Aktionsbereich **License Administration Console**. Die Konsole wird normalerweise sofort angezeigt. Wenn das Dashboard jedoch mit Kennwortschutz konfiguriert wurde, werden Sie aufgefordert, die Anmeldeinformationen für die License Administration Console einzugeben. Informationen zur Verwendung der Konsole finden Sie in der Dokumentation zur Lizenzierung.

Hinzufügen eines Lizenzadministrators:

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Lizenzierung**.
2. Wählen Sie im mittleren Bereich die Registerkarte Lizenzierungsadministratoren.
3. Wählen Sie im Aktionsbereich **Lizenzadministrator hinzufügen**.
4. Navigieren Sie zu dem Benutzer, den Sie als Administrator hinzufügen möchten, und wählen Sie die Berechtigungen.

Ändern der Berechtigungen eines Lizenzadministrators oder Löschen eines Lizenzadministrators

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Lizenzierung**.
2. Wählen Sie die Registerkarte Lizenzadministratoren im mittleren Bereich und dann den Lizenzadministrator.
3. Wählen Sie im Aktionsbereich **Lizenzadministrator bearbeiten** bzw. **Lizenzadministrator löschen**.

Hinzufügen einer Lizenzadministratorgruppe:

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Lizenzierung**.
2. Wählen Sie im mittleren Bereich die Registerkarte Lizenzierungsadministratoren.
3. Wählen Sie im Aktionsbereich **Lizenzierungsadministratorengruppe hinzufügen**.
4. Navigieren Sie zu der Gruppe, deren Mitglieder Sie als Administratoren hinzufügen möchten, und wählen Sie die Berechtigungen. Beim Hinzufügen einer Active Directory-Gruppe werden den Benutzern dieser Gruppe Lizenzierungsadministratorberechtigungen erteilt.

Ändern der Berechtigungen einer Lizenzierungsadministratorengruppe oder Löschen einer Lizenzierungsadministratorengruppe

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Lizenzierung**.
2. Wählen Sie die Registerkarte Lizenzadministratoren im mittleren Bereich und dann die

Lizenzierungsadministratorengruppe.

3. Wählen Sie im Aktionsbereich **Lizenzierungsadministratorengruppe bearbeiten** bzw. **Lizenzierungsadministratorengruppe löschen**.

Zonen

Feb 29, 2016

In Bereitstellungen mit weit auseinanderliegenden Standorten in einem WAN kann es zu Latenz- und Zuverlässigkeitsproblemen kommen. Es gibt zwei Möglichkeiten, diesen Herausforderungen zu begegnen:

- Bereitstellen mehrerer Sites mit eigener SQL Server-Sitedatenbank:

  Diese Option empfiehlt sich für große Unternehmen. Mehrere Sites können einzeln verwaltet werden und erfordern alle eine eigene SQL Server-Sitedatenbank. Jede Site ist eine eigenständige XenApp-Bereitstellung.

- Konfigurieren mehrerer Zonen in einer einzelnen Site:

  Mit Zonen können Benutzer an entfernten Standorten eine Verbindung mit Ressourcen herstellen, ohne dass die Verbindungen durch große WAN-Segmente laufen müssen. Zonen gestatten eine effektive Siteverwaltung über eine einzelne Citrix Studio-Konsole, Citrix Director und die Sitedatenbank. Auf diese Weise können die Kosten für Bereitstellung, Personalbesetzung, Lizenzierung und Betrieb zusätzlicher Sites mit eigenen Datenbanken an entfernten Standorten gespart werden.

  Zonen können bei Bereitstellungen aller Größen nützlich sein. Mit Zonen können Sie Anwendungen und Desktops näher an den Benutzern ansiedeln und so die Leistung verbessern. Aus Redundanz- und Flexibilitätsgründen ist die Installation eines oder mehrerer Controller zonenlokal möglich, jedoch nicht erforderlich.

In diesem Artikel bezieht sich der Begriff "lokal" auf die jeweils behandelte Zone. "Ein VDA registriert sich bei einem lokalen Controller" bedeutet beispielsweise, dass sich der VDA bei einem Controller in der Zone registriert, in der der VDA ist.

Die Zonen in diesem Release ähneln denen in XenApp 6.5 und Vorversionen, sind mit ihnen jedoch nicht identisch. Beispielsweise gibt es in dieser Zonenimplementierung keine Datensammelpunkte. Alle Controller in einer Site kommunizieren mit einer Sitedatenbank in der primären Zone. Auch Failover und bevorzugte Zonen funktionieren in diesem Release anders.

Zonentypen

Eine Site hat immer eine primäre Zone. Sie kann auch eine oder mehrere Satellitenzonen haben. Satellitenzonen können für die Notfallwiederherstellung, entfernte Datencenter, Zweigstellen, eine Cloud oder eine Availability Zone in einer Cloud verwendet werden.

Primäre Zone

Die primäre Zone hat den Standardnamen "Primär" und umfasst SQL Server-Sitedatenbank (sowie ggf. hoch verfügbare SQL Server-Computer), Studio, Director, Citrix StoreFront, Citrix Lizenzserver und NetScaler Gateway. Die Sitedatenbank muss immer in der primären Zone sein.

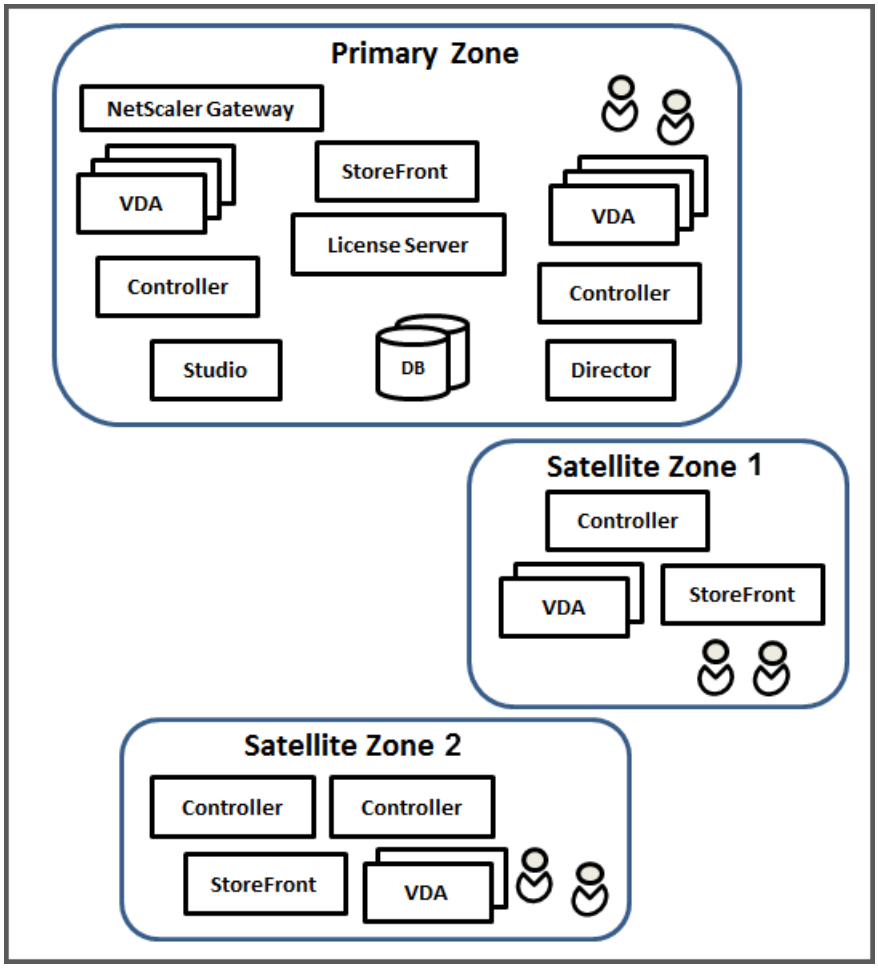
Die primäre Zone sollte aus Redundanzgründen außerdem mindestens zwei Controller enthalten und kann einen oder mehrere VDAs mit Anwendungen umfassen, die eng an die Datenbank und Infrastruktur gekoppelt sind.

Satellitenzonen

Eine Satellitenzone enthält einen oder mehrere VDAs, Controller und StoreFront- sowie NetScaler Gateway-Server. Im Normalbetrieb kommunizieren Controller in einer Satellitenzone direkt mit der Datenbank in der primären Zone.

Satellitenzonen, insbesondere große, können auch einen Hypervisor für die Bereitstellung und/oder Speicherung von Maschinen enthalten. Beim Konfigurieren einer Satellitenzone können Sie dieser eine Hypervisor- oder Clouddienstverbindung zuweisen. Alle Maschinenkataloge, die diese Verbindung verwenden, müssen in der gleichen Zone sein.

Eine Site kann je nach Anforderungen und Umgebung verschiedene Arten von Satellitenzonen enthalten. Die folgende Abbildung zeigt eine primäre Zone und Beispiele von drei Satellitenzonen.



- Die primäre Zone enthält zwei Controller, Studio, Director, StoreFront, den Lizenzserver und die Sitedatenbank (sowie hoch verfügbare SQL Server-Bereitstellungen). Die primäre Zone enthält außerdem mehrere VDAs und ein NetScaler Gateway.
- Satellitenzone 1 – VDAs mit Controller

  Satellitenzone 1 enthält einen Controller, VDAs und einen StoreFront-Server. Die VDAs in dieser Satellitenzone registrieren sich bei dem lokalen Controller. Der lokale Controller kommuniziert mit der Sitedatenbank und dem Lizenzserver in der primären Zone.

  Wenn das WAN ausfällt, kann der Controller in der Satellitenzone dank Verbindungsleasing weiterhin Verbindungen mit VDAs in dieser Zone vermitteln. Eine solche Bereitstellung ist beispielsweise an Standorten nützlich, an denen Mitarbeiter über die lokale StoreFront-Site und den lokalen Controller auf ihre lokalen Ressourcen zugreifen, was möglich ist, selbst wenn die WAN-Verbindung zwischen dem Standort und dem Unternehmensnetzwerk ausfällt.

- Satellitenzone 2 – VDAs mit redundanten Controllern

  Satellitenzone 2 enthält zwei Controller, VDAs und einen StoreFront-Server. Dieser Zonentyp bietet die größte Resilienz bei gleichzeitigem Ausfall des WANs und eines lokalen Controllers.

VDAs-Registrierung und Controllerfailover

Site mit primärer Zone und Satellitenzonen und VDAs, deren Version mindestens 7.7 ist:

- Ein VDA in der primären Zone registriert sich bei einem Controller in der primären Zone. Ein VDA in der primären Zone versucht nie eine Registrierung bei einem Controller in einer Satellitenzone.
- Ein VDA in einer Satellitenzone registriert sich bei einem lokalen Controller, sofern möglich. Dies ist der bevorzugte Controller. Sind keine lokalen Controller verfügbar (z. B. weil sie keine weiteren VDA-Registrierungen annehmen können oder weil sie ausgefallen sind), versucht der VDA die Registrierung bei einem Controller in der primären Zone. In diesem Fall bleibt der VDA in der primären Zone registriert, selbst wenn wieder ein Controller in der Satellitenzone verfügbar wird. Ein VDA in einer Satellitenzone versucht nie eine Registrierung bei einem Controller in einer anderen Satellitenzone.
- Wenn für die VDA-Ermittlung von Controllern die automatische Aktualisierung aktiviert ist und Sie bei der VDA-Installation eine Liste von Controlleradressen angegeben haben, wird aus dieser nach dem Zufallsprinzip ein Controller für die erste Registrierung ausgewählt, unabhängig davon, in welcher Zone der Controller residiert. Wenn die Maschine mit dem VDA neu gestartet wird, versucht dieser die Registrierung bei einem Controller in der lokalen Zone.
- Wenn ein Controller in einer Satellitenzone ausfällt, erfolgt, sofern möglich, ein Failover zu einem anderen lokalen Controller. Ist kein lokaler Controller verfügbar, erfolgt ein Failover auf einen Controller in der primären Zone.
- Wenn Sie einen Controller in eine Zone oder aus einer Zone verschieben und die automatische Aktualisierung aktiviert ist, erhalten die VDAs eine aktualisierte Liste der lokal und in der primären Zone angesiedelten Controller, anhand derer die Registrierung und die Annahme von Verbindungen erfolgt.
- Wenn Sie einen Maschinenkatalog in eine andere Zone verschieben, registrieren sich die VDAs in diesem Katalog bei Controllern in der Zone, in die Sie den Katalog verschoben haben. (Wenn Sie einen Katalog verschieben, verschieben Sie alle zugehörigen Hostverbindungen in die gleiche Zone.)
- Auf Controllern in der primären Zone werden Verbindungsleasingdaten für alle Zonen gespeichert. Auf Controllern in Satellitenzonen werden Verbindungsleasingdaten für die eigene Zone und die primäre Zone, jedoch nicht für die anderen Satellitenzonen gespeichert.

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 sekundären Zonen 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.

Überlegungen, Anforderungen und bewährte Methoden

- Sie können Controller, Maschinenkataloge und Hostverbindungen in einer Zone platzieren. Wenn ein Maschinenkatalog eine Hostverbindung verwendet, müssen Katalog und Verbindung in der gleichen Zone sein.

- Beim Erstellen des ersten Maschinenkatalogs und der ersten Bereitstellungsgruppe einer Produktionssite sind alle Elemente in der primären Zone. Sie können Satellitenzonen erst erstellen, wenn das anfängliche Setup abgeschlossen ist. Wenn Sie eine leere Site erstellen, enthält die primäre Zone zunächst nur einen Controller. Sie können Satellitenzonen vor oder nach dem Erstellen eines Maschinenkatalogs und einer Bereitstellungsgruppe erstellen.
- Beim Erstellen der ersten Satellitenzone mit einem oder mehreren Elementen verbleiben alle anderen Elemente der Site in der primären Zone.
- Die primäre Zone heißt standardmäßig "Primär". Sie können diesen Namen nach Wunsch ändern. Obwohl die primäre Zone in Studio als solche gekennzeichnet ist, empfiehlt sich die Verwendung eines Namens, anhand dessen sie sich leicht identifizieren lässt. Sie können die primäre Zone neu zuweisen, d. h. eine andere Zone als primäre Zone festlegen, die Sitedatenbank und alle hoch verfügbaren Server müssen jedoch immer in der primären Zone sein.
- Die Sitedatenbank muss immer in der primären Zone sein.
- Nach dem Erstellen von Zonen können Sie Elemente zwischen Zonen verschieben. Diese Flexibilität birgt jedoch das Risiko der Trennung von Elementen, die am besten in unmittelbarer Nähe zueinander funktionieren. Das Verschieben eines Maschinenkatalogs in eine andere Zone als die zugehörige Verbindung (Host), durch welche die Maschinen in dem Katalog erstellt werden, kann sich beispielsweise negativ auf die Leistung auswirken. Überlegen Sie daher vor dem Verschieben von Elementen zwischen Zonen, ob dies unerwünschte Auswirkungen haben könnte. Kataloge und zugehörige Hostverbindungen müssen in der gleichen Zone sein.
- Zur Erzielung der optimalen Leistung installieren Sie Studio und Director nur in der primären Zone. Wenn Sie eine zusätzliche Studio-Instanz in einer Satellitenzone installieren möchten, z. B. in einer Satellitenzone mit Controllern, die für ein Failover bei Ausfall der primären Zone verwendet wird, führen Sie Studio als lokal veröffentlichte Anwendung aus. Sie können auch von einer Satellitenzone auf Director zugreifen, da es eine Webanwendung ist.
- Idealerweise sollte NetScaler Gateway in einer Satellitenzone für Benutzerverbindungen aus anderen Zonen oder externen Orten verwendet werden, es kann jedoch auch für zoneninterne Verbindungen verwendet werden.

Erstellen und Verwalten von Zonen

Ein Volladministrator kann alle Aufgaben der Zonenerstellung und -verwaltung ausführen. Sie können jedoch auch eine benutzerdefinierte Rolle zum Erstellen, Bearbeiten oder Löschen einer Zone erstellen. Das Verschieben von Elementen zwischen Zonen erfordert für die Zone selbst lediglich eine Leseberechtigung. Sie benötigen jedoch die Berechtigung zum Bearbeiten der Elemente, die Sie verschieben möchten. Zum Verschieben eines Maschinenkatalogs von einer Zone in eine andere brauchen Sie beispielsweise die Berechtigung zum Bearbeiten des Maschinenkatalogs. Weitere Informationen finden Sie dem Artikel zur delegierten Administration.

Verwendung von Provisioning Services: Die Provisioning Services Console in diesem Release erkennt keine Zonen. Citrix empfiehlt daher die Verwendung von Studio zum Erstellen von Maschinenkatalogen, die Sie in Satellitenzonen platzieren möchten. Verwenden Sie den Assistenten in Studio zum Erstellen des Katalogs und geben Sie die richtige Satellitenzone an. Verwenden Sie dann die Provisioning Services Console zum Bereitstellen von Maschinen in diesem Katalog. Wenn Sie den Katalog mit dem Provisioning Services-Assistenten erstellen, wird er in die primäre Zone platziert und muss anschließend mit Studio in die Satellitenzone verschoben werden.

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Zonen**.
2. Wählen Sie im Aktionsbereich **Zone erstellen**.
3. Geben Sie einen Namen für die Zone und optional eine Beschreibung ein. Der Name muss innerhalb der Site eindeutig sein.

4. Wählen Sie die Elemente, die Sie in der neuen Zone platzieren möchten. Sie können die Liste der verfügbaren Elemente filtern oder durchsuchen. Sie können auch eine leere Zone erstellen. Wählen Sie hierfür einfach keine Elemente aus.
5. Klicken Sie auf **Speichern**.

Alternativ zu dieser Methode können Sie in Studio ein oder mehrere Elemente und im Aktionsbereich dann **Zone erstellen** wählen.

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Zonen**.
2. Wählen Sie eine Zone und dann im Aktionsbereich **Zone bearbeiten**.
3. Ändern Sie den Zonennamen und/oder die Beschreibung. Wenn Sie den Namen der primären Zone ändern, stellen Sie sicher, dass sie weiterhin eindeutig als primäre Zone identifiziert werden kann.
4. Klicken Sie auf **OK** oder **Übernehmen**.

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Zonen**.
2. Wählen Sie mindestens ein Element aus.
3. Ziehen Sie das Element in die Zielzone oder wählen Sie im Aktionsbereich **Elemente verschieben** und geben Sie dann die gewünschte Zielzone an.

Durch eine Meldung mit einer Liste der ausgewählten Elemente werden Sie aufgefordert, das Verschieben zu bestätigen.

Nicht vergessen: Wenn ein Maschinenkatalog eine Hostverbindung zu einem Hypervisor oder Clouddienst verwendet, müssen Katalog und Verbindung in der gleichen Zone sein. Andernfalls kann die Leistung leiden. Wenn Sie eines dieser Elemente verschieben, verschieben Sie auch das andere.

Eine Zone muss leer sein, damit sie gelöscht werden kann. Die primäre Zone kann nicht gelöscht werden.

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Zonen**.
2. Wählen Sie eine Zone aus.
3. Wählen Sie im Aktionsbereich **Zone löschen**. Wenn die Zone nicht leer ist, werden Sie aufgefordert, die Zone auszuwählen, in die die enthaltenen Elemente verschoben werden sollen.
4. Bestätigen Sie die Löschung.

In Sites mit mindestens einer Satellitenzone können Sie beim Hinzufügen einer Hostverbindung oder eines Controllers und beim Erstellen eines Maschinenkatalogs (nach Erstellen der Site) eine Zone für dieses Element angeben.

In den meisten Fällen ist die primäre Zone die Standardeinstellung. Wenn Sie einen Maschinenkatalog mit den Maschinenerstellungsdiensten erstellen, wird die für die Hostverbindung konfigurierte Zone automatisch ausgewählt.

Enthält die Site keine Satellitenzonen, wird die primäre Zone ausgewählt und die Option zur Auswahl der Zone wird nicht angezeigt.

Verbindungen und Ressourcen

Feb 29, 2016

Dieser Abschnitt enthält folgende Themen:

Einführung

Sie erstellen die erste Verbindung mit Hosting-Ressourcen, wenn Sie eine Site erstellen. Später können Sie die Verbindung ändern und neue Verbindungen erstellen. Beim Konfigurieren einer Verbindung wählen Sie den *Typ* der Verbindung aus der Liste unterstützter Hypervisors oder Clouddienste aus. Der von Ihnen ausgewählte Speicher und das Netzwerk sind die *Ressourcen* der Verbindung.

Lesezugriffadministratoren können die Verbindung und Ressourcendetails anzeigen. Sie müssen Volladministrator sein, um Verwaltungsaufgaben an Verbindungen und Ressourcen durchzuführen.

Mit den unterstützten Virtualisierungsplattformen können Sie Maschinen in der XenApp- oder XenDesktop-Umgebung hosten und verwalten. Sie können mit den unterstützten Cloudbereitstellungslösungen Produktkomponenten hosten und virtuelle Maschinen bereitstellen. Mit diesen Lösungen werden Computing-Ressourcen gepoolt, um öffentliche oder private Infrastructure-as-a-Service (IaaS)-Clouds sowie Hybrid-IaaS-Clouds zu erstellen.

Weitere Informationen finden Sie in den folgenden Informationsquellen:

VMware

- Artikel VMware-Virtualisierungsumgebungen
- VMware-Produktdokumentation

Microsoft Hyper-V

- Artikel Microsoft System Center Virtual Machine Manager-Virtualisierungsumgebungen
- Microsoft-Dokumentation

Microsoft Azure

- Artikel Microsoft Azure-Virtualisierungsumgebungen

- Microsoft-Dokumentation
- Beim Erstellen einer Verbindung in Studio können Sie automatisch Informationen aus einer Datei mit Veröffentlichungseinstellungen importieren, die Sie von https://manage.windowsazure.com/publishsettings/index heruntergeladen haben.

Amazon Web Services (AWS)

- CTX140427
- AWS-Dokumentation
- Beim Erstellen einer Verbindung in Studio müssen Sie den API-Schlüssel und die Werte des geheimen Schlüssels angeben. Sie können die Schlüsseldatei mit diesen Werten aus AWS oder CloudPlatform exportieren und anschließend importieren. Sie müssen auch die Werte für Region, Availability Zone, 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 von Studio nicht zum Ausfüllen der Felder "API-Schlüssel" und "Geheimer Schlüssel" verwendet werden. Verwenden Sie AWS IAM-Anmeldeinformationsdateien.

Citrix CloudPlatform

- CTX140428.
- Citrix CloudPlatform-Dokumentation
- Beim Erstellen einer Verbindung in Studio müssen Sie den API-Schlüssel und die Werte des geheimen Schlüssels angeben. Sie können die Schlüsseldatei mit diesen Werten aus CloudPlatform exportieren und anschließend importieren.

Citrix XenServer

- Citrix XenServer-Dokumentation
- Beim Erstellen einer Verbindung müssen Sie die Anmeldeinformationen eines VM-Hauptadministrators oder eines höherrangigen Benutzers eingeben.
- Citrix empfiehlt die Verwendung von HTTPS zur Sicherung der Kommunikation mit XenServer. Um HTTPS zu verwenden, müssen Sie das standardmäßig mit XenServer installierte SSL-Zertifikat ersetzen (siehe CTX128656).
- Sie können hohe Verfügbarkeit konfigurieren, wenn diese auf XenServer aktiviert ist. Citrix empfiehlt, dass Sie alle Server im Pool (über "Server mit hoher Verfügbarkeit bearbeiten") auswählen, um die Kommunikation mit XenServer zu ermöglichen, wenn der Poolmaster ausfällt.
- Sie können einen GPU-Typ und eine GPU-Gruppe oder die Passthrough-Authentifizierung auswählen, wenn der XenServer vGPU unterstützt. Es wird angezeigt, ob die Auswahl dedizierte GPU-Ressourcen umfasst.

Nutanix Acropolis

- CTX202032
- https://portal.nutanix.com/#/page/docs

Erstellen einer Verbindung und von Ressourcen

Die Hosting-Ressourcen müssen vor Erstellen einer Verbindung verfügbar sein.

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Hosting**.
2. Wählen Sie im Aktionsbereich **Verbindung und Ressourcen hinzufügen**.
3. Wählen Sie **Neue Verbindung erstellen**.
4. Wählen Sie auf der Seite **Verbindung** den Verbindungstyp und geben Sie einen Namen für die Verbindung ein. Verwenden Sie einen Namen, anhand dessen Administratoren den Hosttyp und die Adresse der Bereitstellung identifizieren können.
5. Welche zusätzlichen Informationen erforderlich sind, hängt von dem ausgewählten Verbindungstyp ab.
6. Wählen Sie die Tools, die Sie zum Erstellen von virtuellen Maschinen verwenden möchten. Für Hypervisors, die GPU-Ressourcen bereitstellen, wählen Sie **Studio-Tools**.
7. Wählen Sie auf der Seite **Speicher** die Speichertypen und Geräte. Wenn Sie Maschinenerstellungsdienste verwenden, wählen Sie das Netzwerk und Speicherressourcen für die neuen virtuellen Maschinen. Wenn Sie einen freigegebenen Speicher über XenServer-Verbindungen verwenden, können Sie IntelliCache aktivieren, um die Last auf dem Speichergerät zu reduzieren. Weitere Informationen zum Verwenden von IntelliCache finden Sie weiter unten.

8. Wenn die Verbindung GPU-Funktionen bietet, wählen Sie die Option zur Verwendung der Grafikvirtualisierung und anschließend einen GPU-Typ und eine GPU-Gruppe.
9. Geben Sie einen Namen für die Ressourcen ein.

Erstellen von Ressourcen und einer Verbindung aus einer vorhandenen Verbindung

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Hosting**.
2. Wählen Sie im Aktionsbereich **Verbindung und Ressourcen hinzufügen**.
3. Wählen Sie **Vorhandene Verbindung verwenden** und dann die gewünschte Verbindung.
4. Wählen Sie die Tools, die Sie zum Erstellen von virtuellen Maschinen verwenden möchten. Für Hypervisors, die GPU-Ressourcen bereitstellen, wählen Sie **Studio-Tools**. Wenn die Verbindung GPU-Funktionen bietet, wählen Sie die Option zur Verwendung der Grafikvirtualisierung und anschließend einen GPU-Typ und eine GPU-Gruppe.
5. Geben Sie einen Namen für die Ressourcen ein.

Speicher hinzufügen

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Hosting**.
2. Wählen Sie eine Verbindung und dann im Aktionsbereich **Speicher hinzufügen**.
3. Wählen Sie den hinzuzufügenden Speicher aus.

Bearbeiten des Speichers

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Hosting**.
2. Wählen Sie einen Ressourceneintrag unter einer Verbindung und dann im Aktionsbereich **Speicher bearbeiten**.
3. Aktivieren oder deaktivieren Sie auf der Seite **Standardspeicher** die Kontrollkästchen für die Speicherorte, an denen virtuelle Maschinen gespeichert werden. Wenn Sie einen Speicherort deaktivieren, der neue Maschinen angenommen hat, nimmt dieser keine weiteren neuen Maschinen an. Vorhandene Maschinen verwenden weiterhin diesen Speicherort (und schreiben Daten hinein). Daher kann ein Speicherort voll werden, selbst wenn keine neuen Maschinen mehr angenommen werden.
   Bei Verwendung eines Personal vDisk-Speichers aktivieren oder deaktivieren Sie die Kontrollkästchen auf der Seite **PvD-Speicher** ebenfalls.

Bearbeiten einer Verbindung

Verwenden Sie diese Vorgehensweise nicht, um eine Verbindung umzubenennen oder eine neue Verbindung zu erstellen. Dafür sind andere Schritte erforderlich.

Sie können die GPU-Einstellungen für eine Verbindung nicht ändern, da Maschinenkataloge, die auf diese Ressource zugreifen, ein entsprechendes GPU-spezifisches Masterimage verwenden müssen. Erstellen Sie eine neue Verbindung.

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Hosting**.

2. Wählen Sie die Verbindung und dann im Aktionsbereich **Verbindung bearbeiten**.
3. Folgen Sie den Anweisungen unten bei der Auswahl der Einstellungen zum Bearbeiten einer Verbindung.

Seite **Verbindungseigenschaften**:

- Zum Ändern der Verbindungsadresse und -anmeldeinformationen wählen Sie **Einstellungen bearbeiten** und geben die neuen Informationen ein.
- Zum Festlegen der Server mit hoher Verfügbarkeit für eine XenServer-Verbindung wählen Sie **Server mit hoher Verfügbarkeit bearbeiten**. Citrix empfiehlt, dass Sie alle Server im Pool auswählen, um die Kommunikation mit XenServer zu ermöglichen, wenn der Poolmaster ausfällt.

Seite **Erweitert**:

Für eine Wake-On-LAN-Verbindung unter Microsoft System Center Configuration Manager, die mit Remote-PC-Zugriff verwendet wird, geben Sie ConfigMgr Wake Proxy, Magic Packets und Paketübertragungsinformationen an.

Über die Einstellungen für den Einschränkungsschwellenwert können Sie eine maximale Anzahl von Energieaktionen für eine Verbindung festlegen. Diese Einstellungen können nützlich sein, wenn durch die Energieverwaltungseinstellungen der gleichzeitige Start zu vieler oder zu weniger Maschinen zugelassen wird.

- Über **Gleichzeitige Aktionen (alle Typen)** und **Gleichzeitige Updates für Personal vDisk-Inventar** wird Folgendes festgelegt: die maximale absolute Zahl Aktionen/Updates, die gleichzeitig an dieser Verbindung auftreten dürfen und den maximalen Prozentsatz aller Maschinen, die diese Verbindung verwenden. Sie müssen beide Werte angeben, angewendet wird der geringere der Werte.

  Beispiel: Wird in einer Bereitstellung mit 34 Maschinen die Einstellung **Gleichzeitige Aktionen (alle Typen)** auf einen absoluten Wert von 10 und einen Prozentsatz von 10 festgelegt, wird als tatsächliches Limit 3 angewendet (d. h. 10 Prozent von 34 auf die nächste Ganzzahl gerundet – ein kleinerer Wert als die absolute Zahl von 10 Maschinen).

- Der Wert für **Höchstanzahl neue Aktionen pro Minute** ist eine absolute Zahl, kein Prozentwert.

Für jeden Verbindungstyp gibt es bestimmte Standardwerte, die in den meisten Fällen geeignet sind und in der Regel nicht geändert werden sollten.

Hinweis: Geben Sie die Informationen im Feld **Verbindungsoptionen** nur unter der Anleitung eines Supportmitarbeiters von Citrix ein.

Aktivieren und Deaktivieren des Wartungsmodus für eine Verbindung

Wenn Sie den Wartungsmodus für eine Verbindung aktivieren, können keine neuen Energieaktionen auf in dieser Verbindung gespeicherten Maschinen stattfinden. Benutzer können keine Verbindung mit einer Maschine herstellen, wenn sie im Wartungsmodus ist. Wenn Benutzer bereits verbunden sind, wird der Wartungsmodus wirksam, sobald sich die Benutzer abmelden.

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Hosting**.
2. Wählen Sie die Verbindung aus. Zum Aktivieren des Wartungsmodus wählen Sie im Aktionsbereich **Wartungsmodus einschalten**. Zum Deaktivieren des Wartungsmodus wählen Sie **Wartungsmodus ausschalten**.

Sie können den Wartungsmodus auch für einzelne Maschinen ein- und ausschalten (siehe unten). Darüber hinaus können Sie den Wartungsmodus auch für Maschinen in Maschinenkatalogen und Bereitstellungsgruppen aktivieren oder deaktivieren.

Löschen einer Verbindung

Achtung: Das Löschen einer Verbindung kann zur Folge haben, dass eine große Zahl von Maschinen gelöscht wird, Datenverlust eingeschlossen. Stellen Sie sicher, dass die Benutzerdaten auf den betroffenen Maschinen gesichert wurden oder nicht mehr benötigt werden.

Vor dem Löschen einer Verbindung müssen Sie Folgendes sicherstellen:

- Alle Benutzer sind von den in dieser Verbindung gespeicherten Maschinen abgemeldet.
- Es werden keine getrennten Benutzersitzungen ausgeführt.
- Der Wartungsmodus wird für gepoolte und dedizierte Maschinen aktiviert.
- Alle Maschinen in den von der Verbindung verwendeten Maschinenkatalogen sind ausgeschaltet.

Ein Maschinenkatalog kann nicht mehr verwendet werden, wenn Sie eine Verbindung löschen, auf die dieser Katalog verweist. Verweist ein Katalog auf diese Verbindung, haben Sie die Option zum Löschen des Katalogs. Stellen Sie vor dem Löschen eines Katalogs sicher, dass er nicht von anderen Verbindungen verwendet wird.

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Hosting**.
2. Wählen Sie die Verbindung und dann im Aktionsbereich **Verbindung löschen**.
3. Wenn für die Verbindung Maschinen gespeichert sind, werden Sie gefragt, ob die Maschinen gelöscht werden sollen. Wenn dies der Fall ist, geben Sie an, was mit dem zugewiesenen Active Directory-Computerkonten passieren soll.

Umbenennen einer Verbindung

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Hosting**.
2. Wählen Sie die Verbindung und dann im Aktionsbereich **Verbindung umbenennen**.

Anzeigen von Maschinendetails für eine Verbindung

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Hosting**.
2. Wählen Sie die Verbindung und dann im Aktionsbereich **Maschinen anzeigen**.

Im oberen Bereich werden die Maschinen angezeigt, auf die über die Verbindung zugegriffen wird. Wählen Sie eine Maschine aus, um die Details im unteren Bereich anzuzeigen. Für geöffnete Sitzungen werden auch Sitzungsdetails angezeigt.

Sie können das Suchfeature verwenden, um Maschinen schnell aufzufinden. Wählen Sie entweder eine gespeicherte Suche aus der Liste im oberen Bereich des Bildschirms aus oder erstellen Sie eine neue Suche. Sie können nach dem Maschinennamen suchen, indem Sie den ganzen Namen oder einen Teil des Namens eingeben. Alternativ können Sie auch einen Ausdruck für eine erweiterte Suche erstellen. Klicken Sie auf die Erweiterungsschaltfläche, um einen Ausdruck zu erstellen, und wählen Sie dann aus den angezeigten Listen Eigenschaften und Operatoren aus.

Verwalten von Maschinen einer Verbindung

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Hosting**.
2. Wählen Sie eine Verbindung und dann im Aktionsbereich **Maschinen anzeigen**.
3. Wählen Sie eine der folgenden Aktionen im Aktionsbereich. Abhängig vom Maschinenzustand und dem Verbindungshosttyp sind einige Aktionen möglicherweise nicht verfügbar.

- **Starten**: Die Maschine wird gestartet, wenn sie ausgeschaltet oder angehalten ist.
- **Anhalten**: Die Maschine wird ohne Herunterfahren angehalten die Liste der Maschinen wird aktualisiert.
- **Herunterfahren**: Das Betriebssystem wird aufgefordert, herunterzufahren.
- **Herunterfahren erzwingen**: Die Maschine wird zwingend abgeschaltet und die Liste der Maschinen wird aktualisiert.
- **Neu starten**: Das Betriebssystem wird heruntergefahren und die Maschine wird neu gestartet. Wenn das Betriebssystem diese Aufgaben nicht ausführen kann, bleibt der Desktop im aktuellen Zustand.
- **Wartungsmodus aktivieren:** Die Verbindungen zu einer Maschine werden vorübergehend unterbrochen. Benutzer können keine Verbindung mit einer Maschine in diesem Zustand herstellen. Wenn Benutzer verbunden sind, wird der Wartungsmodus wirksam, sobald sich die Benutzer abmelden. Sie können den Wartungsmodus auch für alle Maschinen aktivieren bzw. deaktivieren, auf die über eine Verbindung zugegriffen wird (siehe oben).
- **Aus Bereitstellungsgruppe entfernen**: Beim Entfernen einer Maschine aus einer Bereitstellungsgruppe wird sie nicht aus dem von der Bereitstellungsgruppe verwendeten Maschinenkatalog gelöscht. Sie können eine Maschine nur entfernen, wenn keine Benutzer mit ihr verbunden sind; aktivieren Sie den Wartungsmodus, um zu verhindern, dass Benutzer eine Verbindung herstellen, während Sie die Maschine entfernen.
- **Löschen**: Wenn Sie eine Maschine löschen, können Benutzer nicht mehr darauf zugreifen und die Maschine wird aus dem Maschinenkatalog gelöscht. Stellen Sie vor dem Löschen einer Maschine sicher, dass alle Benutzerdaten gesichert wurden oder nicht mehr benötigt werden. Sie können eine Maschine nur löschen, wenn keine Benutzer mit ihr verbunden sind; aktivieren Sie den Wartungsmodus, um zu verhindern, dass Benutzer eine Verbindung herstellen, während Sie die Maschine löschen.

Bei Aktionen, bei denen eine Maschine heruntergefahren wird, wird diese ausgeschaltet, wenn das Herunterfahren nicht innerhalb von 10 Minuten erfolgt. Wenn Windows versucht, während des Herunterfahrens Updates zu installieren, besteht die Gefahr, dass die Maschine ausgeschaltet wird, bevor die Updates abgeschlossen sind.

Löschen, Umbenennen oder Testen von Ressourcen

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Hosting**.
2. Wählen Sie die Ressource aus und wählen Sie dann den entsprechenden Eintrag im Aktionsbereich: **Ressourcen löschen**, **Ressourcen umbenennen** oder **Ressourcen testen**.

Verwenden von IntelliCache für XenServer-Verbindungen

Durch den Einsatz von IntelliCache werden gehostete VDI-Bereitstellungen kostengünstiger, da eine Kombination aus freigegebenem und lokalem Speicher verwendet werden kann. Dies verbessert die Leistung und reduziert den Datenverkehr im Netzwerk. Das Masterimage aus dem freigegebenen Speicher wird im lokalen Speicher zwischengespeichert, wodurch die

Anzahl der Lesevorgänge im freigegebenen Speicher reduziert wird. Bei gemeinsam genutzten Desktops werden Schreibvorgänge auf den differenzierenden Festplatten in den lokalen Speicher auf dem Host und nicht in den gemeinsam genutzten Speicher geschrieben.

- Der freigegebene Speicher muss NFS sein, wenn Sie IntelliCache verwenden.
- Citrix empfiehlt die Verwendung eines lokalen Speichergeräts mit hoher Leistung, um eine schnellstmögliche Datenübertragung zu gewährleisten.

Um IntelliCache zu verwenden, müssen Sie es in diesem Produkt und XenServer aktivieren.

- Bei der Installation von XenServer, wählen Sie **Enable thin provisioning (Optimized storage for XenDesktop)**. Citrix bietet keine Unterstützung für gemischte Serverpools, auf denen IntelliCache auf manchen Servern aktiviert ist und auf anderen nicht. Weitere Informationen finden Sie in der Dokumentation für XenServer.
- In XenApp und XenDesktop ist IntelliCache standardmäßig deaktiviert. Sie können die Einstellung nur beim Erstellen einer XenServer-Verbindung ändern, IntelliCache kann später nicht deaktiviert werden. Gehen Sie folgendermaßen vor, wenn Sie eine XenServer-Verbindung von Studio aus hinzufügen:
  - Wählen Sie als Speichertyp **Freigegeben** aus.
  - Aktivieren Sie das Kontrollkästchen **IntelliCache verwenden**.

Verbindungstimer

Sie können mit Richtlinieneinstellungen drei Verbindungstimer konfigurieren:

- **Timer für längste Verbindung:** Diese Einstellung legt die Höchstdauer einer ununterbrochenen Verbindung zwischen einem Benutzergerät und einem Desktop fest. Verwenden Sie die Richtlinieneinstellungen **Sitzungsverbindungstimer** und **Sitzungsverbindung - Timerintervall**.
- **Timer für inaktive Verbindungen:** Diese Einstellung legt fest, wie lange eine ununterbrochene Verbindung zwischen einem Benutzergerät und einem virtuellen Desktop erhalten wird, wenn keine Eingabe vom Benutzer erfolgt. Verwenden Sie die Richtlinieneinstellungen **Sitzungsleerlauftimer** und **Sitzungsleerlauf - Timerintervall**.
- **Timer für getrennte Verbindungen:** Diese Einstellung legt fest, wie lange ein getrennter, gesperrter virtueller Desktop gesperrt bleibt, bis die Sitzung abgemeldet wird. Verwenden Sie die Richtlinieneinstellungen **Timer für getrennte Sitzung** und **Getrennte Sitzungen - Timerintervall**.

Wenn Sie eine dieser Einstellungen aktualisieren, achten Sie darauf, dass sie in der ganzen Bereitstellung konsistent sind.

Verbindungsleasing

Feb 29, 2016

Um sicherzustellen, dass die Sitedatenbank immer verfügbar ist, empfiehlt Citrix, unter Befolgung der bewährten Methoden zur hohen Verfügbarkeit von Microsoft mit einer fehlertoleranten SQL Server-Bereitstellung zu beginnen. Delivery Controller können jedoch aufgrund von Netzwerkproblemen und Unterbrechungen möglicherweise nicht auf die Datenbank zugreifen, was dazu führt, dass Benutzer keine Verbindung mit ihren Anwendungen oder Desktops herstellen können.

Das Feature für Verbindungsleasing ergänzt die bewährten Methoden zur hohen Verfügbarkeit bei SQL Server, da es Benutzern die Wiederverbindung mit den zuletzt verwendeten Anwendungen und Desktops ermöglicht, selbst wenn die Sitedatenbank nicht verfügbar ist.

Benutzer verfügen zwar über eine große Anzahl veröffentlichter Ressourcen, verwenden jedoch oft nur wenige davon regelmäßig. Wenn Sie das Verbindungsleasing aktivieren, werden die Benutzerverbindungen mit den zuletzt verwendeten Anwendungen und Desktops im Normalbetrieb (wenn die Datenbank verfügbar ist) von jedem Controller zwischengespeichert.

Die auf jedem Controller generierten Leases werden in die Sitedatenbank für eine regelmäßige Synchronisierung mit den anderen Controllern der Site hochgeladen. Neben den Leases werden in jedem Controllercache Informationen zu Anwendung, Desktop, Symbol und Worker gespeichert. Lease und zugehörige Informationen werden auf dem lokalen Datenträger eines jeden Controllers gespeichert. Wenn die Datenbank nicht mehr verfügbar ist, wechselt der Controller in den Leasingverbindungsmodus und beim Versuch der Herstellung oder des Neuaufbaus einer Verbindung mit einer kürzlich verwendeten Anwendung oder einem kürzlich verwendeten Desktop von StoreFront aus werden die zwischengespeicherten Vorgänge "abgespielt".

Die Verbindungen werden für eine Leasedauer von zwei Wochen zwischengespeichert. Wenn die Datenbank nicht verfügbar ist, besteht daher über StoreFront Zugriff auf die Desktops und Anwendungen, die in den vorherigen zwei Wochen gestartet wurden. Auf Desktops und Anwendungen, die nicht während der zweiwöchigen Leasedauer gestartet wurden, kann jedoch nicht zugegriffen werden, wenn die Datenbank nicht verfügbar ist. Wenn eine Anwendung z. B. vor drei Wochen gestartet wurde, ist ihre Lease abgelaufen und sie kann bei Nichtverfügbarkeit der Datenbank nicht gestartet werden. Leases für langwährende aktive oder getrennte Anwendungen oder Desktopsitzungen werden verlängert und somit nicht als abgelaufen behandelt.

Standardmäßig gilt das Verbindungsleasing für die komplette Site. Sie können jedoch alle Leases für bestimmte Benutzer widerrufen, wodurch verhindert wird, dass diese auf Anwendungen oder Desktops zugreifen können, wenn der Controller im Leasingverbindungsmodus ausgeführt wird. Mehrere weitere Registrierungseinstellungen gelten pro Controller.

Das Verbindungsleasing kann zwar die Verbindungsresilienz und die Produktivität der Benutzer verbessern, es sind jedoch Überlegungen im Hinblick auf Verfügbarkeit, Betrieb und Leistung anderer Funktionen anzustellen.

Das Verbindungsleasing wird für servergehostete Anwendungen und Desktops und statische (zugewiesene) Desktops unterstützt. Es wird nicht unterstützt für gepoolte VDI-Desktops oder Benutzer, denen kein Desktop zugewiesen wurde, wenn die Datenbank betriebsunfähig wird.

Wenn der Controller im Leasingverbindungsmodus ist, gilt Folgendes:

- Administratoren können Studio, Director und die PowerShell-Konsole nicht verwenden.
- Workspace Control ist nicht verfügbar. Wenn sich ein Benutzer bei Citrix Receiver anmeldet, werden Sitzungen nicht

automatisch wieder verbunden. Der Benutzer muss die Anwendung neu starten.

- Wenn eine neue Lease unmittelbar vor dem Nichtverfügbarwerden der Datenbank erstellt wurde, die Leaseinformationen jedoch noch nicht auf allen Controllern synchronisiert wurden, können Benutzer möglicherweise eine betroffene Ressource nicht starten.
- Benutzer servergehosteter Anwendungen und Desktops können möglicherweise mehr Sitzungen verwenden als das für sie konfigurierte Sitzungslimit zulässt. Beispiel:
  - Ein Benutzer stellt eine Verbindung von einem Gerät (extern über NetScaler Gateway) her, während der Controller im normalen Verbindungsmodus ist. Später stellt der Benutzer von einem anderen Gerät im LAN eine Verbindung her, während Controller im Leasingverbindungsmodus ist. In diesem Fall findet möglicherweise kein Roaming der Sitzung statt.
  - Die Wiederverbindung einer Sitzung kann fehlschlagen, wenn eine Anwendung startet, kurz bevor die Datenbank betriebsunfähig wird. In diesem Fall werden eine neue Sitzung und Anwendungsinstanz gestartet.
- Bei statischen (zugewiesenen) Desktops findet keine Energieverwaltung statt. VDAs, die beim Umschalten des Controllers in den Leasingverbindungsmodus ausgeschaltet werden, stehen erst wieder zur Verfügung, wenn die Datenbankverbindung wiederhergestellt ist, es sei denn, der Administrator schaltet sie manuell ein.
- Sind Sitzungsvorabstart und Sitzungsfortbestehen aktiviert, werden neue Vorabstartsitzungen nicht gestartet. Vorab gestartete und fortbestehende Sitzungen werden während der Nichtverfügbarkeit der Datenbank nicht entsprechend den konfigurierten Schwellenwerten beendet.
- Die Lastverwaltung der Site kann beeinträchtigt werden. Serverbasierte Verbindungen werden an den zuletzt verwendeten VDA geleitet. Lastauswertungsprogramme (und insbesondere Sitzungszahlregeln) werden möglicherweise überschritten.
- Der Controller wechselt nicht in den Leasingverbindungsmodus, wenn Sie die Datenbank mit SQL Server Management Studio offline nehmen. Verwenden Sie stattdessen eine der folgenden Transact-SQL-Anweisungen:
  - ALTER DATABASE <Datenbankname> SET OFFLINE WITH ROLLBACK IMMEDIATE
  - ALTER DATABASE <Datenbankname> SET OFFLINE WITH ROLLBACK AFTER <Sekunden>

  Beide Anweisungen beenden ausstehende Transaktionen und trennen die Verbindung des Controllers mit der Datenbank. Der Controller wechselt dann in den Leasingverbindungsmodus.

Beim Verbindungsleasing gibt es zwei kurze Intervalle, während derer Benutzer keine Verbindung (wieder)herstellen können: (1) zwischen dem Zeitpunkt, zu dem die Datenbank betriebsunfähig wird bis zum Umschalten des Controllers in den Leasingverbindungsmodus und (2) vom Zeitpunkt des Umschaltens des Controllers vom Leasingverbindungsmodus bis der Datenbankzugriff vollständig wiederhergestellt ist und die VDAs erneut registriert sind.

Wenn Sie einen nicht standardmäßigen Wert für das Sitzungsroaming festlegen und ein Controller auf eine geleaste Verbindung schaltet, tritt bei Sitzungswiederverbindung wieder der Standardwert in Kraft. Weitere Informationen finden Sie unter Verbindungsleasing und Sitzungsroaming.

Informationen zum Speicherort der Verbindungsleasingdaten finden Sie in dem Artikel Zonen.

Weitere Überlegungen finden Sie unter XenDesktop 7.6 Connection Leasing Design Considerations.

Beim Konfigurieren der Bereitstellung zum Ermöglichen des Verbindungsleasings ist Folgendes zu beachten:

- VDAs müssen mindestens in Version 7.6 und die Maschinenkataloge und Bereitstellungsgruppen, die diese Maschinen verwenden, müssen in der entsprechenden Mindestversion vorliegen.
- Die Speicherplatzanforderungen der Sitedatenbank sind größer.
- Jeder Controller erfordert zusätzlichen Speicherplatz für die zwischengespeicherten Leasedateien.

Das Verbindungsleasing ist standardmäßig aktiviert.

Sie können das Verbindungsleasing im PowerShell-SDK oder in der Windows-Registrierung deaktivieren und aktivieren. Im PowerShell-SDK können Sie auch aktuelle Leases entfernen. Die folgenden PowerShell-Cmdlets wirken sich auf das Verbindungsleasing aus. Informationen hierzu finden Sie in der Cmdlet-Hilfe.

- Set-BrokerSite -ConnectionLeasingEnabled $true | $false: Aktiviert bzw. deaktiviert das Verbindungsleasing. Standard = $true
- Get-BrokerServiceAddedCapability: Gibt "ConnectionLeasing" für den lokalen Controller aus.
- Get-BrokerLease: Ruft alle Leases oder einen gefilterten Satz aktueller Leases auf.
- Remove-BrokerLease: Markiert alle Leases oder einen gefilterten Satz Leases zum Löschen.
- Update-BrokerLocalLeaseCache: aktualisiert den Cache für das Verbindungsleasing auf dem lokalen Controller. Bei der nächsten Synchronisierung werden die Daten neu synchronisiert.

Virtuelle IP-Adressen und virtuelles Loopback

Feb 29, 2016

Hinweis: Diese Features gelten nur für Maschinen unter Windows Server 2008 R2 und Windows Server 2012 R2. Sie gelten nicht für Windows-Desktopbetriebssystemmaschinen.

Die Microsoft virtuelle IP-Adresse stellt einer veröffentlichten Anwendung eine eindeutige dynamisch zugeordnete IP-Adresse für jede Sitzung bereit. Mit dem Citrix Feature des virtuellen Loopbacks können Sie Anwendungen, die mit dem lokalen Host (localhost) kommunizieren (normalerweise 127.0.0.1), so konfigurieren, dass sie eine eindeutige virtuelle Loopbackadresse im Bereich des lokalen Hosts verwenden (127.*).

Einige Anwendungen, z. B. CRM oder CTI, verwenden eine IP-Adresse für die Adressierung, Lizenzierung, Identifizierung und andere Zwecke und erfordern daher eine eindeutige IP-Adresse oder eine Loopbackadresse in Sitzungen. Andere Anwendungen binden sich möglicherweise an einen statischen Port an, sodass das Starten weitere Instanzen einer Anwendung in Mehrbenutzerumgebungen fehlschlägt, da der Port bereits verwendet wird. Damit solche Anwendungen in einer XenApp-Umgebung richtig ausgeführt werden können, benötigen Sie für jedes Gerät eine eindeutige IP-Adresse.

Virtuelle IP-Adressen und virtuelles Loopback sind unabhängige Features. Sie können ein Feature oder beide wählen.

Zusammenfassung der Administratoraktion:

- Zur Verwendung von Microsoft virtuellen IPs aktivieren und konfigurieren Sie die Funktion auf dem Windows-Server.
- Für die Verwendung von virtuellem Loopback von Citrix konfigurieren Sie zwei Einstellungen in einer Citrix Richtlinie.

Wenn die virtuelle IP aktiviert und auf dem Windows-Server konfiguriert ist, scheint jede konfigurierte Anwendung, die in einer Sitzung ausgeführt wird, eine eindeutige Adresse zu haben. Benutzer greifen auf diese Anwendungen auf einem XenApp-Server genauso wie auf andere veröffentlichte Anwendungen zu. Ein Prozess erfordert die virtuelle IP in den folgenden Fällen:

- Der Prozess verwendet eine hartcodierte TCP-Portnummer
- Der Prozess verwendet Windows Sockets und benötigt eine eindeutige IP-Adresse oder eine angegebene TCP-Portnummer

Ermitteln, ob eine Anwendung virtuelle IP-Adressen verwenden muss

1. Beziehen Sie das TCPView-Tool von Microsoft. Das Programm zeigt alle Anwendungen an, die an spezifische IP-Adressen und Ports binden.
2. Deaktivieren Sie das Auflösen von IP-Adressen, sodass statt der Adressen die Hostnamen angezeigt werden.
3. Starten Sie die Anwendung und ermitteln Sie mit TCPView, welche IP-Adressen und Ports von der Anwendung geöffnet werden und welche Prozesse diese Ports öffnen.
4. Konfigurieren Sie alle Prozesse, die die IP-Adresse des Servers, 0.0.0.0 oder 127.0.0.1, öffnen.
5. Starten Sie eine zusätzliche Instanz der Anwendung, um sicherzustellen, dass sie nicht dieselbe IP-Adresse auf einem anderen Port öffnet.

Funktionsweise von Microsoft Remote Desktop-Virtualisierung

- Die virtuelle IP-Adressierung muss auf dem Microsoft Server aktiviert sein.
  Beispiel: In einer Umgebung mit Windows Server 2008 R2 erweitern Sie im Server-Manager "Remotedesktopdienste > Remotedesktop-Sitzungshostverbindungen", um das Remotedesktop-IP-Virtualisierungsfeature zu aktivieren, und konfigurieren Sie die Einstellungen so, dass IP-Adressen dynamisch mit dem DHCP-Server pro Sitzung oder pro Programm zugewiesen werden. Weitere Informationen finden Sie in der Microsoft Dokumentation.

- Nach der Aktivierung des Features fordert der Server beim Sitzungsstart dynamisch zugewiesene IP-Adressen vom DHCP-Server an.
- Das Remotedesktop-IP-Virtualisierungsfeature weist den Remotedesktopverbindungen die IP-Adressen pro Sitzung oder pro Programm zu. Wenn Sie IP-Adressen für mehrere Programme zuweisen, verwenden sie eine gemeine IP-Adresse pro Sitzung.
- Wenn einer Sitzung eine Adresse zugewiesen wurde, verwendet die Sitzung die virtuelle Adresse statt der primären IP-Adresse des Systems bei den folgenden Aufrufen: Bind, Closesocket, Connect, WSAConnect, WSAAccept, getpeername, getsockname, sendto, WSASendTo, WSASocketW, gethostbyaddr, getnameinfo, getaddrinfo

Wenn das IP-Virtualisierungsfeature von Microsoft in der Hostingkonfiguration der Remotedesktopsitzung verwendet wird, sind Anwendungen an bestimmte IP-Adressen gebunden, indem eine Filterkomponente zwischen die Anwendung und den Winsock-Funktionsaufrufen eingefügt wird. Die Anwendung erkennt dann nur die IP-Adresse, die sie verwenden soll. Sollte die Anwendung versuchen, TCP- oder UDP-Kommunikation abzuhören, wird sie automatisch an die zugewiesene virtuelle IP-Adresse (oder Loopbackadresse) gebunden und alle von der Anwendung geöffneten Ausgangsverbindungen gehen von der an die Anwendung gebundene IP-Adresse aus.

In Funktionen, die eine Adresse ausgeben, wie z. B. GetAddrInfo() (über eine Windows--Richtlinie gesteuert), untersucht die virtuelle IP beim Abrufen der IP-Adresse des lokalen Hosts die zurückgegebene IP-Adresse und ändert sie in die virtuelle IP-Adresse der Sitzung. Anwendungen, die mit solchen Namensfunktionen versuchen, die IP-Adresse des lokalen Servers zu ermitteln, erhalten nur die eindeutige virtuelle IP-Adresse, die der Sitzung zugeordnet wurde. Diese IP-Adresse wird oft in späteren Socket-Aufrufen, wie "Bind" oder "Connect", verwendet.

Oft fordern Anwendungen eine Bindung an einen Port zum Abhören der Adresse 0.0.0.0. Wenn eine Anwendung dies versucht und einen statischen Port verwendet, können Sie höchstens eine Instanz der Anwendung starten. Das virtuelle IP-Adressfeature sucht in diesen Aufrufen nach 0.0.0.0 und ändert den Abruf so, dass die angegebene virtuelle IP-Adresse abgehört wird. Dies ermöglicht, dass mehrere Anwendungen denselben Port auf demselben Computer abhören, da sie auf verschiedenen Adressen abhören. Der Aufruf wird nur geändert, wenn er in einer ICA-Sitzungen erfolgt und virtuelle IP-Adressen aktiviert sind. Beispiel: Wenn zwei Instanzen einer Anwendung, die in unterschiedlichen Sitzungen ausgeführt werden, eine Bindung mit allen Schnittstellen (0.0.0.0) und einen bestimmten Port (z. B. 9000) versuchen, werden sie an VIPAddress1:9000 und VIPAddress2:9000 gebunden und es gibt keinen Konflikt.

Bei Aktivierung der Citrix Richtlinieneinstellungen für virtuelles Loopback kann jede Sitzung eine eigene Loopbackadresse für die Kommunikation haben. Verwendet eine Anwendung in einem Winsock-Aufruf die Adresse des lokalen Hosts (Standard ist 127.0.0.1), ersetzt das virtuelle Loopback die Adresse 127.0.0.1 einfach durch 127.X.X.X ersetzt, wobei X.X.X die Sitzungs-ID + 1 ist. Wenn die Sitzungs-ID zum Beispiel 7 ist, ist die Adresse 127.0.0.8. Im unwahrscheinlichen Fall, dass die Sitzungs-ID größer ist, als im vierten Oktett zulässig (mehr als 255), wird beim nächsten Oktett weitergemacht (127.0.1.0) bis zum Maximum von 127.255.255.255.

Ein Prozess erfordert das virtuelle Loopback in den folgenden Fällen:
- Der Prozess verwendet die Windows- Sockets-Loopbackadresse (localhost) (127.0.0.1)
- Der Prozess verwendet eine hartcodierte TCP-Portnummer

Verwenden Sie die Richtlinieneinstellungen für virtuelles Loopback für Anwendungen, die eine Loopbackadresse für prozessübergreifende Kommunikation verwenden. Eine zusätzliche Konfiguration ist nicht erforderlich. Virtuelles Loopback ist nicht von virtueller IP abhängig, sodass der Microsoft-Server nicht konfiguriert werden muss.
- Virtuelle IP - Loopbackunterstützung: Wenn diese Richtlinieneinstellung aktiviert ist, kann jede Sitzung eine eigene virtuelle Loopbackadresse haben. Diese Einstellung ist standardmäßig aktiviert. Das Feature gilt nur für Anwendungen, die

mit der Richtlinieneinstellung Virtuelle IP - Programme für virtuelles Loopback angegeben wurden.
- Virtuelle IP - Programme für virtuelles Loopback: Mit dieser Richtlinieneinstellung geben Sie die Anwendung an, die das Feature "Virtuelles IP-Loopback" verwenden. Diese Einstellung gilt nur, wenn die Richtlinieneinstellung Virtuelle IP - Loopbackunterstützung aktiviert ist.

Verwandtes Feature

Mit den folgenden Registrierungseinstellungen stellen Sie sicher, dass virtuelles Loopback den Vorrang vor virtuelle IP erhält; dies wird als bevorzugtes Loopback bezeichnet. Achten Sie jedoch auf Folgendes:
- Bevorzugtes Loopback wird nur unter Windows 2008 R2 unterstützt.
- Verwenden Sie bevorzugtes Loopback nur, wenn virtuellen IP-Adressen und das virtuelle Loopback aktiviert sind, sonst erhalten Sie u. U. unerwartete Ergebnisse.
- Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.

Führen Sie regedit auf den Servern aus, auf dem die Anwendungen installiert sind.
- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\VIP (HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VIP für 32-Bit-Maschinen)
- Name: PreferLoopback, Typ: REG_DWORD, Wert: 1
- Name: PreferLoopbackProcesses, Typ: REG_MULTI_SZ Wert:

Delivery Controller

Feb 29, 2016

Der Delivery Controller ist die serverseitige Komponente, die für die Verwaltung des Benutzerzugriffs sowie das Brokering und Optimieren von Verbindungen zuständig ist. Controller stellen auch die Maschinenerstellungsdienste zur Erstellung von Desktop- und Serverimages bereit.

Eine Site muss mindestens über einen Controller verfügen. Nach der Installation des ersten Controllers können Sie im Rahmen der Siteerstellung oder auch später weitere Controller hinzufügen. Es gibt zwei Hauptvorteile, mehr als einen Controller in einer Site zu haben.

- Redundanz: Als bewährte Methode sollte eine Produktionssite immer mindestens zwei Controller auf unterschiedlichen physischen Servern haben. Wenn ein Controller ausfällt, können die anderen die Verwaltung der Verbindungen und der Site übernehmen.
- Skalierbarkeit: Je intensiver die Aktivität einer Site, umso mehr nehmen CPU-Auslastung auf dem Controller und die Datenbankaktivität zu. Zusätzliche Controller bieten die Möglichkeit, mehr Benutzer, Anwendungen und Desktopanforderungen zu verarbeiten und die Reaktionszeit insgesamt zu verbessern.

Jeder Controller kommuniziert direkt mit der Sitedatenbank. In einer Site mit mehreren Zonen kommunizieren die Controller in jeder Zone mit der Datenbank in der primären Zone.

Tipp: Ändern Sie weder den Computernamen noch die Domänenmitgliedschaft eines Controllers, nachdem Sie die Site konfiguriert haben.

Erkennen von Controllern durch VDAs

VDAs können erst verwendet werden, wenn sie bei einem Controller der Site registriert wurden (Herstellen der Kommunikation). Zur Suche eines Controllers überprüft der VDA die Controllerliste "ListofDDCs". Die Liste "ListOfDDCs" enthält einen oder mehrere DNS-Einträge oder IP-Adressen, die den VDA an die Controller der Site verweisen. Um einen Lastausgleich zu erzielen, verteilt der VDA die Verbindungen automatisch über alle Controller in der Liste.

Neben der Liste "ListOfDDCs" gibt es die Liste "ListOfSIDs", in der festgelegt ist, über welche Sicherheits-IDs (SIDs) der VDA als Controller angesprochen werden kann. 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.

Die Listen "ListOfDDCs" und "ListOfSIDs" müssen auf allen VDAs auf dem neuesten Stand sein, wenn Controller in der Site hinzugefügt und entfernt werden. Sind die Listen nicht aktuell, werden Sitzungsstarts, die durch einen nicht aufgeführten Controller vermittelt werden, vom VDA möglicherweise abgelehnt. Ungültige Einträge in der Liste können den Start der Systemsoftware des virtuellen Desktops verzögern. Halten Sie die Listen wie folgt auf dem neuesten Stand:

- Verwenden Sie automatische Updates zur automatischen Aktualisierung der Listen "ListOfDDCs" und "ListOfSIDs", wenn Controller hinzugefügt oder entfernt werden. Standardmäßig sind automatische Updates aktiviert.
- Eigenverwaltung: Aktualisieren Sie die Richtlinien- oder Registrierungseinstellungen für die Controller manuell.

Die Informationen in den Listen "ListOfDDCs" und "ListOfSIDs" können aus verschiedenen Orten der Bereitstellung stammen. Folgende Speicherorte werden vom VDA nacheinander überprüft, bis die Listen gefunden werden:

1. Ein Speicherort für den persistenten Speicher für automatische Updates. Dieser Speicherort enthält die Controllerinformationen, wenn automatische Updates aktiviert sind und nachdem der VDA erfolgreich zum ersten Mal nach der Installation registriert wurde. (Der Speicher enthält zudem Maschinenrichtlinieninformationen, damit Richtlinieneinstellungen bei Neustarts beibehalten werden.) Bei der ersten Registrierung nach der Installation, oder wenn automatische Updates deaktiviert sind, prüft der VDA die nachfolgend aufgeführten Stellen.
2. Richtlinieneinstellungen (Controller, Controller-SIDs).
3. Controllerinformationen des Virtual Desktop Agent-Schlüssels in der Registrierung. Diese Werte stammen ursprünglich vom VDA-Installationsprogramm, basierend auf den Controllerinformationen, die Sie bei der Installation des VDAs eingeben.
4. Auf Organisationseinheiten basierende Controller-Discovery. Dies ist eine ältere Methode die zugunsten der Abwärtskompatibilität beibehalten wird.
5. Die durch die Maschinenerstellungsdienste erstellte Datei Personality.ini.

Wenn in ListOfDDCs mehrere Controller angegeben sind, erfolgt die Verbindung mit ihnen durch den VDA in einer zufälligen Reihenfolge. Die Liste "ListOfDDCs" kann auch Controllergruppen enthalten, die an den Klammern um zwei oder mehr Controllereinträge zu erkennen sind. Der VDA versucht, eine Verbindung mit jedem Controller in einer Gruppe herzustellen, bevor er weitere Einträge in der Liste "ListOfDDCs" versucht.

Für XenDesktop-Benutzer, die ein Upgrade einer Version vor 7.0 durchgeführt haben, ersetzt das Feature für automatische Updates die CNAME-Funktion der Vorversion. Sie können die CNAME-Funktion ggf. wieder aktivieren, jedoch funktioniert das DNS-Aliasing nur konsistent, wenn Sie das AutoUpdate-Feature und die CNAME-Funktion nicht zusammen verwenden. Weitere Informationen zum erneuten Aktivieren der CNAME-Funktion finden Sie unter CTX137960.

Informationen zu den Zielorten der VDA-Registrierung in Sites mit mehreren Zonen finden Sie im Artikel "Zonen".

Überlegungen zur Verwendung automatischer Updates oder der Eigenverwaltung

Die Richtlinieneinstellung zur Aktivierung/Deaktivierung der automatischen Updates ist standardmäßig aktiviert.

Bei folgenden Bereitstellungstypen sind keine automatischen Updates möglich, stattdessen muss die Eigenverwaltung verwendet werden:

- Bereitstellungen mit Controllergruppen
- Bereitstellungen, die aus Sicherheitsgründen ListOfSIDs verwenden (Bei Bereitstellungen mit ListOfSIDs zur Verringerung der Active Directory-Last können automatische Updates verwendet werden)
- Bereitstellungen, die Provisioning Services ohne Datenträger für Zurückschreiben verwenden
- Bereitstellungen, die die Controller- oder Controller-SIDs-Richtlinieneinstellung verwenden

Automatische Updates

Die Richtlinieneinstellung *Automatische Controllerupdates aktivieren* ist Teil der Kategorie "Virtual Delivery Agent". Zum Aktivieren automatischer Updates aktivieren Sie die Richtlinieneinstellung (standardmäßig aktiviert). Zum Deaktivieren automatischer Updates deaktivieren Sie die Richtlinieneinstellung

Wird bei aktivierten automatischen Updates ein VDA installiert, versucht der VDA, sich mit einem der Controller-Werte zu registrieren, die bei der Installation des VDAs von Ihnen eingegeben wurden. Das Installationsprogramm schreibt die Controllerinformationen, die Sie bei der Installation des VDAs angegeben haben, in den Registrierungswert "ListOfDDCs".

Nach der VDA-Registrierung sendet der Controller, bei dem die Registrierung erfolgte, eine Liste der vollständig qualifizierten Domänennamen (FQDNs) und Sicherheits-IDs (SIDs) an den VDA. Der VDA schreibt diese Liste in den persistenten Speicher für automatische Updates. Die Sitekonfigurationsdatenbank wird alle 90 Minuten von jedem Controller auf Controllerinformationen überprüft: Wenn seit der letzten Überprüfung ein Controller hinzugefügt oder entfernt wurde oder wenn eine Richtlinie geändert wurde, wird die aktualisierte Liste vom Controller an die registrierten VDAs gesendet. Der VDA nimmt alle Verbindungen von allen Controllern in der aktuellen Liste an.

Geht eine Liste ein, die den Controller, bei dem der VDA registriert ist, nicht enthält (d. h. der Controller wurde aus der Site entfernt), nimmt der VDA eine neue Registrierung bei einem der Controller aus der Liste vor. Nach der Registrierung bzw. Neuregistrierung erhält der VDA eine aktualisierte Liste.

Beispiel:

1. Eine Bereitstellung hat drei Controller: A, B und C. Ein VDA ist installiert und wird bei Controller B registriert (dies wurde bei der Installation des VDAs festgelegt).
2. Zwei Controller (D und E) werden der Site hinzugefügt. Innerhalb von 90 Minuten erhalten die VDAs aktualisierte Listen und können Verbindungen von Controllern A, B, C, D und E annehmen. (Die Last wird erst nach Neustart der VDAs gleichmäßig auf alle Controller verteilt.)
3. Controller B wird aus der Site entfernt. Innerhalb von 90 Minuten erhalten die VDAs aktualisierte Listen, da seit der letzten Überprüfung eine Controlleränderung stattfand. Der in Schritt 1 installierte VDA ist bei Controller B registriert, der jedoch in der Liste nicht mehr enthalten ist. Somit wird der VDA bei einem der anderen Controller der Liste (A, C, D und E) neu registriert.

Eigenverwaltung

Wenn Sie keine automatischen Updates verwenden, müssen Sie die Citrix Richtlinieneinstellung oder die Registrierungswerte für jeden VDA der Site aktualisieren, wenn Delivery Controller in der Site hinzugefügt, verschoben oder entfernt wurden. Registrierungsänderungen können auch mit dem Gruppenrichtlinienobjekt aktualisiert werden.

Verwenden der Eigenverwaltung mit Citrix Richtlinieneinstellungen

1. Aktualisieren Sie die vollqualifizierten Domänennamen in der Richtlinieneinstellung "Controller". Diese Richtlinieneinstellung ist in der Kategorie "Virtual Delivery Agent".
2. Wenn Sie in Ihrer Bereitstellung auch ListOfSIDs-Listen verwenden, aktualisieren Sie die SID-Werte der Einstellung "Controller SIDspolicy".

Verwenden der Eigenverwaltung mit der Registrierung

Achtung: Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.

1. Aktualisieren Sie den Registrierungsschlüssel "ListOfDDCs", der die vollqualifizierten Domänennamen aller Controller in der Site enthält. (Dieser Schlüssel entspricht der Active Directory-Site-Organisationseinheit.) Trennen Sie mehrere Werte mit

Leerzeichen. Umschließen Sie Controllergruppen mit Klammern.
HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfDDCs (REG_SZ)

Wenn die Registrierungsstruktur HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent sowohl die Registrierungsschlüssel "ListOfDDCs" und "FarmGUID" enthält, wird ListOfDDCs für Controller-Discovery verwendet; FarmGUID ist vorhanden, wenn die Organisationseinheit der Site bei der Installation des VDAs angegeben wurde.

2. Aktualisieren Sie wahlweise den Registrierungsschlüssel "ListOfSIDs":
HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs (REG_SZ)

Hinzufügen, Entfernen oder Verschieben von Controllern

Zum Hinzufügen, Entfernen oder Verschieben eines Controllers benötigen Sie die im Artikel "Datenbanken" aufgeführten Serverrollen- und Datenbankrollenberechtigungen.

Hinweis: Die Installation eines Controllers auf einem Knoten in einer SQL-Clustering- oder SQL-Spiegelungsinstallation wird nicht unterstützt.

Wenn in der Bereitstellung Datenbankspiegelung verwendet wird, gilt Folgendes:

- Vor dem Hinzufügen, Entfernen oder Verschieben von Controllern müssen Sie sicherstellen, dass sowohl die gespiegelte als auch die Hauptdatenbank ausgeführt werden. Wenn Sie mit Skripts für SQL Server Management Studio arbeiten, müssen Sie den SQLCMD-Modus vor dem Ausführen des Skripts aktivieren.
- Zum Prüfen der Spiegelung nach dem Hinzufügen, Entfernen oder Verschieben des Controllers führen Sie das PowerShell-Cmdlet **get-configdbconnection** aus, um sicherzustellen, dass der Failoverpartner in der Verbindungszeichenfolge für die Spiegelung eingerichtet wurde.

Gehen Sie nach dem Hinzufügen, Entfernen oder Verschieben eines Controllers wie folgt vor:

- Wenn das automatische Update aktiviert ist, erhalten die VDAs eine aktualisierte Liste der Controller innerhalb von 90 Minuten.
- Ist das automatische Update nicht aktiviert, müssen Sie sicherstellen, dass die Controllerrichtlinieneinstellung oder der Registrierungsschlüssel "ListOfDDCs" für alle VDAs aktualisiert wird. Nachdem Sie einen Controller in eine andere Site verschoben haben, müssen Sie die Richtlinieneinstellung oder den Registrierungsschlüssel in beiden Sites aktualisieren.

Sie können Controller bei der Siteerstellung oder zu einem späteren Zeitpunkt hinzufügen. Sie können einer Site, die mit dieser Softwareversion erstellt wurde, keine Controller hinzufügen, die mit einer früheren Version installiert wurden.

1. Führen Sie das Installationsprogramm auf einem Server mit einem unterstützten Betriebssystem aus. Installieren Sie den Delivery Controller und alle anderen gewünschten Kernkomponenten. Führen Sie die Schritte des Installationsassistenten durch.
2. Wenn Sie noch keine Site erstellt haben, starten Sie Studio; Sie werden aufgefordert, eine Site zu erstellen. Klicken Sie auf der Seite "Datenbanken" im Assistenten für die Siteerstellung auf die Schaltfläche "Auswählen" und geben Sie die Adresse des Servers ein, auf dem Sie den zusätzlichen Controller installiert haben. **Wichtig:** Wenn Sie Skripts für die Initialisierung der Datenbanken generieren möchten, fügen Sie die Controller vor dem Generieren der Skripts hinzu.
3. Wenn Sie bereits eine Site erstellt haben, verweisen Sie Studio auf den Server, auf dem Sie den zusätzlichen Controller installiert haben. Klicken Sie auf **Bereitstellung erweitern** und geben Sie die Siteadresse ein.

Beim Entfernen eines Controllers aus einer Site werden die Citrix Software und andere Komponenten nicht deinstalliert. Es wird lediglich der Controller aus der Datenbank entfernt, der damit für das Brokering von Verbindungen oder sonstige

Aufgaben nicht mehr verfügbar ist. Wenn Sie einen Controller entfernen, können Sie diesen zu einem späteren Zeitpunkt der gleichen oder einer anderen Site wieder hinzufügen. Eine Site benötigt mindestens einen Controller. Aus diesem Grund können Sie den letzten in Studio aufgelisteten Controller nicht entfernen.

Wenn Sie einen Controller von einer Site entfernen, wird die Controller-Anmeldung für den Datenbankserver nicht entfernt. Auf diese Weise wird vermieden, dass eine Anmeldung entfernt wird, die von den Diensten anderer Produkte auf demselben Computer verwendet wird. Die Anmeldung muss manuell entfernt werden, wenn sie nicht mehr erforderlich ist. Dazu benötigen Sie die Berechtigungen der securityadmin-Serverrolle.

Wichtig: Entfernen Sie den Controller erst dann aus Active Directory, wenn Sie ihn aus der Site entfernt haben.

1. Stellen Sie sicher, dass der Controller eingeschaltet ist, sodass Studio in weniger als einer Stunde geladen wird. Wenn Studio den Controller lädt, den Sie entfernen möchten, schalten Sie den Controller aus, wenn Sie dazu aufgefordert werden.
2. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Controller** und anschließend den Controller aus, den Sie entfernen möchten.
3. Wählen Sie im Aktionsbereich **Controller entfernen**. Wenn Sie nicht über die erforderlichen Datenbankrollen und Berechtigungen verfügen, können Sie ein Skript erstellen, mit dem der Datenbankadministrator den Controller für Sie entfernen kann.
4. Möglicherweise müssen Sie das Maschinenkonto des Controllers auf dem Datenbankserver entfernen. Bevor Sie dies durchführen, überprüfen Sie, ob das Konto von einem anderen Dienst verwendet wird.

Nachdem Sie mit Studio einen Controller entfernt haben, besteht ggf. kurze Zeit weiter Datenverkehr zu diesem Controller, um sicherzustellen, dass die aktuellen Tasks einwandfrei abgeschlossen werden. Wenn Sie das Entfernen eines Controllers in sehr kurzer Zeit erzwingen möchten, empfiehlt Citrix, den Server, auf dem er installiert war, herunterzufahren oder aus Active Directory zu entfernen. Starten Sie dann die anderen Controller in der Site neu, um sicherzustellen, dass keine weitere Kommunikation mit dem entfernten Controller stattfindet.

Wenn die Site mehrere Zonen enthält, können Sie Controller in eine andere Zone verschieben. Informationen zu den Auswirkungen des Verschiebens auf die VDA-Registrierung und andere Vorgänge finden Sie im Artikel "Zonen".

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Controller** und anschließend den Controller aus, den Sie verschieben möchten.
2. Wählen Sie im Aktionsbereich **Verschieben**.
3. Geben Sie die Zone an, in die Sie den Controller verschieben möchten.

Controller können nicht in eine Site verschoben werden, die mit einer früheren Version dieser Software erstellt wurde.

1. Wählen Sie in der derzeitigen Site des Controllers (der alten Site) im Studio-Navigationsbereich **Konfiguration > Controller** und wählen Sie anschließend den Controller aus, den Sie verschieben möchten.
2. Wählen Sie im Aktionsbereich **Controller entfernen**. Wenn Sie nicht über die erforderlichen Datenbankrollen und Berechtigungen verfügen, können Sie ein Skript erstellen, mit dem eine Person mit den entsprechenden Berechtigungen, (z. B. der Datenbankadministrator) den Controller für Sie entfernen kann. Eine Site benötigt mindestens einen Controller. Aus diesem Grund können Sie den letzten in Studio aufgelisteten Controller nicht entfernen.
3. Öffnen Sie Studio auf dem zu verschiebenden Controller, setzen Sie bei entsprechender Aufforderung die Dienste zurück, wählen Sie **Vorhandener Site beitreten** und geben Sie die Adresse der neuen Site ein.

Wenn ein VDA mit Provisioning Services bereitgestellt wurde oder wenn er ein vorhandenes Image ist, können Sie einen VDA in eine andere Site (von Site 1 nach Site 2) verschieben, wenn Sie ein Upgrade vornehmen oder wenn Sie ein in einer Testsite erstelltes VDA-Image in eine Produktionssite verschieben. Mit Maschinenerstellungsdienste (MCS) bereitgestellte VDAs können nicht zwischen Sites verschoben werden, da MCS das Ändern der ListOfDDCs nicht unterstützt, die ein VDA zum Registrieren mit einem Controller prüft. Mit Maschinenerstellungsdienste bereitgestellte VDAs prüfen immer die ListOfDDCs, die der Site zugeordnet ist, in der sie erstellt wurden.

Es gibt zwei Möglichkeiten, einen VDA in eine andere Site zu verschieben: mit dem Installationsprogramm oder mit Citrix Richtlinien.

Installationsprogramm: Führen Sie das Installationsprogramm aus und fügen Sie einen Controller hinzu, wobei Sie in Site 2 einen vollqualifizierten Domänennamen (DNS-Eintrag) eines Controllers angeben. **Wichtig:** Geben Sie Controller im Installationsprogramm nur dann an, wenn die Richtlinieneinstellung "Controller" nicht verwendet wird.

Gruppenrichtlinienobjekt-Editor: Im folgenden Beispiel werden mehrere VDAs verschoben.

1. Erstellen Sie eine Richtlinie in Site 1 mit den nachfolgenden Einstellungen und filtern Sie die Richtlinie auf Bereitstellungsgruppenebene, um eine mehrstufige VDA-Migration zwischen den Sites zu erzielen.
   Controller: mit vollqualifizierten Domänennamen (DNS-Einträgen) von einem oder mehreren Controllern der Site 2.
   Automatische Controllerupdates aktivieren: auf "Deaktiviert" gesetzt.
2. Jeder VDA in der Bereitstellungsgruppe wird innerhalb von 90 Minuten auf die neue Richtlinie hingewiesen. Der VDA ignoriert die eingegangene Liste der Controller (da automatische Updates deaktiviert sind) und wählt einen der in der Richtlinie angegebenen Controller, d. h. einen der Controller in Site 2.
3. Wenn der VDA erfolgreich bei einem Controller der Site 2 registriert wurde, empfängt er die Liste "ListOfDDCs" und die Richtlinieninformationen von Site 2, für die automatische Updates standardmäßig aktiviert sind. Da der Controller, bei dem der VDA in Site 1 registriert war, nicht in der vom Controller in Site 2 gesendeten Liste ist, erfolgt eine erneute Registrierung des VDAs unter Auswahl eines Controllers der Liste von Site 2. Ab sofort wird der VDA automatisch mit Informationen von Site 2 aktualisiert.

Auf Organisationseinheiten von Active Directory-basierte Controller-Discovery

Diese Delivery Controller-Erkennungsmethode wird vor allem unterstützt, um Abwärtskompatibilität zu gewährleisten. Sie gilt nur für Virtual Delivery Agents (VDAs) für Windows-Desktopbetriebssysteme, aber nicht für VDAs für Windows-Serverbetriebssysteme. Bei der Active Directory-basierten Discovery müssen alle Computer in einer Site Mitglied einer Domäne sein und zwischen der Domäne, die vom Controller verwendet wird, und den von den Desktops verwendeten Domänen muss eine Vertrauensstellung bestehen. Wenn Sie diese Methode verwenden, müssen Sie die GUID der Organisationseinheit in jeder Desktopregistrierung konfigurieren.

Führen Sie für eine auf Organisationseinheiten basierende Controller-Discovery das PowerShell-Skript Set-ADControllerDiscovery.ps1 auf dem Controller aus (das Skript ist auf jedem Controller im Ordner $Env:ProgramFiles\Citrix\Broker\Service\Setup Scripts). Um das Skript auszuführen, müssen Sie über CreateChild-Berechtigungen für eine übergeordnete Organisationseinheit verfügen sowie über vollständige Administratorrechte.

Wenn Sie eine Site erstellen, müssen Sie eine entsprechende Organisationseinheit in Active Directory erstellen, wenn

Desktops die Controller in der Site mit Active Directory ermitteln sollen. Die Organisationseinheit kann in jeder Domäne in der Gesamtstruktur erstellt werden, die Ihre Computer enthält. Optimalerweise sollte die Organisationseinheit auch die Controller der Site enthalten; dies wird jedoch nicht erzwungen bzw. ist nicht erforderlich. Ein Domänenadministrator mit den entsprechenden Privilegien kann die Organisationseinheit als leeren Container erstellen und dann Administrationsrechte an der Organisationseinheit an einen Citrix Administrator delegieren.

Das Skript erstellt einige wichtige Objekte. Nur Active Directory-Standardobjekte werden erstellt und verwendet. Es ist nicht erforderlich, das Schema zu erweitern.

- Eine Controller-Sicherheitsgruppe. Das Computerkonto aller Controller in der Site muss ein Mitglied dieser Sicherheitsgruppe sein. Desktops in einer Site nehmen nur Daten von Controllern an, die Mitglied dieser Sicherheitsgruppe sind.
  Stellen Sie sicher, dass alle Controller auf allen virtuellen Desktops, auf denen der VDA ausgeführt wird, die Berechtigung "Auf diesen Computer vom Netzwerk aus zugreifen" haben. Geben Sie hierfür der Controller-Sicherheitsgruppe dieses Privileg. Wenn Controller nicht über diese Berechtigung verfügen, werden VDAs nicht registriert.

- Ein Dienstverbindungspunkt-Objekt, das Informationen zur Site enthält, wie den Namen der Site. Wenn Sie eine Organisationseinheit der Site mit dem Verwaltungstool "Active Directory-Benutzer und -Computer" prüfen, müssen Sie ggf. "Erweiterte Funktionen" im Menü "Ansicht" aktivieren, um Dienstverbindungspunkt-Objekte anzuzeigen.
- Einen "RegistrationServices" genannten Container, der in der Organisationseinheit der Site erstellt wird. Dieser Container enthält ein Dienstverbindungspunkt-Objekt für jeden Controller in der Site. Bei jedem Start des Controllers wird der Inhalt des Dienstverbindungspunkts geprüft und ggf. aktualisiert.

Wenn nach dem Abschluss der Erstinstallation mehrere Administratoren Controller hinzufügen oder entfernen, benötigen sie Berechtigungen zum Erstellen und Löschen von untergeordneten Objekten für den RegistrationServices-Container und zum Schreiben der Eigenschaften der Controller-Sicherheitsgruppe (diese Berechtigungen werden automatisch dem Administrator gewährt, der das Skript "Set-ADControllerDiscovery.ps1" ausführt). Der Domänenadministrator oder der Administrator der Originalinstallation kann diese Berechtigungen zuweisen; Citrix empfiehlt, dass Sie eine Sicherheitsgruppe für diesen Zweck einrichten.

Wenn Sie eine Organisationseinheit der Site verwenden:

- Informationen werden nur bei der Installation oder Deinstallation dieser Software in Active Directory geschrieben oder wenn beim Start eines Controllers die Informationen im Dienstverbindungspunkt aktualisiert werden müssen (der Controller wurde beispielsweise umbenannt oder der Kommunikationsport wurde geändert). In der Standardeinstellung erstellt das Skript "Set-ADControllerDiscovery.ps1" die richtigen Berechtigungen für die Organisationseinheit der Site und gibt jedem Controller Schreibrechte für den Dienstverbindungspunkt. Mit dem Inhalt der Objekte in der Organisationseinheit der Site wird eine Vertrauensstellung zwischen Desktops und Controllern erstellt. Stellen Sie Folgendes sicher:
  - Nur autorisierte Administratoren können der Controller-Sicherheitsgruppe über die Zugriffssteuerungsliste der Sicherheitsgruppe Computer hinzufügen oder Computer aus der Gruppe entfernen.
  - Nur autorisierte Administratoren und der relevante Controller können Informationen im Dienstverbindungspunkt des Controllers ändern.
- Bei einer Bereitstellung mit Replikation entstehen möglicherweise Verzögerungen; Weiteres hierzu finden Sie in der Microsoft Dokumentation. Dies ist besonders wichtig, wenn Sie die Organisationseinheit der Site in einer Domäne erstellen, die Domänencontroller in mehreren Active Directory-Sites enthält. Abhängig vom Standort der Desktops, der Controller und der Domänencontroller sind Änderungen, die Sie an Active Directory beim erstmaligen Erstellen der Organisationseinheit der Site, beim Installieren oder Deinstallieren von Controllern oder beim Ändern von Controllernamen

oder Kommunikationsports vornehmen, erst nach der Replikation auf den entsprechenden Domänencontroller für Desktops erkennbar. Symptome einer solchen Replikationsverzögerung sind u. a. Desktops, die keine Verbindung mit Controllern herstellen können und daher nicht für Benutzerverbindungen verfügbar sind.

- Diese Software verwendet mehrere standardmäßige Computerobjektattribute in Active Directory zum Verwalten von Desktops. Je nach Bereitstellung kann der vollqualifizierte Domänenname des Maschinenobjekts so wie er im Active Directory-Datensatz des Desktops gespeichert ist in den Verbindungseinstellungen eingeschlossen werden, die an den Benutzer zum Herstellen einer Verbindung zurückgegeben werden. Stellen Sie sicher, dass diese Informationen mit den Informationen in der DNS-Umgebung übereinstimmen.

Zum Verschieben eines Controllers in eine andere Site mithilfe der OU-basierten Controller-Discovery befolgen Sie die o. a. Anweisungen für das Verschieben von Controllern. Nach dem Entfernen des Controllers aus der alten Site (Schritt 2), führen Sie das PowerShell-Skript **Set-ADControllerDiscover – synch** aus. Das Skript synchronisiert die Organisationseinheit mit dem aktuellen Satz an Controllern. Nach dem Beitritt zur vorhandenen Site (Schritt 3), führen Sie das gleiche Skript auf einem Controller in der neuen Site aus.

Sitzungen

Feb 29, 2016

Das Erhalten der Sitzungsaktivität ist wichtig, um eine optimale Benutzererfahrung zu gewährleisten. Eine Unterbrechung der Verbindung aufgrund von unzuverlässigen Netzwerken, stark variierender Netzwerklatenz oder Bereichseinschränkungen von drahtlosen Geräten kann zu Frustrationen bei den Benutzern führen. Ein schneller Wechsel zwischen Arbeitsstationen und Zugriff auf dieselben Anwendungen bei jeder Anmeldung ist eine Priorität für viele mobile Mitarbeiter, z. B. von Mitarbeitern in einem Krankenhaus.

Die folgenden Features dienen dazu, die Sitzungszuverlässigkeit zu optimieren, Unannehmlichkeiten, Ausfallzeiten und Produktivitätsverluste zu reduzieren, und mobilen Benutzern einen schnellen und einfachen Wechsel zwischen Geräten zu ermöglichen.

- Sitzungszuverlässigkeit
- Automatische Wiederverbindung von Clients
- ICA-Keep-Alive
- Workspace Control
- Sitzungsroaming

Im Abschnitt Anmeldeintervall wird beschrieben, wie Sie die Standardeinstellung ändern.

Sie können Benutzer von einer Sitzung abmelden, Sitzungen trennen und Sitzungsvorabstart sowie Sitzungsfortbestehen konfigurieren. Informationen hierzu finden Sie im Artikel Verwalten von Sitzungen über Bereitstellungsgruppen.

Sitzungszuverlässigkeit

Durch die Sitzungszuverlässigkeit bleiben Sitzungen aktiv und auf dem Bildschirm des Benutzers, wenn die Netzwerkkonnektivität unterbrochen wird. Die Benutzer sehen so lange weiterhin die Anwendung, die sie verwenden, bis die Netzwerkkonnektivität wiederhergestellt ist.

Diese Funktion ist besonders für mobile Benutzer mit drahtlosen Verbindungen geeignet. Ein Benutzer mit einer drahtlosen Verbindung fährt z. B. in einen Tunnel und die Verbindung wird vorübergehend unterbrochen. Normalerweise würde die Sitzung getrennt und nicht mehr auf dem Bildschirm angezeigt. Der Benutzer müsste sich neu mit der getrennten Sitzung verbinden. Mit der Sitzungszuverlässigkeit bleibt die Sitzung auf der Maschine aktiv. Der Verlust der Verbindung ist zu erkennen, da auf dem Client der Bildschirm fixiert und der Mauszeiger als sich drehende Sanduhr angezeigt wird, bis die Verbindung am Ende des Tunnels wiederhergestellt ist. Der Benutzer kann während der Unterbrechung weiterhin auf die Anzeige zugreifen und mit der Anwendung weiterarbeiten, wenn die Netzwerkverbindung wiederhergestellt ist. Die Sitzungszuverlässigkeit verbindet Benutzer ohne Neuauthentifizierung wieder.

Citrix Receiver-Benutzer können die Controllereinstellung nicht überschreiben.

Sie können die Sitzungszuverlässigkeit mit Transport Layer Security (TLS) verwenden. Mit TLS werden nur die Daten verschlüsselt, die zwischen dem Benutzergerät und NetScaler Gateway gesendet werden.

Sie aktivieren und konfigurieren die Sitzungszuverlässigkeit mit den folgenden Einstellungen:

- Mit der Richtlinieneinstellung "Sitzungszuverlässigkeit - Verbindungen" können Sie die Sitzungszuverlässigkeit aktivieren oder deaktivieren.

- Der Standardwert für die Einstellung "Sitzungszuverlässigkeit - Timeout" ist 180 Sekunden (3 Minuten). Obwohl Sie den Zeitraum vergrößern können, den die Sitzungszuverlässigkeit eine Sitzung offen lässt, sollten Sie dabei berücksichtigen, dass diese Funktion den Benutzer nicht zu einer Neuauthentifizierung auffordert, um den Bedienungskomfort zu erhöhen. Je länger eine Sitzung offen gelassen wird, desto höher ist das Risiko, dass der Benutzer abgelenkt wird und das Benutzergerät verlässt. Benutzer ohne Berechtigung hätten in dem Fall möglicherweise Zugriff auf die Sitzung.
- Eingehende Sitzungszuverlässigkeitsverbindungen verwenden Port 2598, es sei denn, die Portnummer wurde unter "Sitzungszuverlässigkeit - Portnummer" geändert.
- Verwenden Sie die Funktion zur automatischen Wiederverbindung von Clients, wenn Sie möchten, dass Benutzer eine Verbindung mit unterbrochenen Sitzungen nur mit einer Neuauthentifizierung wiederherstellen können. Sie können die Einstellung für die Citrix Richtlinie "Authentifizierung bei automatischer Wiederverbindung von Clients" so konfigurieren, dass Benutzer aufgefordert werden, sich neu zu authentifizieren, wenn sie sich mit einer unterbrochenen Sitzung wiederverbinden.

Wenn Sie sowohl Sitzungszuverlässigkeit als auch die Funktion zur automatischen Wiederverbindung verwenden, werden beide Funktionen nacheinander ausgeführt. Die Sitzungszuverlässigkeit beendet oder trennt die Benutzersitzung, nachdem der mit der Option "Sitzungszuverlässigkeit - Timeout" festgelegte Zeitraum abgelaufen ist. Anschließend werden die Richtlinieneinstellungen für die automatische Wiederverbindung von Clients wirksam und es wird versucht, eine Verbindung mit der unterbrochenen Sitzung wiederherzustellen.

Automatische Wiederverbindung von Clients

Mit der automatischen Wiederverbindung von Clients kann Citrix Receiver unabsichtlich getrennte ICA-Sitzungen erkennen und die Benutzer automatisch wieder mit den betroffenen Sitzungen verbinden. Wenn diese Funktion auf dem Server aktiviert ist, müssen Benutzer nicht manuell eine neue Verbindung herstellen, um mit ihrer Arbeit fortfahren zu können.

Bei Anwendungssitzungen versucht Citrix Receiver, die Verbindung mit der Sitzung wiederherzustellen, bis die Wiederverbindung erfolgreich war oder der Benutzer die Wiederverbindung abbricht.

Bei Desktopsitzungen versucht Citrix Receiver eine festgelegte Zeit lang, die Verbindung mit der Sitzung wiederherzustellen, bis die Wiederverbindung erfolgreich war oder der Benutzer die Wiederverbindung abbricht. Der Standardwert für diese Zeit ist fünf Minuten. Um die Zeit zu ändern, bearbeiten Sie die Registrierung auf dem Benutzergerät:

HKLM\Software\Citrix\ICA Client\TransportReconnectRetryMaxTimeSeconds; DWORD;

wobei <*Sekunden*> die Zeit in Sekunden ist, nach deren Ablauf keine weiteren Versuche der Sitzungswiederherstellung erfolgen.

Sie aktivieren und konfigurieren die automatische Wiederverbindung von Clients mit den folgenden Einstellungen:

- **Automatische Wiederverbindung von Clients**: Aktiviert oder deaktiviert die automatische Wiederverbindung desselben Clients, nach dem die Verbindung unterbrochen wurde.
- **Authentifizierung bei automatischer Wiederverbindung von Clients**: Aktiviert oder deaktiviert die erforderliche Benutzerauthentifizierung bei der automatischen Wiederverbindung
- **Protokollierung der automatischen Wiederverbindung von Clients**: Aktiviert oder deaktiviert die Protokollierung von Wiederverbindungsereignissen im Ereignisprotokoll. Die Protokollierung ist standardmäßig deaktiviert. Wenn diese Einstellung aktiviert ist, werden Informationen zu erfolgreichen oder fehlgeschlagenen automatischen Wiederverbindungsereignissen im Systemprotokoll des Servers aufgezeichnet. Jeder Server speichert die Informationen zu Wiederverbindungsereignissen im eigenen Systemprotokoll; die Site stellt kein Protokoll aller Wiederverbindungsereignisse

aller Server bereit.

Bei der automatischen Wiederverbindung von Clients findet eine Authentifizierung mit verschlüsselten Anmeldeinformationen statt. Wenn sich ein Benutzer anmeldet, verschlüsselt und speichert der Server die Anmeldeinformationen und erstellt und sendet ein Cookie mit einem Verschlüsselungsschlüssel an Citrix Receiver. Citrix Receiver übergibt den Schlüssel zum Wiederverbinden an den Server. Der Server entschlüsselt die Anmeldeinformationen und gibt sie an die Windows-Anmeldung für eine Authentifizierung weiter. Benutzer müssen sich beim Ablaufen von Cookies neu authentifizieren, um Sitzungen wiederherzustellen.

Cookies werden nicht verwendet, wenn Sie die Einstellung "Authentifizierung bei automatischer Wiederverbindung von Clients" aktivieren. Stattdessen wird der Benutzer in einem Dialogfeld zur Eingabe der Anmeldeinformationen aufgefordert, wenn Citrix Receiver versucht, die Verbindung automatisch wiederherzustellen.

Zum maximalen Schutz der Anmeldeinformationen von Benutzern und von Sitzungen verwenden Sie die Verschlüsselung für die gesamte Kommunikation zwischen Clients und Site.

Sie deaktivieren die automatische Wiederverbindung in Citrix Receiver für Windows mit der Datei icaclient.adm. Diese Datei liegt derzeit nur in Englisch vor. Weitere Informationen finden Sie in der Dokumentation zu Ihrer Version von Citrix Receiver für Windows.

Einstellungen für Verbindungen wirken sich auch auf die automatische Wiederverbindung von Clients aus:

- In der Standardeinstellung wird die automatische Wiederverbindung von Clients durch Richtlinieneinstellungen auf der Siteebene aktiviert (siehe oben). Der Benutzer muss sich nicht authentifizieren. Wenn jedoch die ICA-TCP-Verbindung eines Servers so konfiguriert wurde, dass Sitzungen mit einer unterbrochenen Kommunikationsverbindung zurückgesetzt werden, findet die automatische Wiederverbindung nicht statt. Die automatische Wiederverbindung von Clients funktioniert nur, wenn der Server Sitzungen trennt, wenn eine unterbrochene Verbindung oder eine Verbindungstimeout vorliegt. In diesem Zusammenhang verweist "ICA-TCP-Verbindung" auf den virtuellen Serverport (nicht auf eine tatsächliche Netzwerkverbindung), der für Sitzungen in TCP/IP-Netzwerken verwendet wird.
- Standardmäßig ist die ICA-TCP-Verbindung auf einem Server so eingestellt, dass Sitzungen mit unterbrochenen Verbindungen oder Verbindungen, die das Zeitlimit überschritten haben, getrennt werden. Getrennte Sitzungen bleiben im Systemspeicher intakt und stehen für eine Wiederverbindung durch Citrix Receiver zur Verfügung.
- Die Verbindung kann so konfiguriert werden, dass Sitzungen mit unterbrochenen Verbindungen oder Verbindungen mit Timeouts zurückgesetzt oder abgemeldet werden. Wenn eine Sitzung zurückgesetzt wird, wird bei einem Wiederverbindungsversuch eine neue Sitzung eingeleitet; die Umgebung des Benutzers wird in der verwendeten Anwendung nicht wiederhergestellt, sondern die Anwendung wird neu gestartet.
- Wenn der Server für das Zurücksetzen von Sitzungen konfiguriert ist, erstellt die automatische Wiederverbindung von Clients eine neue Sitzung. Benutzer müssen dann ihre Anmeldeinformationen eingeben, um sich am Server anzumelden.
- Die automatische Wiederverbindung kann fehlschlagen, wenn Citrix Receiver oder das Plug-In falsche Authentifizierungsinformationen übergibt (dies kann während eines Angriffs passieren), oder wenn der Server feststellt, dass zu viel Zeit seit dem Erkennen der unterbrochenen Verbindung verstrichen ist.

ICA-Keep-Alive

ICA-Keep-Alive verhindert, dass Sitzungen durch unterbrochene Verbindungen getrennt werden. Wenn der Server keine Aktivität erkennt (z. B. keine Zeitänderungen, Mausbewegungen oder Bildschirmaktualisierungen) wird verhindert, dass die Sitzung durch die Remotedesktopdienste getrennt wird. Der Server sendet alle paar Sekunden Keep-Alive-Pakete, um zu

erkennen, ob die Sitzung aktiv ist. Wenn die Sitzung nicht mehr aktiv ist, wird die Sitzung vom Server als "Getrennt" gekennzeichnet.

Hinweis: ICA-Keep-Alive funktioniert nur, wenn Sie die Sitzungszuverlässigkeit nicht verwenden. Die Sitzungszuverlässigkeit hat eigene Mechanismen für das Aufrechterhalten von Verbindungen. Konfigurieren Sie ICA-Keep-Alive nur für Verbindungen, die keine Sitzungszuverlässigkeit verwenden.

ICA-Keep-Alive-Einstellungen überschreiben Keep-Alive-Einstellungen, die für Microsoft Windows-Gruppenrichtlinien konfiguriert wurden.

Sie aktivieren und konfigurieren ICA-Keep-Alive mit den folgenden Einstellungen:

- **ICA-Keep-Alive - Timeout**: Gibt das Intervall (1-3600 Sekunden) für das Senden von ICA-Keep-Alive-Meldungen an. Konfigurieren Sie diese Option nicht, wenn die Netzwerksoftware 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 beim Server können Benutzer eine Verbindung zu all ihren Desktops oder Anwendungen jederzeit wiederherstellen, indem Sie auf "Wiederverbinden" klicken. Beim Wiederverbinden werden standardmäßig sowohl getrennte Desktops oder Anwendungen geöffnet als auch alle aktiven Anwendungen, die derzeit auf einem anderen Clientgerät ausgeführt werden. Sie können die Wiederverbindung so konfigurieren, dass nur die Desktops oder Anwendungen geöffnet werden, deren Verbindung der Benutzer zuvor getrennt hat.
- **Abmelden**: Bei Benutzern, die Desktops oder Anwendungen über StoreFront öffnen, können Sie den Abmeldebefehl so

konfigurieren, dass Benutzer entweder von StoreFront und allen aktiven Sitzungen gleichzeitig oder nur von StoreFront abgemeldet werden.
- **Verbindung wird getrennt**: Benutzer können die Verbindung mit allen ausgeführten Desktops und Anwendungen gleichzeitig trennen.

Workspace Control ist nur für Benutzer von Citrix Receiver verfügbar, die über eine Citrix StoreFront-Verbindung auf Desktops und Anwendungen zugreifen. Workspace Control ist standardmäßig für virtuelle Desktopsitzungen deaktiviert, für gehostete Anwendungen aber aktiviert. Die Sitzungsfreigabe zwischen veröffentlichten Desktops und veröffentlichten Anwendungen in diesen Desktops erfolgt nicht standardmäßig.

Benutzerrichtlinien, Clientlaufwerkzuordnungen und Druckerkonfigurationen ändern sich entsprechend, wenn ein Benutzer ein neues Clientgerät verwendet. Diese Richtlinien und Zuordnungen werden auf dem Clientgerät angewendet, auf dem der Client derzeit bei der Sitzung angemeldet ist. Wenn sich Pflegepersonal z. B. von einem Clientgerät in der Notaufnahme des Krankenhauses abmeldet und dann bei einer Arbeitsstation in der Röntgenabteilung anmeldet, gelten für die Sitzung die Richtlinien, Druckerzuordnungen und Clientlaufwerkzuordnungen der Röntgenabteilung, solange die Sitzung gestartet wird.

Sie können die den Benutzern angezeigten Drucker je nach Standort anpassen. Außerdem können Sie steuern, ob Benutzer auf lokalen Druckern drucken können, wie viel Bandbreite bei einer Remoteverbindung verwendet wird sowie andere Aspekte des Druckens.

Weitere Informationen zur Aktivierung und Konfiguration von Workspace Control für Benutzer finden Sie in der StoreFront-Dokumentation.

Sitzungsroaming

Standardmäßig wechseln Sitzungen zusammen mit dem Benutzer von Clientgerät zu Clientgerät. Wenn ein Benutzer eine Sitzung startet und dann mit einem anderen Gerät weiterarbeitet, wird die gleiche Sitzung verwendet und die Anwendungen stehen auf beiden Geräten zur Verfügung. Die Anwendungen folgen dem Benutzer unabhängig von dem Gerät und davon, ob aktuelle Sitzungen vorhanden sind. In vielen Fällen folgen auch Drucker und andere Ressourcen, die einer Anwendung zugewiesen sind.

Dieses Standardverhalten bietet viele Vorteile, ist aber nicht in allen Fällen ideal. Sie können das Sitzungsroaming mit dem PowerShell-SDK verhindern.

Beispiel 1: Ein Mitarbeiter eines Krankenhauses verwendet beim Ausfüllen eines Versicherungsformulars einen Desktop-PC und ein Tablet zum Anzeigen von Patientendaten.

- Bei aktiviertem Sitzungsroaming werden beide Anwendungen auf beiden Geräten angezeigt (eine auf einem Gerät gestartete Anwendung ist auf allen Geräten zu sehen). Dies entspricht möglicherweise nicht den Sicherheitsanforderungen.
- Wenn das Sitzungsroaming deaktiviert ist, werden die Patientendaten nicht auf dem PC angezeigt und das Versicherungsformular nicht auf dem Tablet.

Beispiel 2: Ein Produktionsmanager startet eine Anwendung auf dem PC im Büro. Gerätename und Standort bestimmen, welche Drucker und anderen Ressourcen für die Sitzung verfügbar sind. Später nimmt er bei einer Besprechung in einem anderen Gebäude teil und muss etwas ausdrucken.

- Bei aktiviertem Sitzungsroaming kann er wahrscheinlich nicht auf die Drucker in der Nähe des Besprechungsraums zugreifen, da ihm durch den Anwendungsstart Drucker und Ressourcen für den Standort Büro zugewiesen wurden.

- Ist das Sitzungsroaming deaktiviert, wird bei der Anmeldung bei einem anderen Gerät (mit denselben Anmeldeinformationen) eine neue Sitzung gestartet und Drucker und Ressourcen in der Nähe werden verfügbar.

Zum Konfigurieren des Sitzungsroamings verwenden Sie die folgenden Anspruchsrichtlinienregel-Cmdlets mit der Eigenschaft "SessionReconnection". Optional können Sie auch die Eigenschaft "LeasingBehavior" festlegen. Weitere Informationen finden Sie weiter unten unter "Verbindungsleasing und Sitzungsroaming".

Desktopsitzungen:

> Set-BrokerEntitlementPolicyRule <*Name der Bereitstellungsgruppe*> -SessionReconnection <*Wert*> -LeasingBehavior Allowed|Disallowed

Anwendungssitzungen:

> Set-BrokerAppEntitlementPolicyRule <*Name der Bereitstellungsgruppe*> -SessionReconnection <*Wert*> -LeasingBehavior Allowed|Disallowed

<*Wert*> kann einer der folgenden Werte sein:

- **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.

Wenn Sie nicht mit dem Verbindungsleasing vertraut sind, lesen Sie den Artikel Verbindungsleasing.

Wenn ein Controller auf eine geleaste Verbindung schaltet, tritt für die Sitzungswiederverbindung wieder der Standardwert in Kraft, d. h. die Wiederverbindung erfolgt nur mit einer aktiven oder getrennten Sitzung für den Desktop bzw. die Anwendung.

Zur Gewährleistung zusätzlicher Sicherheit sollten Sie, wenn Sie für das Sitzungsroaming einen anderen als den

Standardwert konfiguriert haben und mehrere Benutzer auf mehreren Geräten dieselben Anmeldeinformationen verwenden, das Verbindungsleasing für die Bereitstellungsgruppe, die das verwendete Benutzerkonto enthält, deaktivieren.

Erklärung In diesem Szenario wird eine Sitzung auf allen Geräten gemeinsam verwendet. Das ist möglicherweise unerwünscht, z. B. wenn ein Benutzer vertrauliche Informationen anzeigt, die andere Benutzer, die sich mit denselben Anmeldeinformationen wieder verbinden, während der Controller im Leasingverbindungsmodus ausgeführt wird, nicht sehen sollen.

Durch Deaktivieren des Verbindungsleasings in der Anspruchsrichtlinie wird dies verhindert, d. h. Benutzer können die Sitzung anderer mit den gleichen Anmeldeinformationen angemeldeter Benutzer nicht sehen, selbst wenn der Controller im Leasingverbindungsmodus ausgeführt wird. Andere Anspruchsrichtlinien können bestehen bleiben; einzelne Benutzerkonten können das Verbindungsleasing über separate Ansprüche nutzen.

Zum Deaktivieren des Verbindungsleasings in einer Anspruchrichtlinie fügen Sie die Eigenschaft "LeasingBehavior Disallowed" dem Cmdlet der Anspruchsrichtlinie hinzu. Wenn Sie das Verbindungsleasing deaktivieren, müssen Sie alle für die Anspruchsrichtlinie bereits erstellten und zwischengespeicherten Startleases manuell löschen. Andernfalls können sich die Benutzer nach wie vor wieder verbinden, wenn es zum Ausfall der Datenbank kommt.

Anmeldeintervall

Wenn eine virtuelle Maschine mit einem Desktop-VDA geschlossen wird, bevor die Anmeldung abgeschlossen ist, können Sie dem Prozess mehr Zeit zuteilen. Die Standardeinstellung in Version 7.6 und höher ist 180 Sekunden (die Standardeinstellung für Version 7.0-7.5 ist 90 Sekunden).

Legen Sie auf der Maschine (oder dem im Maschinenkatalog verwendeten Masterimage) folgenden Registrierungsschlüssel fest:

Schlüssel: HKLM\SOFTWARE\Citrix\PortICA

Wert: AutoLogonTimeout

Typ: DWORD

Geben Sie die Zeit als Dezimalwert in Sekunden ein, zulässig ist ein Wert von 0 bis 3600.

Wenn Sie ein Masterimage ändern, aktualisieren Sie den Katalog.

Hinweis: Diese Einstellung gilt nur für VMs mit Desktop-VDAs, das Anmeldetimeout auf Server-VDAs wird von Microsoft gesteuert.

Verwenden der Suche in Studio

Feb 29, 2016

Verwenden Sie die Suchfunktion, um Informationen zu spezifischen Maschinen, Sitzungen, Maschinenkatalogen, Anwendungen oder Bereitstellungsgruppen zu finden.

1. Wählen Sie im Studio-Navigationsbereich Suchen aus.
   Hinweis: Sie können mit dem Suchfeld der Registerkarten "Maschinenkataloge" oder "Bereitstellungsgruppen" keine Suche durchführen. Verwenden Sie den Suchknoten im Navigationsbereich.
   Zum Anzeigen weiterer Suchkriterien klicken Sie auf das Pluszeichen neben den Dropdownlisten. Klicken Sie zum Entfernen von Suchkriterien auf das Minuszeichen.
2. Geben Sie den Namen ein oder verwenden Sie die Dropdownliste, um eine andere Suchoption für das gesuchte Element auszuwählen.
3. Speichern Sie Ihre Suche, falls gewünscht, durch Wählen von Speichern unter. Die Suche wird in der Liste "Gespeicherte Suchvorgänge" angezeigt.

Sie können auch auf das Symbol "Suche erweitern" (doppelte nach unten gerichtete spitze Klammern) klicken, um eine Dropdownliste mit Sucheigenschaften anzuzeigen. Führen Sie eine erweiterte Suche durch, indem Sie einen Ausdruck anhand der Eigenschaften in der Dropdownliste zusammenstellen.

Tipps zur Verbesserung der Suche:

- Um zusätzliche Eigenschaften in die Anzeige zu integrieren, anhand derer Sie dann suchen und sortieren können, klicken Sie mit der rechten Maustaste auf eine Spalte und wählen Sie Spalten auswählen.
- Wählen Sie zum Suchen eines mit einer Maschine verbundenen Benutzergeräts "Client (IP)" und "ist", und geben Sie die IP-Adresse des Geräts ein.
- Wenn Sie aktive Sitzungen suchen, verwenden Sie "Sitzungszustand", "ist" und "Verbunden".
- Um alle Maschinen in einer Bereitstellungsgruppe aufzuführen, wählen Sie im Navigationsbereich Bereitstellungsgruppen, wählen Sie die Gruppe aus und wählen Sie dann im Aktionsbereich Maschinen anzeigen.

Unterstützung für IPv4/IPv6

Feb 29, 2016

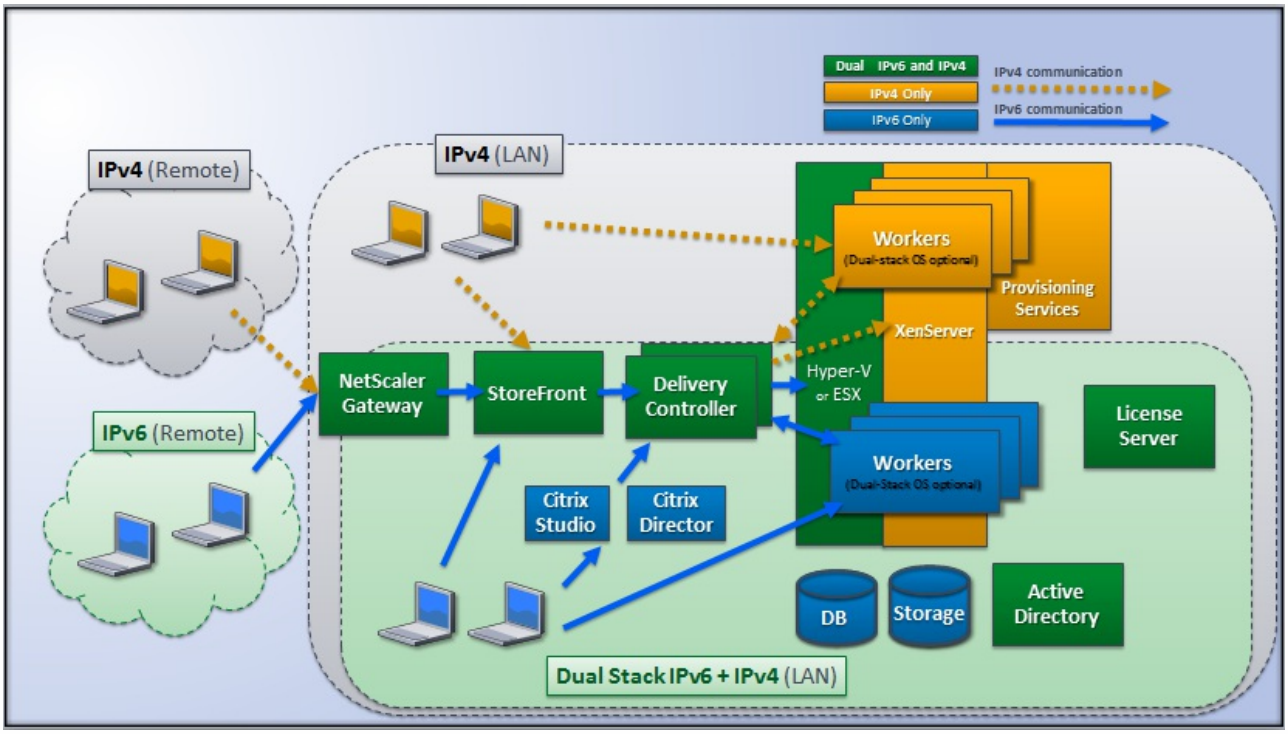
Dieses Release unterstützt reines IPv4, reines IPv6 und Bereitstellungen mit dualem Stapel, bei denen überlappende IPv4- und IPv6-Netzwerke verwendet werden.

Die IPv6-Kommunikation wird mit zwei verbindungsspezifischen Citrix Richtlinieneinstellungen für Virtual Delivery Agent (VDA) gesteuert:

- Die primäre Einstellung erzwingt die Verwendung von IPv6: Nur IPv6-Controllerregistrierung verwenden.
- Die abhängige Einstellung definiert eine IPv6-Netzwerkmaske: IPv6-Netzwerkmaske für Controllerregistrierung.

Wenn Nur IPv6-Controllerregistrierung verwenden aktiviert ist, erfolgt die VDA-Registrierung bei einem Delivery Controller für eingehende Verbindungen über eine IPv6-Adresse.

Die folgende Abbildung zeigt eine IPv4-/IPv6-Bereitstellung mit dualem Stapel. In diesem Szenario ist ein Worker ein auf einem Hypervisor oder auf einer physischen Maschine installierter VDA, der primär zum Aktivieren von Verbindungen für Anwendungen und Desktops verwendet wird. Komponenten, die für den Parallelbetrieb von IPv6 und IPv4 ausgelegt sind, werden auf Betriebssystemen ausgeführt, die Tunneling oder Dual Protocol-Software nutzen.



Diese Citrix Produkte, Komponenten und Features unterstützen nur IPv4:

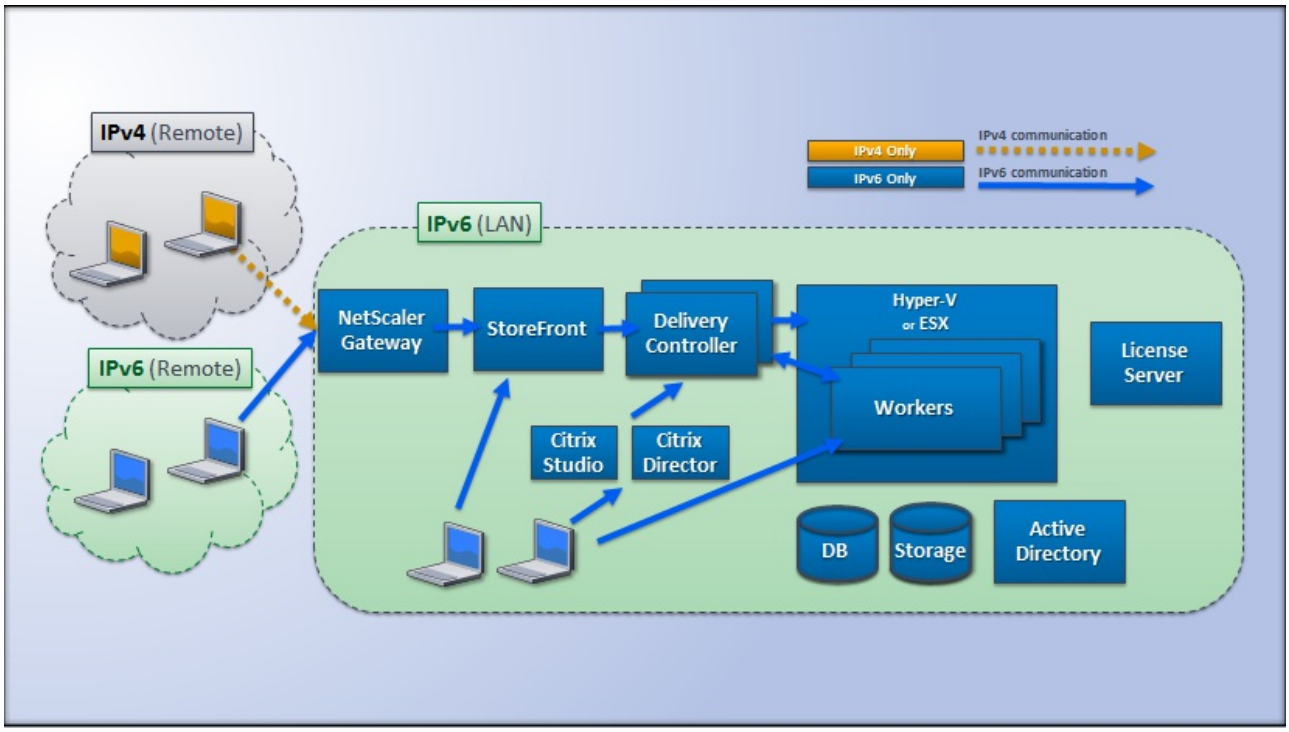
- Provisioning Services
- XenServer Version 6.x
- VDAs, die nicht mit der Richtlinieneinstellung **Nur IPv6-Controllerregistrierung verwenden** gesteuert werden
- XenApp-Versionen vor 7.5, XenDesktop-Versionen vor 7 und EdgeSight

In dieser Bereitstellung gilt:

- Wenn ein Team häufig ein IPv6-Netzwerk verwendet und der Administrator die Nutzung von IPv6-Datenverkehr

wünscht, veröffentlicht der Administrator IPv6-Desktops und -Anwendungen für die Benutzer auf der Basis eines Workerimages oder einer Organisationseinheit, für das bzw. die die primäre IPv6-Richtlinieneinstellung (Nur IPv6-Controllerregistrierung verwenden) aktiviert ist.
- Wenn ein Team häufig ein IPv4-Netzwerk verwendet, veröffentlicht der Administrator IPv4-Desktops und -Anwendungen für die Benutzer auf der Basis eines Workerimages oder einer Organisationseinheit, für das bzw. die die primäre IPv6-Richtlinieneinstellung deaktiviert ist (d. h. Nur IPv6-Controllerregistrierung verwenden ist deaktiviert = Standardeinstellung).

Die folgende Abbildung zeigt eine reine IPv6-Bereitstellung. Für dieses Szenario gilt:
- Die Komponenten werden auf Betriebssystemen ausgeführt, die ein IPv6-Netzwerk unterstützen.
- Die primäre Citrix Richtlinieneinstellung (Nur IPv6-Controllerregistrierung verwenden) ist für alle VDAs aktiviert; sie müssen sich beim Controller mit einer IPv6-Adresse registrieren.



Bei reiner IPv6-Implementierung bzw. Implementierung von IPv4/IPv6 mit dualem Stapel sind zwei Citrix Richtlinieneinstellungen relevant. Konfigurieren Sie die folgenden verbindungsbezogenen Einstellungen:
- **Nur IPv6 Controllerregistrierung verwenden**: steuert das Adressformat, mit dem der Virtual Delivery Agent (VDA) beim Delivery Controller registriert wird. Standard = deaktiviert
  - Wenn der VDA mit dem Controller kommuniziert, wird eine IPv6-Adresse verwendet, deren Auswahl folgender Reihenfolge unterliegt: globale IP-Adresse, Unique Local Address (ULA), Link-Local-Adresse (nur wenn keine anderen IPv6-Adressen verfügbar sind).
  - Bei deaktivierter Einstellung wird der VDA mit der IPv4-Adresse der Maschine für die Kommunikation beim Controller registriert.
- **IPv6-Netzwerkmaske für Controllerregistrierung**: Eine Maschine kann über mehrere IPv6-Adressen verfügen. Mit dieser Richtlinieneinstellung können Administratoren den VDA auf ein bevorzugtes Subnetz beschränken (anstelle einer globalen IP, sofern registriert). Mit dieser Einstellung wird das Netzwerk festgelegt, in dem der VDA registriert wird: Der VDA wird nur bei der ersten Adresse registriert, die mit der angegebenen Netzwerkmaske übereinstimmt. Diese

Einstellung ist nur gültig, wenn die Richtlinieneinstellung Nur IPv6-Controllerregistrierung verwenden aktiviert ist. Standard = leere Zeichenfolge

Wichtig: Die Verwendung von IPv4 oder IPv6 durch einen VDA wird ausschließlich über diese Richtlinieneinstellungen gesteuert. Das bedeutet, um die IPv6-Adressierung nutzen zu können, muss der VDA von einer Citrix Richtlinie gesteuert werden, bei der die Einstellung **Nur IPv6-Controllerregistrierung verwenden** aktiviert ist.

Wenn Ihre Umgebung sowohl IPv4- und IPv6-Netzwerke umfasst, benötigen Sie separate Bereitstellungsgruppenkonfigurationen für IPv4-exklusive Clients und für die Clients, die Zugriff auf das IPv6-Netzwerk haben. Verwenden Sie ggf. Namen, die manuelle Active Directory-Gruppenzuweisung oder SmartAccess-Filter zur Unterscheidung der Benutzer.

Die Wiederverbindung mit einer Sitzung kann fehlschlagen, wenn die Verbindung auf einem IPv6-Netzwerk initiiert wird und dann Wiederverbindungsversuche von einem internen Client erfolgen, der nur über IPv4-Zugriff verfügt.

Clientordnerumleitung

Feb 29, 2016

Durch die Clientordnerumleitung ändert sich der Zugriff auf clientseitige Dateien bei der hostseitigen Sitzung. Wird auf dem Server nur die Clientlaufwerkzuordnung aktiviert, werden die clientseitigen vollständigen Volumes den Sitzungen automatisch als UNC-Link (Universal Naming Convention) zugeordnet. Wenn Sie die Clientordnerumleitung auf dem Server aktivieren und der Benutzer sie auf dem Benutzergerät konfiguriert, wird der Teil des vom lokalen Benutzer angegebenen lokalen Volumes umgeleitet.

Nur die vom Benutzer angegebenen Ordner statt des kompletten Dateisystems auf dem Benutzergerät werden als UNC-Links in den Sitzungen angezeigt. Wenn Sie UNC-Links durch die Registrierung deaktivieren, werden Clientordner als zugeordnete Laufwerke in der Sitzung angezeigt.

Die Clientordnerumleitung wird nur auf Windows-Desktopbetriebssystemmaschinen unterstützt.

Client folder redirection for an external USB drive will not be saved on detaching and reattaching the device.

Aktivieren Sie die Clientordnerumleitung auf dem Server. Geben Sie dann auf dem Clientgerät an, welche Ordner umgeleitet werden sollen (die Anwendung, die Sie zur Angabe der Clientordneroptionen verwenden, ist in diesem Release von Citrix Receiver enthalten).

Achtung: Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.

1. Auf dem Server:
    1. Erstellen Sie einen Schlüssel: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Client Folder Redirection.
    2. Erstellen Sie einen Wert für REG_DWORD.
        - Name: CFROnlyModeAvailable
        - Typ: REG_DWORD
        - Wert: Stellen Sie 1 ein.
2. Auf dem Benutzergerät:
    1. Stellen Sie sicher, dass die neueste Version von Citrix Receiver installiert ist.
    2. Starten Sie vom Installationsverzeichnis von Citrix Receiver 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.

Benutzerprofile

Feb 29, 2016

Standardmäßig wird bei der Installation des Virtual Delivery Agents die Citrix Profilverwaltung ohne Benutzereingriff auf Masterimages installiert. Sie muss jedoch nicht als Profillösung verwendet werden.

Mit XenApp- und XenDesktop-Richtlinien können Sie auf die Maschinen jeder Bereitstellungsgruppe ein anderes Profilverhalten anwenden, um die Profile an unterschiedliche Benutzerbedürfnisse anzupassen. Beispiel: Eine Bereitstellungsgruppe erfordert möglicherweise verbindliche Citrix Profile, deren Vorlage an einem Netzwerkspeicherort gespeichert ist, aber eine andere Bereitstellungsgruppe erfordert möglicherweise Citrix Roamingprofile an einem anderen Speicherort mit mehreren umgeleiteten Ordnern.

- Wenn andere Administratoren in Ihrer Organisation für XenApp- und XenDesktop-Richtlinien zuständig sind, stimmen Sie gemeinsam ab, welche profilbezogenen Richtlinien für die Bereitstellungsgruppen gelten.
- Richtlinien zur Profilverwaltung können auch in der Gruppenrichtlinie sowie in der INI-Datei der Profilverwaltung und lokal auf einzelnen virtuellen Maschinen festgelegt werden. Diese verschiedenen Methoden zum Definieren des Profilverhaltens werden in der folgenden Reihenfolge gelesen:
  1. Gruppenrichtlinie (ADM- oder ADMX-Dateien)
  2. XenApp- und XenDesktop-Richtlinien im Knoten "Richtlinie"
  3. Lokale Richtlinien auf der virtuellen Maschine, zu der der Benutzer eine Verbindung herstellt
  4. INI-Datei der Profilverwaltung

  Beispiel: Wenn Sie die gleiche Richtlinie sowohl in der Gruppenrichtlinie als auch im Knoten "Richtlinie" konfigurieren, wird die Richtlinieneinstellung in der Gruppenrichtlinie vom System gelesen und die XenApp- bzw. XenDesktop-Richtlinieneinstellung wird ignoriert.

Unabhängig davon, für welche Lösung Sie sich entscheiden, können Director-Administratoren auf Diagnoseinformationen zugreifen und Problembehandlung für Benutzerprofile durchführen. Weitere Informationen finden Sie in der Dokumentation für Director.

Wenn Sie das Personal vDisk-Feature verwenden, werden Citrix Benutzerprofile standardmäßig auf den persönlichen vDisks der virtuellen Desktops gespeichert. Löschen Sie die Kopie eines Profils im Benutzerspeicher nicht, wenn gleichzeitig eine Kopie auf der persönlichen vDisk verbleibt. Dies würde einen Profilverwaltungsfehler auslösen und dazu führen, dass für Anmeldungen an dem virtuellen Desktop ein temporäres Profil verwendet wird.

Der Desktoptyp wird automatisch basierend auf der VDA-Installation erkannt und entsprechende Standardwerte für die Profilverwaltung werden neben Ihrer Konfigurationsauswahl in Studio festgelegt.

Die Richtlinien, die von der Profilverwaltung angepasst werden, werden in der Tabelle unten angezeigt. Nicht-Standard-Richtlinieneinstellungen bleiben erhalten und werden nicht von diesem Feature überschrieben. Weitere Informationen zu jeder Richtlinie finden Sie in der Dokumentation zur Profilverwaltung. Die Maschinentypen, für die Profile erstellt werden, wirken sich auf die angepassten Richtlinien aus. Wichtig ist, ob Maschinen persistent oder bereitgestellt sind, und ob sie von mehreren Benutzern gemeinsam verwendet werden oder nur einem dedizierten Benutzer zugeordnet sind.

Persistente Systeme verfügen über einen lokalen Speicher, dessen Inhalt auch nach dem Abschalten des Systems bestehen bleibt. Persistente Systeme imitieren u. U. mit Speichertechnologien wie Speichernetzwerke (Storage Area Networks, 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 Netzwerk-Disk imitiert.

Letztere wird oft über ein SAN mit einer Hochgeschwindigkeitsverbindung zur Verfügung gestellt. Für die Bereitstellung wird allgemein Provisioning Services oder die Maschinenerstellungsdienste (oder ein entsprechendes Produkt eines Drittanbieters) verwendet. Manchmal haben bereitgestellte Systeme persistenten lokalen Speicher, der möglicherweise durch persönliche vDisks zur Verfügung gestellt wird; diese werden als persistent klassifiziert.

Zusammen definieren diese beiden Faktoren die folgenden Maschinentypen:

- **Persistent und dediziert**: Beispiele sind Desktopbetriebssystemmaschinen mit festen Zuweisungen und einer persönlichen vDisk, die mit den Maschinenerstellungsdiensten erstellt wurden, Desktops mit persönlichen vDisks, die in VDI-in-a-Box erstellt wurden, physische Arbeitsstationen und Laptops.
- **Persistent und freigegeben**: Beispiele sind Serverbetriebssystemmaschinen, die mit den Maschinenerstellungsdiensten erstellt wurden.
- **Bereitgestellt und dediziert**: Beispiele sind Desktopbetriebssystemmaschinen mit statischen Zuweisungen, aber ohne persönliche vDisk, die mit Provisioning Services erstellt wurden.
- **Bereitgestellt und freigegeben**: Beispiele sind Desktopbetriebssystemmaschinen mit zufälliger Zuweisung, die mit Provisioning Services erstellt wurden, und Desktops ohne persönliche vDisks, die mit VDI-in-a-Box erstellt wurden.

Die folgenden Richtlinieneinstellungen der Profilverwaltung werden für die verschiedenen Maschinentypen empfohlen. Sie funktionieren in den meisten Fällen gut, aber Sie müssen sie ggf. an die Anforderungen Ihrer Bereitstellung anpassen.

Wichtig: Lokal zwischengespeicherte Profile nach Abmeldung löschen, Profilstreaming und Immer zwischenspeichern werden durch die automatische Konfiguration erzwungen. Passen Sie die anderen Richtlinien manuell an.

Persistente Maschinen

Richtlinie	Persistent und dediziert	Persistent und freigegeben
Lokal zwischengespeicherte Profile nach 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 und freigegeben
Lokal zwischengespeicherte Profile nach Abmeldung	Deaktiviert (Hinweis 5)	Aktiviert

löschen Richtlinie	Bereitgestellt und dediziert	Bereitgestellt und freigegeben
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 XenApp-Servern roamen. Aktivieren Sie in dieser Situation diese Richtlinie.
4. Deaktivieren Sie Anmeldungen lokaler Administratoren verarbeiten, außer für gehostete, freigegebene Desktops. Aktivieren Sie in dieser Situation diese Richtlinie.
5. Deaktivieren Sie Lokal zwischengespeicherte Profile nach Abmeldung löschen. Damit bleiben lokal zwischengespeicherte Profile erhalten. Da die Maschinen beim Abmelden zurückgesetzt werden, aber einzelnen Benutzern zugewiesen sind, ist die Anmeldung mit zwischengespeicherten Profile schneller.
6. Deaktivieren Sie Immer zwischenspeichern. Sie können sicherstellen, dass große Dateien möglichst bald nach der Anmeldung in Profile geladen werden, wenn Sie diese Richtlinie aktivieren und mit ihr ein Dateigrößenlimit definieren (in MB). Dateien, die diese Größe überschreiten, werden so schnell wie möglich lokal zwischengespeichert.
7. Aktivieren Sie Anmeldungen lokaler Administratoren verarbeiten, außer für Benutzer, die zwischen XenApp- und XenDesktop-Servern roamen. Deaktivieren Sie in dieser Situation diese Richtlinie.

Die Ordnerumleitung ermöglicht das Speichern von Benutzerdaten auf Netzwerkfreigaben, die nicht zum Speichern von Profilen verwendet werden. Dies verringert die Profilgröße und die Ladezeit, hat aber möglicherweise Auswirkungen auf die Netzwerkbandbreite. Zur Ordnerumleitung müssen keine Citrix Benutzerprofile verwendet werden. Sie können die Benutzerprofile selbst verwalten und dennoch Ordner umleiten.

Konfigurieren Sie die Ordnerumleitung mit den Citrix Richtlinien in Studio.

- Stellen Sie sicher, dass die Netzwerkspeicherorte zum Speichern des Inhalts von umgeleiteten Ordnern verfügbar sind, und die erforderlichen Berechtigungen richtig sind. Die Speicherorteigenschaften werden überprüft.
- Umgeleitete Ordner werden im Netzwerk eingerichtet und mit Inhalten der virtuellen Desktops bei der Anmeldung aufgefüllt.

Hinweis: Konfigurieren Sie die Ordnerumleitung entweder mit den Citrix Richtlinien oder den Active Directory-Gruppenrichtlinienobjekten, jedoch nicht mit beiden. Das Konfigurieren der Ordnerumleitung mit beiden Richtlinienengines kann zu unvorhersehbarem Verhalten führen.

In Bereitstellungen mit mehreren Betriebssystemen können Sie Teile eines Benutzerprofils für jedes Betriebssystem

freigeben. Der Rest des Profils ist nicht freigegeben und kann nur von einem Betriebssystem verwendet werden. Um sicherzustellen, dass die Benutzererfahrung für alle Betriebssysteme konsistent ist, benötigen Sie für jedes Betriebssystem eine andere Konfiguration. Dies ist die erweiterte Ordnerumleitung. Beispiel: Bei verschiedenen Versionen einer Anwendung auf zwei Betriebssystemen muss möglicherweise eine freigegebene Datei gelesen oder bearbeitet werden. Sie entscheiden daher, sie an einen einzigen Speicherort im Netzwerk umzuleiten, von dem beide Versionen auf sie zugreifen können. Oder Sie entscheiden, da die Inhalte des Startmenüordners der beiden Betriebssysteme unterschiedlich strukturiert sind, nur einen Ordner statt beide umzuleiten. Dadurch werden die Startmenüordner und die Inhalte auf jedem Betriebssystem getrennt, und die Benutzererfahrung ist konsistent.

Wenn Sie die erweiterte Ordnerumleitung in Ihrer Bereitstellung benötigen, müssen Sie die Struktur der Profildaten Ihrer Benutzer genau kennen und festlegen, welche Teile davon zwischen Betriebssystemen freigegeben werden können. Dies ist wichtig, weil eine falsch angewendete Ordnerumleitung zu unvorhersehbarem Verhalten führen kann.

Umleiten von Ordnern in erweiterten Bereitstellungen

- Verwenden Sie eine separate Bereitstellungsgruppe für jedes Betriebssystem.
- Informieren Sie sich, wo die Benutzerdaten und -einstellungen von den virtuellen Anwendungen, einschließlich solcher auf virtuellen Desktops, gespeichert werden, und wie die Daten strukturiert sind.
- Leiten Sie die Ordner bei freigegebenen Profildaten, bei denen ein sicheres Datenroaming gewährleistet ist (da sie in jedem Betriebssystem identisch strukturiert sind), in jeder Bereitstellungsgruppe um.
- Bei nicht freigegebenen Profildaten, für die kein Roaming möglich ist, leiten Sie den Ordner nur in einer Desktopgruppe um. Dies ist in der Regel diejenige mit dem am häufigsten verwendeten Betriebssystem oder diejenige mit den relevantesten Daten. Alternativ können Sie bei nicht freigegebenen Daten, für die kein Roaming zwischen Betriebssystemen möglich ist, die Ordner beider Betriebssysteme an separate Netzwerkadressen umleiten.

Beispiel einer erweiterten Bereitstellung: Diese Bereitstellung umfasst Anwendungen einschließlich Versionen von Microsoft Outlook und Internet Explorer, die auf Windows 8-Desktops und Anwendungen ausgeführt werden, sowie andere Versionen von Outlook und Internet Explorer, die von Windows Server 2008 bereitgestellt werden. Sie haben hierfür bereits zwei Bereitstellungsgruppen für die beiden Betriebssysteme eingerichtet. Die Benutzer möchten auf dieselben Kontakte und Favoriten in beiden Versionen dieser beiden Anwendungen zugreifen.
Wichtig: Die folgenden Entscheidungen und Hinweise gelten für die hier beschriebenen Betriebssysteme und die beschriebene Bereitstellung. Die Ordner, die Sie in Ihrer Organisation umleiten oder freigeben, hängen von mehreren Faktoren ab, die nur für Ihre Bereitstellung relevant sind.

- Sie leiten mit Richtlinien, die auf Bereitstellungsgruppen angewendet werden, die folgenden Ordner um:

Ordner	Umleitung in Windows 8?	Umleitung in Windows Server 2008?
Dokumente	Ja	Ja
Anwendungsdaten	Nein	Nein
Kontakte	Ja	Ja
Desktop	Ja	Nein
Downloads	Nein	Nein
Favoriten	Ja	Ja

Ordner	Umleitung in Windows 8?	Umleitung in Windows Server 2008?
Verknüpfungen	Ja	Nein
Musik	Ja	Ja
Bilder	Ja	Ja
Videos	Ja	Ja
Suchen	Ja	Nein
Gespeicherte Spiele	Nein	Nein
Startmenü	Ja	Nein

- Bei freigegebenen, umgeleiteten Ordnern:
  - Nach der Analyse der Datenstruktur der von anderen Versionen von Outlook und Internet Explorer gespeicherten Daten entscheiden Sie, dass es sicher ist, die Ordner für Kontakte und Favoriten freizugeben.
  - Sie wissen, dass die Struktur der Ordner Eigene Dokumente, Musik, Bilder und Videos auf allen Betriebssystemen gleich ist, und sie können daher für jede Bereitstellungsgruppe am gleichen Netzwerkspeicherort gespeichert werden.
- 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 unterschiedlich in den beiden Betriebssystemen organisiert sind. Eine Freigabe ist daher nicht möglich.
  - Um ein vorhersagbares Verhalten für diese nicht freigegebenen Daten sicherzustellen, leiten Sie sie nur in der Windows 8-Bereitstellungsgruppe um. Sie entscheiden dies, da Windows 8 öfter von den Benutzern bei ihrer täglichen Arbeit verwendet wird, die vom Server bereitgestellten Anwendungen hingegen werden nur gelegentlich genutzt. Außerdem sind in diesem Fall die nicht freigegebenen Daten relevanter für eine Desktop- als für eine Anwendungsumgebung. Desktopverknüpfungen werden beispielsweise im Ordner "Desktop" gespeichert und sind nützlich, wenn sie von einer Windows 8-Maschine, aber nicht von einem Windows-Server stammen.
- Bei nicht umgeleiteten Ordnern:
  - Die Server sollen keine von Benutzern heruntergeladene Dateien ansammeln, und Sie leiten den Ordner "Downloads" daher nicht um.
  - Daten von einzelnen Anwendungen können zu Kompatibilitäts- und Leistungsproblemen führen. Daher leiten Sie den Ordner "Anwendungsdaten" nicht um.

Weitere Informationen zur Ordnerumleitung finden Sie unter http://technet.microsoft.com/en-us/library/cc766489%28v=ws.10%29.aspx.

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 die Ausschlussfunktion arbeiten zusammen, d. h. wenn Sie sicherstellen, dass keine umgeleiteten

Ordner ausgeschlossen sind, können sie von der Profilverwaltung wieder in die Profilordnerstruktur verschoben werden, während gleichzeitig die Datenintegrität beibehalten wird, sollten sie später doch nicht umgeleitet werden. Weitere Informationen zu Ausschlüssen finden Sie unter Aufnehmen und Ausschließen von Objekten.

Überwachung

Feb 29, 2016

Administratoren und Helpdesk-Mitarbeiter können XenApp- und XenDesktop-Sites mit einer Reihe von Features und Tools überwachen. Sie können Folgendes überwachen:

- Benutzersitzungen und Sitzungsverwendung
- Anmeldungsleistung
- Verbindungen und Computer, einschließlich Ausfälle
- Lastauswertung
- Historische Trends
- Infrastruktur

Citrix Director

Director ist ein Echtzeit-Webtool, mit dem Sie Endbenutzer überwachen, Fehler beheben und Support leisten können.

Weitere Informationen finden Sie in den Artikeln zu Director.

Sitzungsaufzeichnung

Die Sitzungsaufzeichnung ermöglicht das Aufzeichnen von Bildschirmaktivitäten in der Sitzung eines Benutzers über eine beliebige Verbindung von einem XenApp-Server (im Einklang mit den Unternehmensrichtlinien und gesetzlichen Vorschriften). Mit der Sitzungsaufzeichnung können Sie Sitzungen aufzeichnen, katalogisieren und archivieren und sie erneut aufrufen und wiedergeben.

Die Sitzungsaufzeichnung verwendet flexible Richtlinien, mit denen automatisch Aufnahmen von Anwendungssitzungen ausgelöst werden können. Das IT-Team kann damit die Benutzeraktivität von Anwendungen überwachen und prüfen, z. B. Buchhaltungs- und Patienteninformationssysteme für das Gesundheitswesen, und interne Kontrollen zur Einhaltung von gesetzlichen Vorschriften und die Sicherheitsüberwachung unterstützen. Die Sitzungsaufzeichnung vereinfacht auch den technischen Support, da die Problemerkennung und Behebung der Probleme beschleunigt werden.

Weitere Informationen finden Sie in den Artikeln zur Sitzungsaufzeichnung.

Konfigurationsprotokollierung

Die Konfigurationsprotokollierung ist ein Feature, mit dem Administratoren administrative Änderungen verfolgen, die an einer Site vorgenommen werden. Die Konfigurationsprotokollierung ermöglicht Administratoren die Diagnose und Problembehandlung nach der Durchführung von Konfigurationsänderungen, Hilfe beim Änderungsmanagement und der Nachverfolgung von Konfigurationen sowie Berichte über Administratoraktivitäten.

Sie können Berichte mit protokollierten Informationen über Studio generieren und anzeigen. Zum Zweck der Benachrichtigung über Konfigurationsänderungen können Sie protokollierte Elemente außerdem in der Trendansicht von Director anzeigen. Dieses Feature ist für Administratoren nützlich, die keinen Zugriff auf Studio haben.

Die Trendansicht bietet historische Daten von Konfigurationsänderungen in einem bestimmten Zeitraum, sodass Administratoren beurteilen können, welche Änderungen wann und von wem an einer Site vorgenommen wurden, um die Ursache eines Problems zu finden. Konfigurationsinformationen werden in dieser Ansicht in drei Kategorien unterteilt.

- Verbindungsfehler

- Fehlgeschlagene Desktopmaschinen
- Fehlgeschlagene Servermaschinen

Weitere Informationen zum Aktivieren und Konfigurieren der Konfigurationsprotokollierung finden Sie im Artikel Konfigurationsprotokollierung. Im Artikel Director wird beschrieben, wie protokollierte Informationen über dieses Tool angezeigt werden.

Überwachungsdienst-API mit OData-Protokoll

Mit der Überwachungsdienst-API einer Site können Administratoren unter Verwendung des OData-Protokolls historische Daten durchsuchen. Dies ermöglicht IT-Mitarbeitern das Analysieren historischer Trends für die Planung, das Durchführen gezielter Problembehandlung bei Verbindungs- und Maschinenfehlern und das Extrahieren von Informationen für die Eingabe in andere Tools und Prozesse.

Das Schema des Überwachungsdiensts bietet folgende Datentypen:

- Daten zu Verbindungsfehlern
- Maschinen in fehlerhaftem Zustand
- Sitzungsnutzung
- Anmeldedauer
- Daten zum Lastausgleich

Weitere Informationen finden Sie in den Artikeln zur Überwachungsdienst-OData-API.

Diagnose Tool für persönliche vDisks

Mit dem PvD-Diagnosetool können Sie Änderungen überwachen, die Benutzer an Benutzer- und Anwendungskomponenten ihrer persönlichen vDisks vornehmen, z. B. Installation von Anwendungen oder Änderungen an Dateien.

Weitere Informationen finden Sie in dem Artikel Überwachen von Personal vDisks.

Sitzungsaufzeichnung

Feb 29, 2016

Die Sitzungsaufzeichnung ermöglicht das Aufzeichnen von Bildschirmaktivitäten in der Sitzung eines Benutzers von einer VDA-Serverbetriebssystemmaschine über eine beliebige Verbindung (im Einklang mit den Unternehmensrichtlinien und gesetzlichen Vorschriften). Mit der Sitzungsaufzeichnung können Sie Sitzungen aufzeichnen, katalogisieren und archivieren und sie erneut aufrufen und wiedergeben.

Die Sitzungsaufzeichnung verwendet flexible Richtlinien, mit denen automatisch Aufnahmen von Anwendungssitzungen ausgelöst werden können. Das IT-Team kann damit die Benutzeraktivität von Anwendungen überwachen und prüfen, z. B. Buchhaltungs- und Patienteninformationssysteme für das Gesundheitswesen, und interne Kontrollen zur Einhaltung von gesetzlichen Vorschriften und die Sicherheitsüberwachung unterstützen. Die Sitzungsaufzeichnung vereinfacht auch den technischen Support, da die Problemerkennung und Behebung der Probleme beschleunigt werden.

Erhöhte Sicherheit durch Protokollierung und Überwachung: Mit der Sitzungsaufzeichnung können Unternehmen die Aktivität der Benutzer auf dem Bildschirm für Anwendungen aufzeichnen, die vertrauliche Informationen verarbeiten. Dies ist besonders in stark regulierten Branchen wichtig, z. B. im Gesundheits- und Finanzwesen. Richtliniensteuerelemente ermöglichen eine selektive Aufzeichnung, wenn persönliche Daten ins Spiel kommen, die nicht aufgezeichnet werden dürfen.

Leistungsfähige Aktivitätsüberwachung: Die Sitzungsaufzeichnung erfasst und archiviert Bildschirmaktualisierungen, einschließlich Mausklicks und die visuelle Ausgabe von Tastaturanschlägen in gesicherten Videoaufzeichnungen, um die Aktivität für bestimmte Benutzer, Anwendungen und Server zu dokumentieren.

Die Sitzungsaufzeichnung ist nicht dafür ausgelegt oder vorgesehen, Beweismittel für Rechtsverfahren zu sammeln. Citrix empfiehlt, dass Unternehmen, die die Sitzungsaufzeichnung verwenden, andere Methoden der Beweismittelsammlung nutzen, z. B. konventionelle Videoaufzeichnungen in Kombination mit textbasierten eDiscovery-Tools.

Schnellere Problembehebung: Wenn sich Benutzer mit einem Problem an den Helpdesk wenden, das schwer zu reproduzieren ist, können die Supportmitarbeiter die Aufzeichnung von Benutzersitzungen aktivieren. Wenn das Problem wieder auftritt, stellt die Sitzungsaufzeichnung eine visuelle Aufzeichnung des Fehlers bereit, einschließlich Zeitstempel, mit der Benutzerprobleme schneller gelöst werden können.

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

Konfigurationsprotokollierung

Feb 29, 2016

Die Konfigurationsprotokollierung dient zum Erfassen der Sitekonfigurationsänderungen und Administratoraktivitäten in einer Datenbank. Sie können den protokollierten Inhalt folgendermaßen verwenden:

- Diagnose und Problembehandlung nach der Durchführung von Konfigurationsänderungen; das Protokoll liefert eine Breadcrumbspur.
- Hilfe beim Änderungsmanagement und der Nachverfolgung von Konfigurationen
- Bericht über Administratoraktivitäten

Zum Festlegen der Einstellungen für die Konfigurationsprotokollierung, zum Anzeigen der Konfigurationsprotokolle und zum Generieren von HTML- und CSV-Berichten verwenden Sie Citrix Studio. Sie können die Anzeige des Konfigurationsprotokolls durch Datumsbereiche und durch Ergebnisse der Volltextsuche filtern. Ist die verbindliche Protokollierung aktiviert, verhindert sie, dass Änderungen an der Konfiguration vorgenommen werden, es sei denn diese können protokolliert werden. Mit der entsprechenden Berechtigung können Sie Einträge aus dem Konfigurationsprotokoll löschen. Sie können das Feature der Konfigurationsprotokollierung nicht zum Bearbeiten des Inhalts von Protokollen verwenden.

Die Konfigurationsprotokollierung verwendet ein PowerShell 2.0-SDK und den Konfigurationsprotokollierungsdienst. Der Konfigurationsprotokollierungsdienst wird auf allen Controllern in der Site ausgeführt. Wenn ein Controller ausfällt, übernimmt automatisch der Dienst auf einem anderen Controller die Verarbeitung von Protokollanforderungen.

Standardmäßig ist die Konfigurationsprotokollierung aktiviert und verwendet die Datenbank, die zusammen mit der Site erstellt wurde (die Sitekonfigurationsdatenbank). Citrix empfiehlt dringend, den Speicherort der Datenbank für die Konfigurationsprotokollierung so schnell wie möglich nach der Erstellung einer Site zu ändern. Die Konfigurationsprotokollierungsdatenbank unterstützt dieselben Features für hohe Verfügbarkeit wie die Sitekonfigurationsdatenbank.

Der Zugriff auf die Konfigurationsprotokollierung wird über die delegierte Administration mit den Einstellungen "Protokollierungseinstellungen bearbeiten" und "Konfigurationsprotokolle anzeigen" gesteuert.

Konfigurationsprotokolle werden bei der Erstellung lokalisiert. Beispiel: Ein in Englisch erstelltes Protokoll wird unabhängig vom Gebietsschema des Lesers in Englisch gelesen.

Gegenstand der Protokollierung

Konfigurationsänderungen und Administratoraktivitäten, die von Studio, Director und PowerShell-Skripts ausgehen, werden protokolliert. Beispiele protokollierter Konfigurationsänderungen sind Arbeiten (Erstellen, Bearbeiten, Löschen, Zuweisen) mit:

- Maschinenkataloge
- Bereitstellungsgruppen (einschließlich Ändern der Energieverwaltungseinstellungen)
- Administratorrollen und Geltungsbereiche
- Hostressourcen und Verbindungen
- Citrix Richtlinien über Studio

Beispiele protokollierter Administratoraktivitäten:

- Energieverwaltung für eine virtuelle Maschine oder einen Benutzerdesktop
- Senden einer Nachricht an einen Benutzer von Studio oder Director aus

Die folgenden Vorgänge werden nicht protokolliert:

- Autonome Vorgänge wie das Einschalten virtueller Maschinen per Poolverwaltung.
- Über die Gruppenrichtlinien-Verwaltungskonsole implementierte Richtlinienaktionen; verwenden Sie Microsoft-Tools, um Protokolle dieser Aktionen anzuzeigen.
- Über die Registrierung vorgenommene Änderungen, direkter Zugriff von der Datenbank oder von anderen Quellen als Studio, Director oder PowerShell.
- Wenn die Bereitstellung initialisiert wird, steht die Konfigurationsprotokollierung ab dem Zeitpunkt zur Verfügung, zu dem die erste Instanz des Konfigurationsprotokollierungsdiensts sich beim Konfigurationsdienst registriert. Daher werden die frühen Phasen der Konfiguration nicht protokolliert (z. B., wenn das Datenbankschema bei der Initialisierung eines Hypervisors abgerufen und angewendet wird).

Verwalten der Konfigurationsprotokollierung

Standardmäßig wird für die Konfigurationsprotokollierung die Datenbank verwendet, die zusammen mit einer Site erstellt wird (die Sitekonfigurationsdatenbank). Citrix empfiehlt aus folgenden Gründen, einen anderen Speicherort für die Konfigurationsprotokollierungsdatenbank und die Überwachungsdatenbank zu wählen:

- Die Backupstrategie für die Konfigurationsprotokollierungsdatenbank unterscheidet sich wahrscheinlich von der Backupstrategie für die Sitekonfigurationsdatenbank.
- Die Menge der für die Konfigurationsprotokollierung (und den Überwachungsdienst) gesammelten Daten kann den für die Sitekonfigurationsdatenbank verfügbaren Speicherplatz zu stark limitieren.
- Eine einzelne Fehlerquelle für die drei Datenbanken wird beseitigt (d. h. aufgeteilt).

Hinweis: Produkteditionen, die keine Konfigurationsprotokollierung unterstützen, haben keinen Knoten namens "Protokollierung" in Studio.

Aktivieren/Deaktivieren der Konfigurationsprotokollierung und der verbindlichen Protokollierung

Standardmäßig ist die Konfigurationsprotokollierung aktiviert und die verbindliche Protokollierung ist deaktiviert.

1. Wählen Sie im Studio-Navigationsbereich **Protokollierung** aus.
2. Wählen Sie im Aktionsbereich **Einstellungen** aus. Das Dialogfeld "Konfigurationsprotokollierung" enthält die Datenbankinformationen und Angaben dazu, ob Konfigurationsprotokollierung und verbindliche Protokollierung aktiviert oder deaktiviert sind.
3. Wählen Sie die gewünschte Aktion:

   Zum Aktivieren der Konfigurationsprotokollierung wählen Sie das Optionsfeld **Protokollierung aktivieren**. Dies ist die Standardeinstellung. Wenn nicht in die Datenbank geschrieben werden kann, werden die Informationen verworfen,

der Vorgang wird jedoch fortgesetzt.

Zum Deaktivieren der Konfigurationsprotokollierung wählen Sie das Optionsfeld **Protokollierung deaktivieren**. Wenn die Protokollierung zuvor aktiviert war, können bereits vorhandene Protokolle weiterhin mit dem PowerShell-SDK gelesen werden.

Zum Aktivieren der verbindlichen Protokollierung deaktivieren Sie das Kontrollkästchen **Änderungen zulassen, wenn die Verbindung mit der Datenbank getrennt ist**. Es wird dann keine Konfigurationsänderung oder administrative Aktivität, die normalerweise protokolliert würde, zugelassen, es sei denn, sie kann in die Konfigurationsprotokollierungsdatenbank geschrieben werden. Sie können die verbindliche Protokollierung nur aktivieren, wenn die Konfigurationsprotokollierung aktiviert ist, d. h. wenn das Optionsfeld **Protokollierung aktivieren** für die Konfigurationsprotokollierung aktiviert ist. Tritt bei dem Dienst für die Konfigurationsprotokollierung ein Fehler auf, und die hohe Verfügbarkeit wird nicht verwendet, beginnt die verbindliche Protokollierung. In solchen Fällen werden Vorgänge, die normalerweise protokolliert würden, nicht ausgeführt.

Zum Deaktivieren der verbindlichen Protokollierung aktivieren Sie das Kontrollkästchen **Änderungen zulassen, wenn die Verbindung mit der Datenbank getrennt ist**. Konfigurationsänderungen und administrative Aktivitäten sind dann zulässig, selbst wenn kein Zugriff auf die Datenbank für die Konfigurationsprotokollierung besteht. Dies ist die Standardeinstellung.

Ändern des Speicherorts für die Konfigurationsprotokollierungsdatenbank

Hinweis: Sie können den Speicherort der Datenbank nicht ändern, wenn die verbindliche Protokollierung aktiviert ist, da bei der Standortänderung eine kurze Trennung verursacht wird, die nicht protokolliert werden kann.

1. Erstellen Sie einen Datenbankserver mit einer unterstützten SQL Server-Version.
2. Wählen Sie im Studio-Navigationsbereich **Protokollierung** aus.
3. Wählen Sie im Aktionsbereich **Einstellungen** aus.
4. Klicken Sie im Dialogfeld "Protokollierungseinstellungen" auf **Protokollierungsdatenbank ändern**.
5. Geben Sie im Dialogfeld "Protokollierungsdatenbank ändern" den Speicherort des Servers mit dem neuen Datenbankserver ein. Gültige Formate sind im Artikel "Datenbanken" aufgeführt.
6. Damit die Datenbank von Studio erstellt wird, klicken Sie auf **OK**. Wenn Sie dazu aufgefordert werden, klicken Sie auf **OK** und die Datenbank wird automatisch erstellt. Studio versucht, mit den Anmeldeinformationen des aktuellen Studio-Benutzers auf die Datenbank zuzugreifen; wenn dies fehlschlägt, werden Sie zur Eingabe der Anmeldeinformationen des Datenbankbenutzers aufgefordert. Das Datenbankschema wird dann von Studio in die Datenbank hochgeladen. (Die Anmeldeinformationen werden nur während der Datenbankerstellung gespeichert.)
7. Zum manuellen Erstellen der Datenbank klicken Sie auf **Datenbankskript erstellen**. Das generierte Skript enthält Anweisungen zum manuellen Erstellen der Datenbank. Stellen Sie vor dem Hochladen des Schemas sicher, dass die Datenbank leer ist und dass mindestens ein Benutzer Zugriffs- bzw. Änderungsberechtigung für die Datenbank hat.

Die Daten der Konfigurationsprotokollierung aus der älteren Datenbank werden nicht in die neue Datenbank importiert. Die Protokolle beider Datenbanken können beim Abrufen von Protokollen nicht aggregiert werden. Der erste Protokolleintrag in der neuen Datenbank für die Konfigurationsprotokollierung gibt an, dass eine Datenbankänderung stattfand; die vorherige Datenbank wird jedoch nicht identifiziert.

Anzeigen des Konfigurationsprotokolls

Beim Initiieren von Konfigurationsänderungen und bei Verwaltungsaktivitäten werden die von Studio und Director bewirkten High-Level-Operationen im oberen mittleren Bereich von Studio angezeigt. Eine High-Level-Operation führt zu mindestens einem Dienst- und SDK-Aufruf, bei dem es sich um eine Low-Level-Operation handelt. Wenn Sie eine High-Level-Operation im oberen mittleren Bereich auswählen, werden im unteren mittleren Bereich die Low-Level-Operationen angezeigt.

Schlägt eine Operation vor der Beendigung fehl, kann die Protokollierung evtl. in der Datenbank nicht abgeschlossen werden, sodass z. B. ein Startdatensatz keinen entsprechenden Stoppdatensatz hat. In solchen Fällen wird im Protokoll angezeigt, dass Informationen fehlen. Wenn Sie Protokolle auf Zeitbereichsbasis anzeigen, werden unvollständige Protokolle angezeigt, wenn die Daten in den Protokollen mit den Kriterien übereinstimmen. Beispiel: Wenn alle Protokolle für die letzten fünf Tage angefordert werden und ein Protokoll eine in den letzten fünf Tagen gelegene Startzeit aber keine Endzeit hat, wird dieses ebenfalls angezeigt.

Wenn Sie bei Verwendung eines Skripts zum Aufrufen von PowerShell-Cmdlets eine Low-Level-Operation erstellen ohne die übergeordnete High-Level-Operation anzugeben, wird von der Konfigurationsprotokollierung eine Ersatz-High-Level-Operation erstellt.

Zum Anzeigen des Inhalts des Konfigurationsprotokolls wählen Sie im Studio-Navigationsbereich **Protokollierung**. Standardmäßig wird im mittleren Bereich der Protokollinhalt chronologisch (neueste Einträge zuerst), angezeigt, wobei die Einträge durch das Datum getrennt sind.

Zum Filtern der Anzeige nach folgenden Kriterium	Führen Sie folgenden Schritt aus
Suchergebnisse	Geben Sie Text in das Feld "Suchen" oben im mittleren Bereich ein. Die gefilterte Anzeige enthält die Anzahl der Suchergebnisse. Zum Zurückkehren zur Standardprotokollanzeige löschen Sie den Text im Feld Suchen.
Spaltenüberschrift	Klicken Sie auf eine Spaltenüberschrift, um die Anzeige nach dem entsprechenden Feld zu sortieren.
Datumsbereich	Wählen Sie aus der Dropdownliste neben dem Feld "Suchen" oben im mittleren Bereich ein Intervall aus.

Erstellen von Berichten

Sie können CSV- und HTML-Berichte mit Konfigurationsprotokolldaten generieren.

- Der CSV-Bericht enthält alle Protokolldaten aus einem angegebenen Zeitintervall. Die hierarchischen Daten in der Datenbank werden in eine einzelne CSV-Tabelle vereinfacht. Kein Aspekt der Daten hat Vorrang in der Datei. Es wird keine Formatierung verwendet und keine Lesbarkeit angenommen. Die Datei (unter dem Namen "MyReport") enthält lediglich die Daten in einem allgemein verwendbaren Format. CSV-Dateien werden oft für die Archivierung oder als Datenquelle für ein Tool zur Bearbeitung von Berichten oder Daten (z. B. Microsoft Excel) verwendet.

- Der HTML-Bericht enthält Protokolldaten aus einem angegebenen Zeitintervall in lesbarem Format. Er bietet eine strukturierte Ansicht für die Prüfung auf Änderungen, durch die navigiert werden kann. Der HTML-Bericht umfasst zwei Dateien: Zusammenfassung und Details. Die Zusammenfassung enthält High-Level-Operationen mit Informationen zu Zeitpunkt, Auslöser und Ergebnis. Durch Klicken auf den Link Details neben jedem Vorgang navigieren Sie zu den Low-Level-Operationen in der Datei Details, die zusätzliche Informationen bietet.

Zum Generieren eines Konfigurationsprotokollierungsberichts wählen Sie im Studio-Navigationsbereich **Protokollierung** und dann im Aktionsbereich **Benutzerdefinierten Bericht erstellen**.

- Wählen Sie den Datumsbereich für den Bericht.
- Wählen Sie das Berichtsformat: CSV, HTML oder beides.
- Navigieren Sie zu dem Speicherort, an dem der Bericht gespeichert werden soll.

Löschen des Konfigurationsprotokolls

Zum Löschen des Konfigurationsprotokolls müssen Sie über bestimmte Rechte der delegierten Administration und Berechtigungen für die SQL Server-Datenbank verfügen.

- **Delegierte Administration**: Sie müssen eine Rolle der delegierten Administration haben, mit der die Bereitstellungskonfiguration gelesen werden kann. Die integrierte Volladministratorrolle hat diese Berechtigung. Für eine benutzerdefinierte Rolle muss für die Kategorie "Andere Berechtigungen" "Lesen" oder "Verwalten" aktiviert sein. Wenn Sie die Konfigurationsprotokolldaten vor dem Löschen sichern möchten, muss die benutzerdefinierte Rolle in der Kategorie der Protokollierungsberechtigungen Lese- oder Verwaltungsberechtigung haben.

- **SQL Server-Datenbank**: Sie müssen einen Anmeldenamen für SQL Server haben und zum Löschen von Datensätzen aus der Datenbank berechtigt sein. Dies kann mit zwei Möglichkeiten erreicht werden:
  - Verwenden Sie zur Anmeldung für die SQL Server-Datenbank die Serverrolle "sysadmin", mit der Sie beliebige Aktivitäten auf dem Datenbankserver durchführen können. Auch die Serverrollen "serveradmin" oder "setupadmin" sind zum Löschen von Vorgängen berechtigt.
  - Wenn Ihre Bereitstellung zusätzliche Sicherheit erfordert, verwenden Sie Anmeldeinformationen einer anderen Rolle als "sysadmin", die einem Datenbankbenutzer zugeordnet sind, der zum Löschen von Datensätzen aus der Datenbank berechtigt ist.
    1. Erstellen Sie in SQL Server Management Studio eine SQL Server-Anmeldung mit einer anderen Serverrolle (nicht "sysadmin").
    2. Ordnen Sie diese Anmeldung einem Benutzer in der Datenbank zu; SQL Server erstellt automatisch einen Benutzer in der Datenbank mit dem gleichen Namen wie die Anmeldung.
    3. Geben Sie für die Datenbankrollen-Mitgliedschaft mindestens eines der Rollenmitglieder für den Datenbankbenutzer an: ConfigurationLoggingSchema_ROLE oder dbowner.

    Weitere Informationen finden Sie in der Dokumentation zu SQL Server Management Studio.

Löschen der Konfigurationsprotokolle:

1. Wählen Sie im Studio-Navigationsbereich **Protokollierung** aus.
2. Wählen Sie im Aktionsbereich **Protokolle löschen** aus.
3. Sie haben nun die Möglichkeit, vor dem Löschen ein Backup der Protokolle anzulegen. Wenn Sie eine Backupdatei erstellen, navigieren Sie zu dem Speicherort, an dem diese gespeichert werden soll. Das Backup wird als CSV-Datei erstellt.

Nach dem Löschen der Konfigurationsprotokolle wird das Löschen des Protokolls als erste Aktivität im leeren Protokoll

erfasst. Dieser Eintrag enthält Details darüber, wann und von wem die Protokolle gelöscht wurden.

Überwachen von Personal vDisks

Feb 29, 2016

Sie können ein Diagnosetool zum Überwachen der Änderungen verwenden, die von Benutzern an beiden Bereichen persönlicher vDisks (Benutzerdaten- und Anwendungsbereiche) vorgenommen werden. Zu diesen Änderungen gehören Anwendungen, die von Benutzern installiert wurden, und von ihnen geänderte Dateien. Die Änderungen werden in einer Reihe von Berichten erfasst.

1. Führen Sie auf der zu überwachenden Maschine **C:\Programme\Citrix\personal vDisk\bin\CtxPvdDiag.exe** aus.
2. Navigieren Sie zu einem Speicherort, an dem die Berichte und Protokolle gespeichert werden sollen, legen Sie fest, welche Berichte generiert werden sollen, und klicken Sie auf **OK**. Die verfügbaren Berichte sind unten aufgeführt.

Softwarestrukturbericht: Dieser Bericht generiert die beiden Dateien Software.Dat.Report.txt und Software.Dat.delta.txt.
In Software.Dat.Report.txt werden die Änderungen erfasst, die vom Benutzer an der Struktur "HKEY_LOCAL_MACHINE\Software" vorgenommen wurden. Der Bericht besteht aus den folgenden Abschnitten:

- List of Applications installed on the base: Anwendungen, die auf Ebene 0 installiert wurden
- List of user installed software: Anwendungen, die vom Benutzer im Anwendungsbereich der persönlichen vDisk installiert wurden
- List of software uninstalled by user: ursprünglich auf Ebene 0 installierte Anwendungen, die vom Benutzer entfernt wurden

Weitere Informationen zu Software.Dat.delta.txt finden Sie im Strukturdeltabericht.

Systemstrukturbericht: In der Datei SYSTEM.CurrentControlSet.DAT.Report.txt werden die Änderungen erfasst, die vom Benutzer an der Struktur "HKEY_LOCAL_MACHINE\System" vorgenommen wurden. Der Bericht besteht aus den folgenden Abschnitten:

- List of user installed services: vom Benutzer installierte Dienste und Treiber
- Startup of following services were changed: Dienste und Treiber, deren Starttyp vom Benutzer geändert wurde

Sicherheitsstrukturbericht: In der Datei SECURITY.DAT.Report.txt werden die Änderungen erfasst, die vom Benutzer an der Struktur "HKEY_LOCAL_MACHINE\Security" vorgenommen wurden.

Strukturbericht für die Sicherheitskontenverwaltung (SAM): In der Datei SAM.DAT.Report.txt werden die Änderungen erfasst, die vom Benutzer an der Struktur "HKEY_LOCAL_MACHINE\SAM" vorgenommen wurden.

Strukturdeltabericht: In der Datei Software.Dat.delta.txt werden alle hinzugefügten und entfernten Registrierungsschlüssel und alle Werte erfasst, die vom Benutzer an der Struktur "HKEY_LOCAL_MACHINE\Software" geändert wurden.

Personal vDisk-Protokolle: Die Protokolldateien Pud-IvmSupervisor.log, PvDActivation.log, PvDSvc.log, PvDWMI.log, SysVol-IvmSupervisor.log und vDeskService-<#>.log werden standardmäßig im Ordner P:\Users\\AppData\Local\Temp\PVDLOGS erstellt, jedoch an den ausgewählten Speicherort verschoben.

Windows-Betriebssystemprotokolle

- EvtLog_App.xml und EvtLog_System.xml sind die Anwendungs- und Systemereignisprotokolle im XML-Format aus dem Personal vDisk-Volume.

- Die Protokolle Setupapi.app.log und setuperr.log enthalten Protokollmeldungen bezüglich der Ausführung von msiexec.exe bei der Installation von Personal vDisk.
- Setupapi.dev.log enthält Protokollmeldungen über die Geräteinstallation.
- Msinfo.txt enthält die Ausgabe von msinfo32.exe. Informationen hierzu finden Sie in der Dokumentation von Microsoft.

Dateisystembericht: In der Datei FileSystemReport.txt werden die Änderungen erfasst, die vom Benutzer in folgenden Bereichen des Dateisystems vorgenommen wurden:

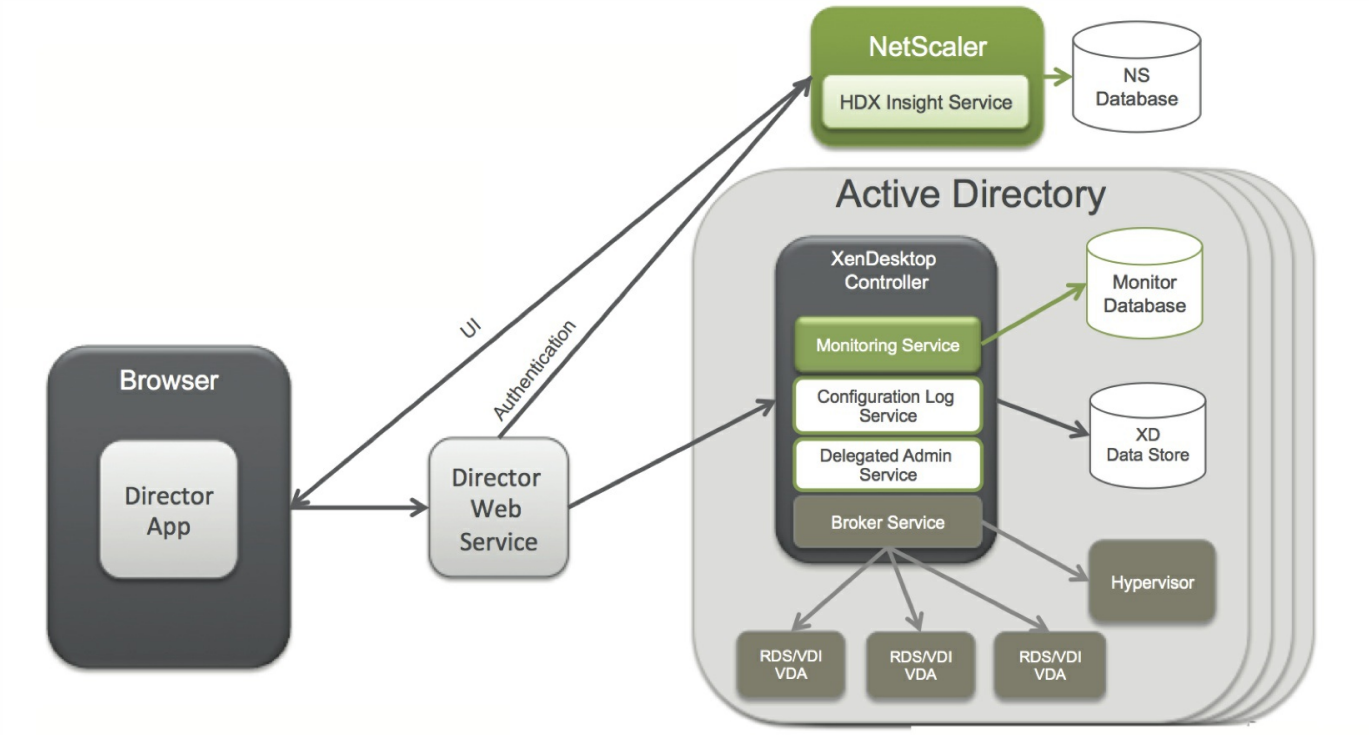
- Files Relocated: Dateien auf Ebene 0, die vom Benutzer zur vDisk verschoben wurden. Dateien der Ebene 0 sind Dateien, die aus dem Masterimage von der Maschine geerbt wurden, der die persönliche vDisk angefügt ist.
- Files Removed: Dateien auf Ebene 0, die durch eine Benutzeraktion (z. B. Entfernen einer Anwendung) verborgen wurden.
- Files Added (MOF,INF,SYS): Dateien mit der Erweiterung "mof", "inf" oder "sys", die vom Benutzer der Personal vDisk hinzugefügt wurden (z. B. bei der Installation einer Anwendung wie Visual Studio 2010, bei der eine MOF-Datei für die automatische Wiederherstellung registriert wird).
- Files Added Other: Andere Dateien, die der vDisk vom Benutzer hinzugefügt wurden (z. B. beim Installieren einer Anwendung).
- Base Files Modified But Not Relocated: Dateien auf Ebene 0, die vom Benutzer geändert wurden, jedoch nicht von den Personal vDisk-Kernelmodustreibern in der vDisk erfasst wurden.

Director

Feb 29, 2016

Dieser Abschnitt enthält folgende Themen:

Director ist ein Echtzeit-Webtool, mit dem Administratoren Endbenutzer überwachen, Fehler beheben und Support leisten können.



Director hat auf Folgendes Zugriff:

- Echtzeitdaten vom Broker Agent über eine einheitliche Konsole, die mit EdgeSight-Features, Leistungsverwaltung und Netzwerkinspektion integriert ist.
  - Die EdgeSight-Features umfassen Leistungsverwaltung zum Sicherstellen von Integrität und Kapazität, sowie historische Trends und Netzwerkanalyse (von NetScaler HDX Insight) zum Identifizieren von Engpässen, die auf dem Netzwerk in der XenApp- oder XenDesktop-Umgebung beruhen.
- In der Überwachungsdatenbank gespeicherte historische Daten für den Zugriff auf die Datenbank für die

Konfigurationsprotokollierung.

- ICA-Daten von NetScaler Gateway mit HDX Insight.
  - Übersicht über die Endbenutzererfahrung für virtuelle Anwendungen, Desktops und Benutzer in XenApp oder XenDesktop.
  - Korrelation von Netzwerkdaten mit Anwendungsdaten und Echtzeitmetrik für effektive Problembehandlung.
  - Integration mit dem Überwachungstool von XenDesktop 7 Director.
- Personal vDisk-Daten, die die Ausführungsüberwachung anhand von Basiszuordnung und Helpdesk-Mitarbeitern das Zurücksetzen von Personal vDisks ermöglichen (nur im Notfall zu verwenden).
  - Das Befehlszeilentool CtxPvdDiag.exe wird zum Sammeln von Benutzerinformationen in einer Datei zur Problembehandlung verwendet.

Director hat ein Dashboard zur Problembehandlung, das die Echtzeitzustandsüberwachung der XenApp- oder XenDesktop-Site ermöglicht. Mit dieser Funktion können Administratoren Fehler in Echtzeit sehen und einen besseren Eindruck von der Endbenutzererfahrung erhalten.

Ansichten

Director bietet verschiedene Ansichten der Schnittstelle, die auf bestimmte Administratoren abgestimmt sind. Produktberechtigungen bestimmen, was angezeigt wird und welche Befehle verfügbar sind.

Beispiel: Helpdeskadministratoren sehen eine auf Helpdeskaufgaben abgestimmte Schnittstelle. Director ermöglicht Helpdeskadministratoren, nach dem Benutzer zu suchen, der das Problem gemeldet hat, und die diesem Benutzer zugeordneten Aktivitäten anzuzeigen, z. B. den Status der Anwendungen und Prozesse des Benutzers. So können Probleme schnell gelöst werden, indem Aktionen wie z. B. das Beenden einer nicht reagierenden Anwendung oder eines Prozesses, das Spiegeln von Vorgängen auf der Maschine des Benutzers, der Neustart der Maschine oder das Zurücksetzen des Benutzerprofils durchgeführt werden.

Im Gegensatz dazu sehen und verwalten Volladministratoren die gesamte Website 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.

Director ist standardmäßig als Website auf dem Delivery Controller installiert. Informationen zu Voraussetzungen und anderen Details finden Sie in der Dokumentation zu den Systemanforderungen für dieses Release.

Dieses Release von Director ist nicht kompatibel mit XenApp-Bereitstellungen vor Version 6.5 und XenDesktop-Bereitstellungen vor Version 7.

Wenn Director in einer Umgebung mit mehreren Sites verwendet wird, synchronisieren Sie die Systemuhren auf allen Servern, auf denen Controller, Director und andere wichtige Kernkomponenten installiert sind. Ansonsten werden die Sites in Director möglicherweise nicht richtig angezeigt.

Tipp: Wenn Sie beabsichtigen, neben XenApp 7.5- und XenDesktop 7.x-Sites auch XenApp 6.5-Sites zu überwachen, empfiehlt Citrix, Director und die Director-Konsole, die zur Überwachung von XenApp 6.5-Sites verwendet wird, auf separaten Servern zu installieren.
Wichtig: Zum Schutz von als Nur-Text über das Netzwerk gesendeten Benutzernamen und Kennwörtern empfiehlt Citrix dringend, nur Director-Verbindungen mit HTTPS und nicht mit HTTP zuzulassen. Bestimmte Tools können Nur-Text-

Benutzernamen und -Kennwörter in (unverschlüsselten) HTTP-Netzwerkpaketen lesen, wodurch ein Sicherheitsrisiko für Benutzer entsteht.

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.
- Bei Benutzergeräten mit VDA-Versionen vor 7 ist eine zusätzliche Konfiguration erforderlich. Siehe Konfigurieren von Berechtigungen für VDAs vor XenDesktop 7.

Installieren Sie Director mit dem Produktinstallationsprogramm für XenApp und XenDesktop. Dieses prüft, ob die Voraussetzungen erfüllt sind, installiert fehlende Komponenten, richtet die Director-Website ein und führt die Grundkonfiguration durch. Die Standardkonfiguration, die der Installer bietet, eignet sich für typische Bereitstellungen. Fügen Sie Director mit dem Installationsprogramm hinzu, falls dies während der Installation nicht geschehen ist. Zum Hinzufügen zusätzlicher Komponenten führen Sie den Installer erneut aus und wählen Sie die zu installierenden Komponenten aus. Informationen zur Verwendung des Installationsprogramms finden Sie unter Installieren über die grafische Oberfläche in der Installationsdokumentation. Citrix empfiehlt, dass Sie die Installation ausschließlich mit dem 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. 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.

Führen Sie die folgenden Schritte aus, um Director für XenApp 6.5 zu installieren. In der Regel wird Director auf einem anderen Computer als die XenApp-Controller installiert.

1. Installieren Sie Director von dem XenApp 7.7-Installationsmedium. Wenn Director bereits für XenDesktop installiert ist, überspringen Sie diesen Schritt und fahren Sie mit dem nächsten Schritt fort.
2. Verwenden Sie die IIS-Verwaltungskonsole auf jedem Director-Server, um die Liste der XenApp-Serveradressen in den Anwendungseinstellungen zu aktualisieren (siehe Abschnitt "Hinzufügen von Sites zu Director" im Artikel Erweiterte Konfiguration).
   Geben Sie pro XenApp-Site die Serveradresse eines Controllers an: Die anderen Controller in einer XenApp-Site werden dann automatisch zum Failover verwendet. Director führt keinen Lastausgleich zwischen Controllern aus.

   Wichtig: Stellen Sie bei XenApp-Adressen sicher, dass Sie die Einstellung "Service.AutoDiscoveryAddressesXA" und nicht die Standardeinstellung "Service.AutoDiscoveryAddresses" verwenden.
3. Der Installer für den WMI Provider von Director ist auf der DVD im Ordner **Support\DirectorWMIProvider**. Installieren Sie ihn auf den jeweiligen XenApp-Servern (Controller und Worker, wenn Sitzungen ausgeführt werden).
   Wenn **winrm** nicht konfiguriert ist, führen Sie den Befehl **winrm qc** aus.
4. Konfigurieren Sie jeden XenApp-Workerserver für die Annahme von WinRM-Abfragen, wie unter Konfigurieren von Berechtigungen beschrieben.
5. Konfigurieren Sie eine Firewallausnahme für Port 2513, der für die Kommunikation zwischen Director und XenApp verwendet wird.
6. Citrix empfiehlt die Implementierung von TLS auf der IIS-Website, die Director hostet, um die Kommunikation zwischen dem Browser und dem Webserver zu schützen.
   In der Dokumentation von Microsoft zu IIS finden Sie entsprechende Anweisungen. Zum Aktivieren von TLS ist keine Director-Konfiguration erforderlich.

> ### Hinweis
>
> Damit Director alle XenApp-Worker in der Farm findet, müssen Sie eine Reverse-DNS-Zone für die Subnetze hinzufügen, in denen sich die XenApp-Server auf den von der Farm verwendeten DNS-Servern befinden.

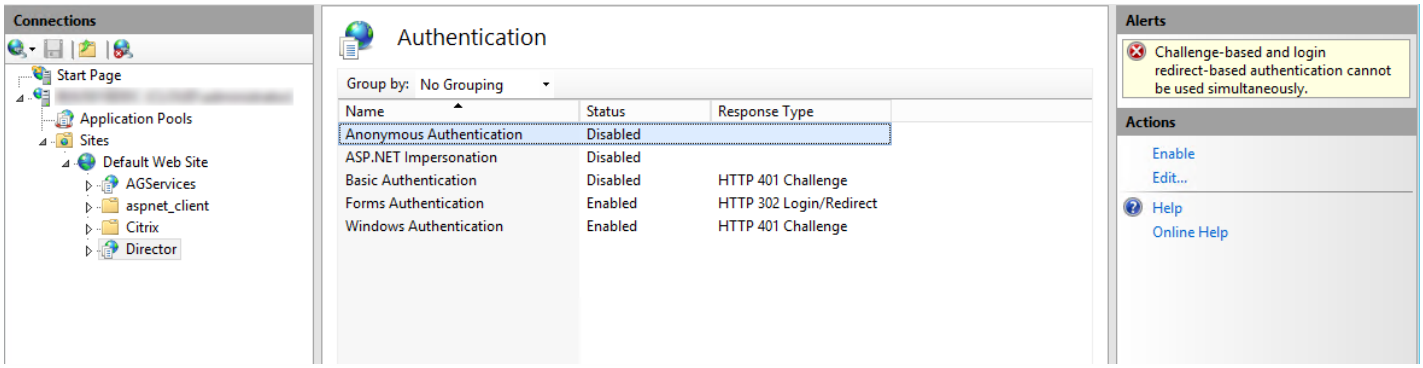
Die Director-Website ist unter https oder http:///Director.

Wenn eine der Sites einer Bereitstellung mit mehreren Sites ausfällt, dauert die Anmeldung für Director etwas länger, während Verbindungsversuche mit dieser Site laufen.

Mit der integrierten Windows-Authentifizierung erhalten in die Domäne eingebundene Benutzer direkten Zugriff auf Director, ohne ihre Anmeldeinformationen auf der Director-Anmeldeseite erneut eingeben zu müssen. Für die Verwendung der integrierten Windows-Authentifizierung mit Director gelten folgende Voraussetzungen:

- Die integrierte Windows-Authentifizierung muss auf der IIS-Website, die Director hostet, aktiviert werden. Bei der Installation von Director sind Formularauthentifizierung und anonyme Authentifizierung aktiviert. Zur Verwendung der integrierten Windows-Authentifizierung mit Director deaktivieren Sie die anonyme Authentifizierung und aktivieren Sie die Windows-Authentifizierung. Die Formularauthentifizierung sollte 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 **Aktivieren**.



- 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** und wählen Sie den Director-Computer zum Zuweisen der Delegierungsberechtigung.
  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 auf **Automatische Anmeldung** oder **Benutzeranmeldeinformationen** festlegen.

Erweiterte Konfiguration

Feb 29, 2016

Dieser Abschnitt enthält folgende Themen:

Unterstützen von Benutzern in mehreren Active Directory-Domänen und -Gesamtstrukturen

Hinzufügen von Sites zu Director

Deaktivieren der Sichtbarkeit von ausgeführten Anwendungen im Aktivitätsmanager

Einige Elemente der erweiterten Director-Konfigurationen, z. B. die Unterstützung mehrerer Sites oder mehrerer Active Directory-Gesamtstrukturen, wird durch die Einstellungen im Internetinformationsdienste-Manager (IIS) gesteuert.
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.

Platinum-Lizenzen behalten Daten standardmäßig 90 Tage lang bei. Weitere Informationen zu Konfigurationen finden Sie unter Datengranularität und -beibehaltung.

Director sucht in Active Directory nach Benutzern und nach zusätzlichen Benutzer- und Maschineninformationen. Standardmäßig durchsucht Director die folgende Domäne oder Gesamtstruktur:

- In der das Konto des Administrators Mitglied ist
- In der der Director-Webserver Mitglied ist (falls unterschiedlich)

Director versucht, Suchen auf Gesamtstrukturebene mit dem globalen Active Directory-Katalog durchzuführen Wenn der Administrator keine Berechtigungen zum Suchen auf der Gesamtstrukturebene hat, wird nur die Domäne durchsucht.

Für die Suche nach Daten aus einer anderen Active Directory-Domäne oder Gesamtstrukturebene müssen Sie explizit die zu durchsuchenden Domänen oder Gesamtstrukturen festlegen. Konfigurieren Sie die folgenden Einstellungen:
Connector.ActiveDirectory.Domains = (user),(server)
Die Werte der Attribute Benutzer und Server stellen die Domänen des Director-Benutzers (Administrator) bzw. des Director-Servers dar.

Um Suchen von einer zusätzlichen Domäne oder Gesamtstruktur zu ermöglichen, fügen Sie, wie in diesem Beispiel gezeigt, den Namen der Domäne der Liste hinzu:

Connector.ActiveDirectory.Domains = (user),(server),,
Director versucht, Suchen für jede Domäne in der Liste auf der Gesamtstrukturebene durchzuführen. Wenn der Administrator keine Berechtigungen zum Suchen auf der Gesamtstrukturebene hat, wird nur die Domäne durchsucht.

Wenn Director bereits installiert ist, richten Sie das Programm für die Arbeit mit mehreren Sites ein. Verwenden Sie hierzu die

IIS-Manager-Konsole auf jedem Director-Server zum Aktualisieren der Liste der Serveradressen in den Anwendungseinstellungen.

Fügen Sie folgender Einstellung eine Controller-Adresse von jedem Standort hinzu:
Service.AutoDiscoveryAddresses = SiteAController,SiteBController
wobei SiteAController und SiteBController die Adressen von XenDesktop-Controllern zweier verschiedener Sites sind.

Fügen Sie bei XenApp 6.5-Sites der folgenden Einstellung eine Controller-Adresse von den jeweiligen XenApp-Farmen hinzu:
Service.AutoDiscoveryAddressesXA = FarmAController,FarmBController
wobei FarmAController und FarmBController die Adressen von XenApp-Controllern von zwei verschiedenen Farmen sind.

Dies ist eine weitere Methode für XenApp 6.5-Sites, einen Controller von einer XenApp-Farm hinzuzufügen:
DirectorConfig.exe /xenapp FarmControllerName

Standardmäßig wird im Aktivitätsmanager von Director eine Liste aller ausgeführten Anwendungen für die Benutzersitzung 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 Schutz der Privatsphäre im Hinblick auf Benutzer und die von ihnen ausgeführten Anwendungen können Sie die Auflistung der ausgeführten Anwendungen auf der Registerkarte "Anwendungen" deaktivieren.

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. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.

1. Ändern Sie für den VDA den Registrierungsschlüssel in HKLM\Software\Citrix\Director\TaskManagerDataDisplayed. Standardmäßig ist dieser Schlüssel auf 1 eingestellt. Ändern Sie den Wert auf 0, was bedeutet, dass die Informationen nicht im Aktivitätsmanager angezeigt werden.
2. Bearbeiten Sie auf dem Server, auf dem Director installiert ist, die Einstellung zur Steuerung der Sichtbarkeit ausgeführter Anwendungen. In der Standardeinstellung ist der Wert "Wahr", wodurch die Sichtbarkeit der ausgeführten Anwendungen auf der Registerkarte Anwendungen zugelassen wird. Ändern Sie den Wert in "Falsch", wodurch die Sichtbarkeit deaktiviert wird. Diese Option gilt nur für den Aktivitätsmanager in Director, nicht für den VDA.
   Ändern Sie den Wert der folgenden Einstellung:
   UI.TaskManager.EnableApplications = false

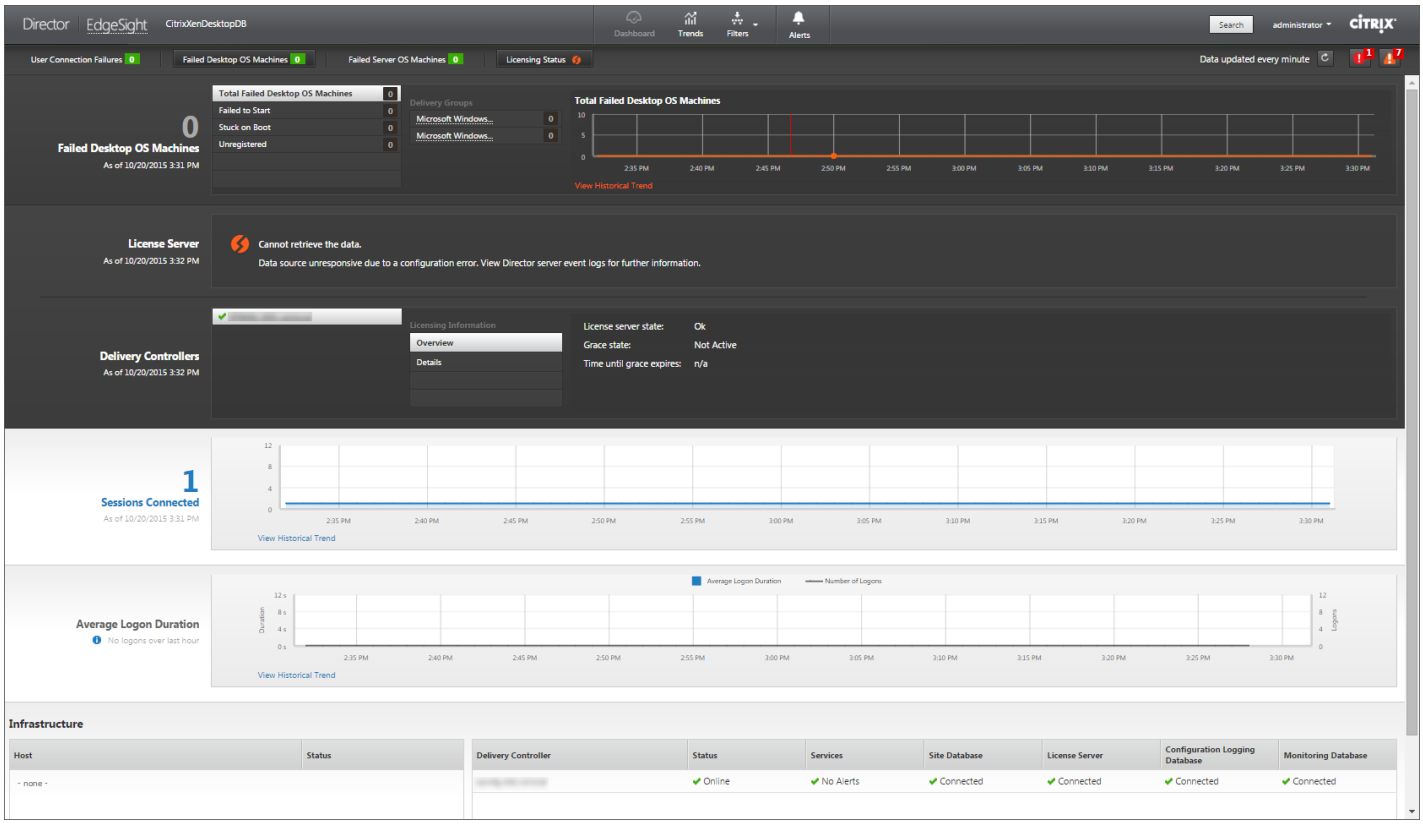
Wichtig: Zum Deaktivieren der Ansicht ausgeführter Anwendungen empfiehlt Citrix, dass beide Änderungen durchgeführt werden, damit die Daten im Aktivitätsmanager nicht angezeigt werden.

Überwachen von Bereitstellungen

Feb 29, 2016

Dieser Abschnitt enthält folgende Themen:

Wenn Sie Director mit Volladministratorrechten öffnen, erscheint das Dashboard zur Überwachung der Integrität und Nutzung einer Site.



Wenn es zurzeit keine Fehler gibt und keine Fehler in den letzten 60 Minuten aufgetreten sind, bleiben Bereiche ausgeblendet. Wenn Fehler auftreten, wird der zugehörige Fehlerbereich automatisch angezeigt.

Hinweis: Je nachdem, über welche Lizenzierung Ihre Organisation verfügt und welche Administratorrechte vorliegen, stehen einige Optionen oder Features möglicherweise nicht zur Verfügung.

Bereich	Beschreibung
Benutzerverbindungsfehler	Verbindungsfehler während der letzten 60 Minuten. Klicken Sie auf die Kategorien neben der Gesamtzahl zum Anzeigen von Metriken für diesen Fehlertyp. In der nebenstehenden Tabelle wird angezeigt, wie sich dieser Wert auf die Bereitstellungsgruppen verteilt. Verbindungsfehler umfassen auch solche, die aufgrund von Anwendungslimits auftreten. Weitere Informationen zu Anwendungslimits finden Sie unter Verwalten von Anwendungen.
Fehlgeschlagene Desktopbetriebssystemmaschinen bzw. Fehlgeschlagene Serverbetriebssystemmaschinen	Gesamtanzahl der Fehler in den letzten 60 Minuten unterteilt nach Bereitstellungsgruppen. Fehler unterteilt nach Typ, einschließlich "konnte nicht gestartet werden", "beim Starten hängen geblieben" und "nicht registriert". Bei Serverbetriebssystemmaschinen wird auch das Erreichen der maximalen Last angegeben.
Lizenzierungsstatus	• Lizenzserverwarnungen werden vom Lizenzserver gesendet und enthalten für eine Auflösung der jeweiligen Warnung erforderlichen Aktionen. • Delivery Controller-Warnungen enthalten vom Controller erfasste Zustandsangaben zur Lizenzierung und werden vom Delivery Controller gesendet. Sie können den Schwellenwert für Warnungen in Studio festlegen. Lizenzserver- bzw. Delivery Controller-Warnungen werden nicht angezeigt, wenn die Lizenzserverversion älter ist 11.12.1 bzw. wenn die Delivery Controller-Version älter ist als XenApp 7.6 oder XenDesktop 7.6.
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.
Infrastruktur	Integritätsstatus der Hosts, Controller und Infrastruktur. Anzeige von Leistungswarnungen. Für Hosts werden der Verbindungsstatus sowie der Zustand der CPU, Arbeitsspeicher, Bandbreite (Netzwerkverwendung) und Speicher (Datenträgernutzung) anhand von Informationen von XenServer oder VMware überwacht. 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

Bereich	Beschreibung
	Warnungswiederholungsintervall 60 Minuten, Sie können jedoch auch eine andere Einstellung wählen. Weitere Informationen finden Sie in der XenServer-Dokumentation unter Konfigurieren von Leistungswarnungen.

Hinweis: Wird für eine bestimmte Metrik kein Symbol angezeigt, bedeutet dies, dass diese Metrik von dem verwendeten Hosttyp nicht unterstützt wird. Beispiel: Für System Center Virtual Machine Manager-, AWS- und CloudStack-Hosts sind keine Integritätsdaten verfügbar.
Fahren Sie mit dem Beheben von Problemen mit den folgenden Optionen (Erläuterung siehe weiter unten) fort:

- Steuern der Energieverwaltung der Benutzermaschine
- Verhindern von Verbindungen mit Maschinen

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. Siehe Wiederherstellen von Sitzungen.
Anzeigen der Gesamtanzahl der verbundenen Sitzungen in allen Bereitstellungsgruppen	Im Dashboard im Bereich Verbundene Sitzungen zeigen Sie die Gesamtzahl der verbundenen Sitzungen in allen Bereitstellungsgruppen in den letzten 60 Minuten an. 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.
Anzeigen der Daten über einen längeren Zeitraum	Klicken Sie in der Ansicht Trends auf die Registerkarte Sitzungen, um detailliertere Nutzungsdaten für verbundene und getrennte Sitzungen über einen längeren Zeitraum anzuzeigen (d. h. Sitzungsgesamtanzahl, die länger als 60 Minuten zurückliegt). 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.

Wenn Sie auf Zahlen im Dashboard klicken oder im Menü Filter einen vordefinierten Filter auswählen, wird die Ansicht Filter geöffnet und zeigt Daten für die ausgewählte Maschine oder den Fehlertyp an.

Vordefinierten Filter können nicht bearbeitet werden. Sie können einen vordefinierten Filter jedoch als benutzerdefinierten Filter speichern und dann bearbeiten. Sie können auch benutzerdefinierten Ansichten mit Filter für Maschinen, Verbindungen und Sitzungen für alle Bereitstellungsgruppen erstellen.

1. Wählen Sie eine Ansicht aus:

- **Maschinen**: Wählen Sie Desktopbetriebssystemmaschinen oder Serverbetriebssystemmaschinen. Diese Ansicht zeigt die Anzahl der konfigurierten Computer. Die Registerkarte "Serverbetriebssystemmaschinen" enthält auch den Lastauswertungsprogrammindex, der die Verteilung der Leistungsindikatoren und Quickinfo der Sitzungsanzahl angibt, wenn Sie mit dem Mauszeiger auf den Link zeigen.
- **Sitzungen**: Sie können die Sitzungsanzahl auch in der Ansicht "Maschinen" anzeigen.
- **Verbindungen**: Filtern Sie Verbindungen nach verschiedenen Zeiträumen, u. a. die letzten 60 Minuten, die letzten 24 Stunden, oder die letzten 7 Tage.

2. Wählen Sie für "Fehler" die Kriterien 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.
   Wenn Sie den Filter später öffnen möchten, wählen Sie im Menü Filter den Filtertyp (Maschinen, Sitzungen oder Verbindungen) und dann den gespeicherten Filter.
6. Verwenden Sie u. U. für die Ansichten "Maschinen" oder "Verbindungen" für alle in der gefilterten Liste ausgewählten Maschinen Energiesteuerelemente aus. Verwenden Sie in der Ansicht "Sitzungen" die Sitzungssteuerelemente oder die Option zum Senden von Nachrichten.

Fahren Sie mit dem Beheben von Problemen mit den folgenden Optionen (Erläuterung siehe weiter unten) fort:

- Steuern der Energieverwaltung der Benutzermaschine
- Verhindern von Verbindungen mit Maschinen

Die Ansicht "Trends" zeigt Verlaufstrenddaten für Sitzungen, Verbindungsfehler, Maschinenfehler, Anmeldeleistung und Lastauswertung für jede Site an. Klicken Sie zur Anzeige dieser Informationen im Dashboard oder in der Anzeige "Filter" auf "Trends".

Das Vergrößerungsfeature beim Drilldown ermöglicht Ihnen das Navigieren durch Trenddiagramme, indem Sie bestimmte Zeiträume vergrößern (durch Klicken auf einen Datenpunkt im Diagramm) und die Detailinformationen zum Trend anzeigen. Durch dieses Feature können Sie die genauen Auswirkungen der angezeigten Trends besser verstehen.

Wenden Sie einen anderen Filter auf die Daten an, um den Standardgeltungsbereich der einzelnen Diagramme zu ändern.

Aktion	Beschreibung
Graphdaten exportieren	Wählen Sie die Registerkarte aus, die die Daten enthält, die Sie exportieren möchten. Klicken Sie auf "Exportieren" und wählen Sie das Format: PDF oder CVS.
Trends für Sitzungen anzeigen	Wählen Sie auf der Registerkarte "Sitzungen" die Bereitstellungsgruppe und den Zeitraum aus, um weitere Informationen zur Anzahl gleichzeitiger Sitzungen anzuzeigen.
Trends für Verbindungsfehler anzeigen	Wählen Sie auf der Registerkarte "Verbindungsfehler" den Maschinentyp, den Fehlertyp, die Bereitstellungsgruppe und den Zeitraum, um weitere Informationen über die Verbindungsfehler der Site anzuzeigen.
Trends für Maschinenfehler	Wählen Sie auf der Registerkarte "Desktopbetriebssystemmaschinenfehler" bzw. "Serverbetriebssystemmaschinen" den Fehlertyp, die Bereitstellungsgruppe und den Zeitraum,

anzeigen	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. Brokeringdauer, VM-Startzeit usw. Diese Daten beziehen sich speziell auf Benutzeranmeldungen und nicht auf Benutzer, die sich mit getrennten Sitzungen wiederverbinden.
Trends für die Lastauswertung anzeigen	Die Registerkarte "Lastauswertungsindex" bietet ein Diagramm, das ausführliche Informationen zur Last enthält, die auf die Serverbetriebssystemmaschinen verteilt ist. Als Filteroptionen für dieses Diagramm stehen Bereitstellungsgruppe oder Serverbetriebssystemmaschine in einer Bereitstellungsgruppe, Serverbetriebssystemmaschine (nur bei Auswahl von Serverbetriebssystemmaschine in einer Bereitstellungsgruppe) und Bereich zur Verfügung.
Anzeigen der Nutzung gehosteter Anwendungen	Die Verfügbarkeit dieser Funktion hängt von den Lizenzen des Unternehmens ab. Wählen Sie auf der Registerkarte "Kapazitätsverwaltung" die Registerkarte "Verwendung gehosteter Anwendungen" und dann die Bereitstellungsgruppe und den Zeitraum, um eine Kurve der höchsten gleichzeitigen Nutzung sowie eine Tabelle mit der anwendungsbasierten Verwendung anzuzeigen. In der Tabelle "Anwendungsbasierte Verwendung" können Sie eine bestimmte Anwendung auswählen, um Details und eine Liste der Benutzer anzuzeigen, die die Anwendung verwenden oder verwendet haben.
Anzeigen der Nutzung von Desktop- und Serverbetriebssystem	In der Ansicht "Trends" wird die Desktopbetriebssystemnutzung nach Site und Bereitstellungsgruppe angezeigt. Bei Auswahl von "Site" wird die Nutzung nach Bereitstellungsgruppe angezeigt. Bei Auswahl von "Bereitstellungsgruppe" wird die Nutzung nach Benutzer angezeigt. In der Ansicht "Trends" wird außerdem die Serverbetriebssystemnutzung nach Site, Bereitstellungsgruppe und Maschine angezeigt. Bei Auswahl von "Site" wird die Nutzung nach Bereitstellungsgruppe angezeigt. Bei Auswahl von "Bereitstellungsgruppe" wird die Nutzung nach Maschine und nach Benutzer angezeigt. Bei Auswahl von "Maschine" wird die Nutzung nach Benutzer angezeigt.
Nutzung virtueller Maschinen anzeigen	Wählen Sie auf der Registerkarte "Nutzung" die Option "Desktopbetriebssystemmaschinen" oder "Serverbetriebssystemmaschinen", um einen Überblick über die Nutzung der VMs in Echtzeit zu erhalten, sodass Sie den Kapazitätsbedarf der Site schnell einschätzen können. Verfügbarkeit der Desktopbetriebssysteme: Zeigt den aktuellen Zustand der Desktopbetriebssystemmaschinen (VDIs) nach Verfügbarkeit für die gesamte Site oder für bestimmte Bereitstellungsgruppen an. Verfügbarkeit der Serverbetriebssysteme: Zeigt den aktuellen Zustand der Serverbetriebssystemmaschinen nach Verfügbarkeit für die gesamte Site oder für bestimmte Bereitstellungsgruppen an.

Netzwerkanalysedaten mit HDX Insight anzeigen	Die Verfügbarkeit dieser Funktion richtet sich nach der Lizenzierung der Organisation und den Administratorberechtigungen. Überwachen Sie auf der Registerkarte "Netzwerk" die Netzwerkanalyse, die eine kontextbezogene Ansicht der Benutzer, Anwendungen und Desktops im Netzwerk bereitstellt. Director bietet mit diesem Feature eine erweiterte Analyse des ICA-Datenverkehrs in der Bereitstellung.

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.

Fahren Sie mit dem Beheben von Problemen mit den folgenden Optionen (Erläuterung siehe weiter unten) fort:

- Steuern der Energieverwaltung der Benutzermaschine
- Verhindern von Verbindungen mit Maschinen

Zum Anzeigen der auf einem bestimmten Maschinen-VDA (physisch oder VM) installierten Hotfixes wählen Sie die Ansicht Maschinendetails.

Steuern Sie den Zustand der in Director ausgewählten Maschinen mit den Optionen für die Energieverwaltung. Diese Optionen stehen für Desktopbetriebssystemmaschinen, aber möglicherweise nicht für Serverbetriebssystemmaschinen zur Verfügung.

Hinweis: Diese Funktionen stehen nicht für physische Maschinen zur Verfügung, die Remote-PC-Zugriff verwenden.

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.
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 erneutes Anschließen und Einschalten des Servers.
Herunterfahren	Die VM wird ordnungsgemäß heruntergefahren und alle ausgeführten Prozesse werden einzeln angehalten.
Herunterfahren erzwingen	Die VM wird zwingend heruntergefahren, ohne dass das Verfahren zum Herunterfahren durchgeführt wird. Dieser Befehl funktioniert genauso wie das Trennen des Netzsteckers eines physischen Servers. Es werden möglicherweise nicht immer alle ausgeführten Prozesse

Befehl	Funktion
	heruntergefahren, sodass bei diesem Verfahren die Gefahr von Datenverlust besteht.
Suspend	Die laufende VM wird im aktuellen Zustand angehalten und dieser Zustand wird in einer Datei im Standardspeicherrepository gespeichert. Diese Option ermöglicht das Herunterfahren der VM auf dem Hostserver und später, nach einem Neustart, die Wiederaufnahme der VM mit dem ursprünglichen Ausführungsstatus.
Fortfahren	Nimmt eine angehaltene VM wieder auf und stellt den ursprünglichen Ausführungsstatus wieder her.
Starten	Startet eine ausgeschaltete VM.

Sollten die Energieverwaltungsaktionen fehlschlagen, zeigen Sie mit der Maus auf die Warnung und es wird eine Meldung mit Details zum Fehler angezeigt.

Verwenden Sie den Wartungsmodus, um vorübergehend neue Verbindungen zu verhindern, während der entsprechende Administrator Wartungsaufgaben am Image durchführt.

Wenn Sie den Wartungsmodus auf Maschinen aktivieren, werden keine neuen Verbindungen zugelassen, bis Sie ihn wieder deaktivieren. Wenn Benutzer momentan angemeldet sind, wird der Wartungsmodus erst wirksam, sobald alle Benutzer abgemeldet sind. Benutzern, die sich nicht abmelden, müssen Sie eine Nachricht senden, die sie darüber informiert, dass die Maschine zu einem bestimmten Zeitpunkt heruntergefahren wird. Verwenden Sie die Energieverwaltung, um die Maschinen zwingend herunterzufahren.

1. Wählen Sie die Maschine aus, z. B. auf der Ansicht Benutzerdetails, oder eine Gruppe von Maschinen in der Ansicht Filter.
2. Klicken Sie auf Wartungsmodus und aktivieren Sie die Option.

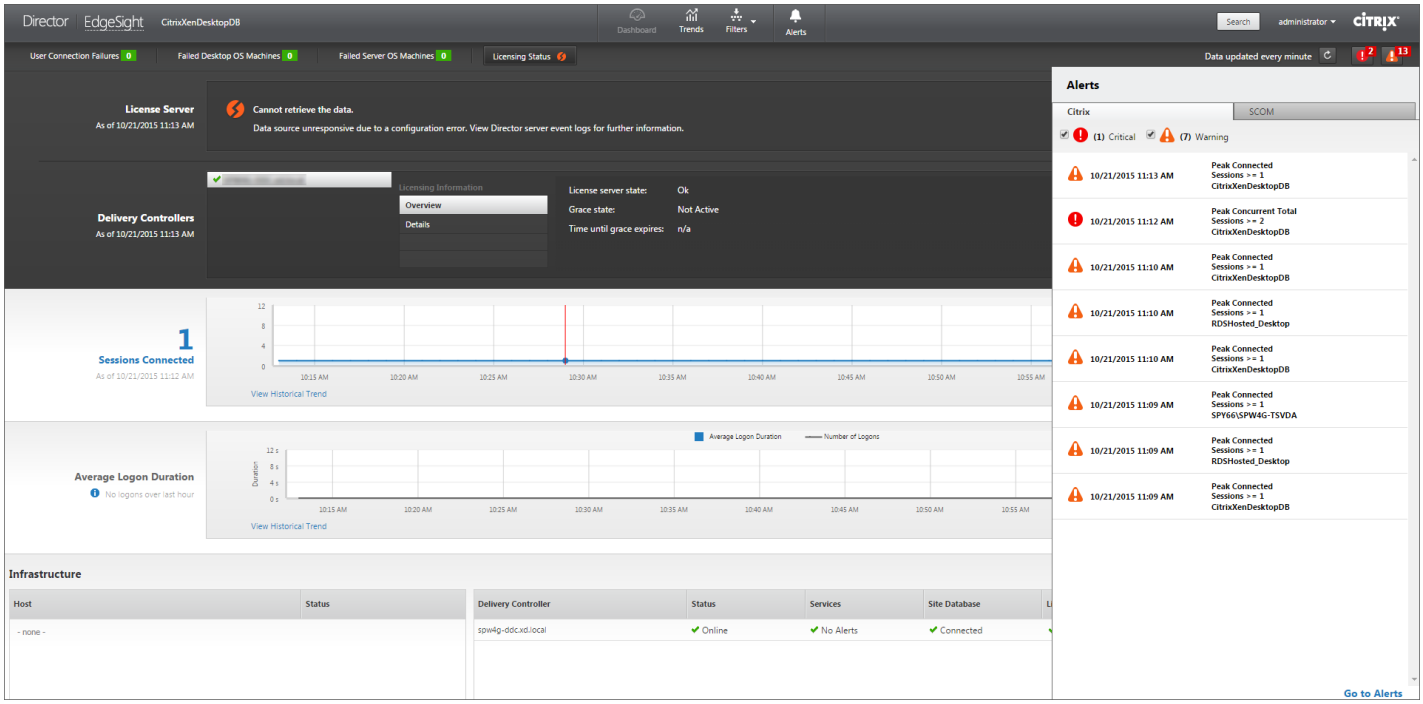
Wenn ein Benutzer versucht, eine Verbindung zu einem zugewiesenen Desktop herzustellen, während er im Wartungsmodus ist, wird eine Meldung angezeigt, dass der Desktop zurzeit nicht verfügbar ist. Es können keine neuen Verbindungen hergestellt werden, bis der Wartungsmodus deaktiviert wird.

Warnungen und Benachrichtigungen

Jul 22, 2016

Dieser Abschnitt enthält folgende Themen:

In Director werden im Dashboard und in anderen Ansichten der oberen Ebene Warnungen und kritische Warnungen mit entsprechenden Symbolen angezeigt. Die Anzeige von Warnungen wird jede Minute automatisch aktualisiert und kann bei Bedarf auch manuell aktualisiert werden.

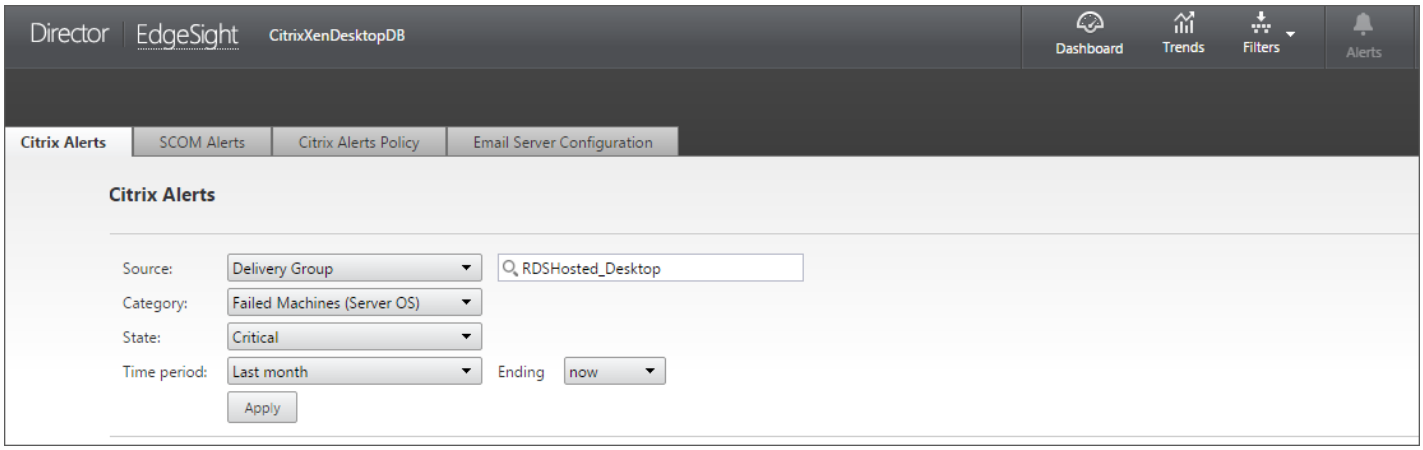


Eine Warnung (gelbes Dreieck) zeigt an, dass der minimale Schwellenwert einer Bedingung erreicht wurde.

Eine kritische Warnung (roter Kreis) zeigt an, dass der maximale Schwellenwert einer Bedingung überschritten wurde.

Detaillierte Informationen zu Warnungen können Sie aufrufen, indem Sie eine Warnung auf der Randleiste auswählen, auf den Link **Warnmeldungen** unten auf der Randleiste klicken oder oben auf der Director-Seite **Warnungen** wählen.

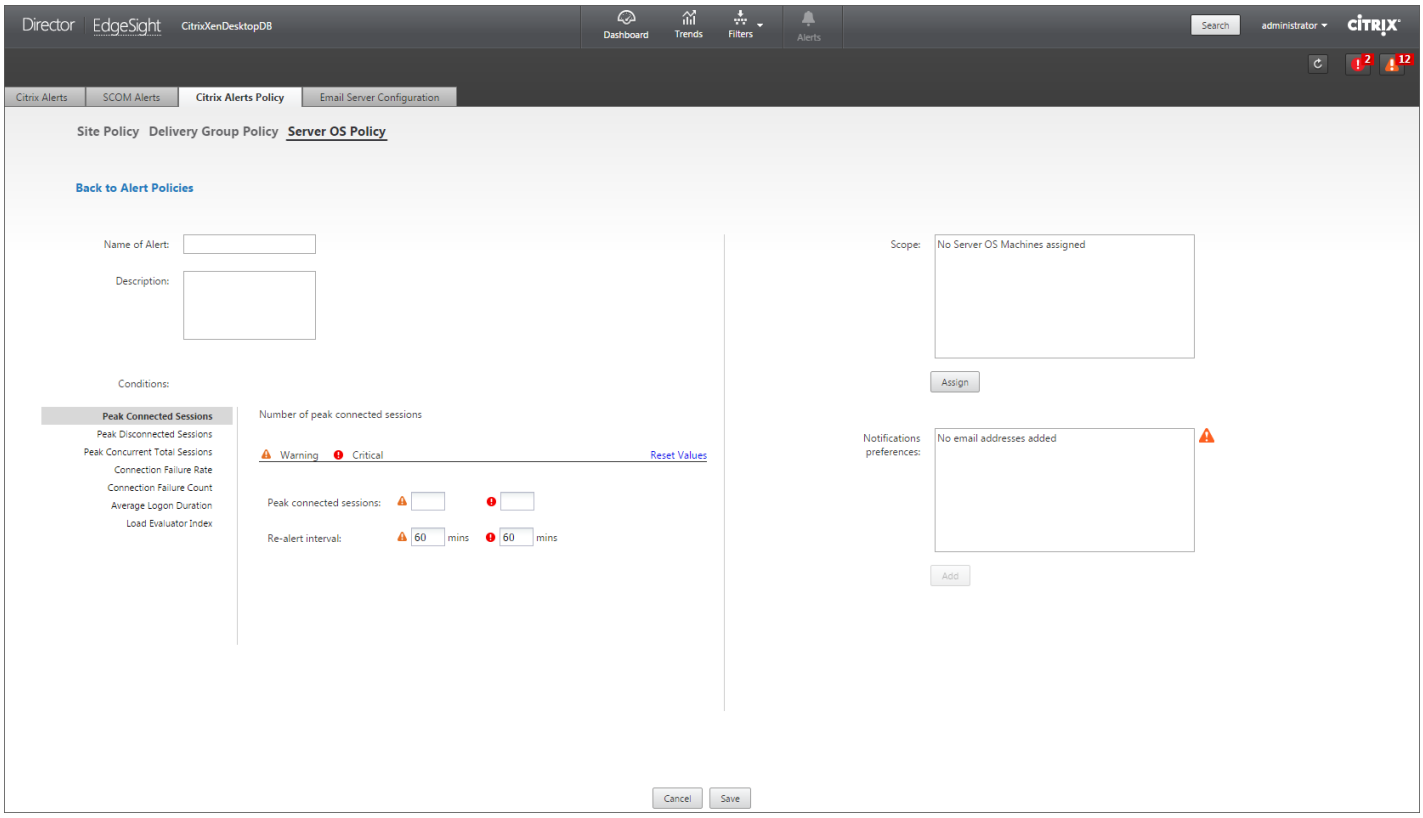
In der Ansicht "Warnungen" können Sie Warnungen filtern und exportieren. Beispielsweise können Sie fehlerhafte Serverbetriebssystemmaschinen für eine bestimmte Bereitstellungsgruppe im vergangenen Monat anzeigen.



Citrix Warnungen: Citrix Warnungen in Director stammen von Citrix Komponenten. Sie Citrix Warnungen in Director über **Warnungen** > **Citrix Warnungen** konfigurieren. Im Rahmen der Konfiguration können Sie den Versand von Benachrichtigungen per E-Mail an Personen und Gruppen festlegen, wenn die Schwellenwerte erreicht bzw. überschritten werden. Weitere Informationen zum Einrichten von Citrix Warnungen finden Sie unter Erstellen von Warnungsrichtlinien.

SCOM-Warnungen: Warnungen von Microsoft System Center 2012 Operations Manager (SCOM) enthalten detaillierte Angaben zu Datencenterintegrität und Leistung in Director. Weitere Informationen finden Sie unter "SCOM-Warnungen" und "Konfigurieren der SCOM-Integration".

Die neben den Warnsymbolen vor dem Erweitern der Randleiste angezeigte Zahl entspricht der Summe der Citrix und SCOM-Warnungen.



Gehen Sie zum Erstellen einer Warnungsrichtlinie, z. B. zum Generieren einer Warnung bei Eintreten bestimmter Sitzungszahlbedingungen, folgendermaßen vor:

1. Navigieren Sie zu **Warnungen** > **Citrix Warnmeldungsrichtlinie** und wählen Sie beispielsweise "Serverbetriebssystemrichtlinie".
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 Warnungsrichtlinien".
4. Legen Sie das Warnmeldungsintervall fest. Wenn die Bedingungen für die Warnung weiterhin erfüllt sind, wird die Warnung nach diesem Zeitintervall erneut ausgelöst und es wird, sofern dies in der Warnungsrichtlinie 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 Warnungsrichtlinien 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 der Abschluss der Konfiguration ca. eine halbe Minute dauern. Während dieses Zeitraums wird ein Drehfeld angezeigt.

Bedingung der Warnungsrichtlinie	Beschreibung und empfohlene Aktionen
Max. verbundener Sitzungen	Maximalzahl verbundener Sitzungen Empfohlene Aktionen: • Prüfen Sie die Maximalzahl verbundener Sitzungen in der Trendansicht von Director. • Vergewissern Sie sich, dass genügend Kapazität für die Sitzungslast verfügbar ist. • Fügen Sie neue Maschinen hinzu, falls erforderlich.
Max. getrennter Sitzungen	Maximalzahl getrennter Sitzungen Empfohlene Aktionen: • Prüfen Sie die Maximalzahl getrennter Sitzungen in der Trendansicht von Director. • Vergewissern Sie sich, dass genügend Kapazität für die Sitzungslast verfügbar ist. • Fügen Sie neue Maschinen hinzu, falls erforderlich.

	• Melden Sie getrennte Sitzungen ab, falls erforderlich.
Max. gleichzeitiger Sitzungen insgesamt	Maximalzahl gleichzeitiger Sitzungen Empfohlene Aktionen: • Prüfen Sie die Maximalzahl getrennter Sitzungen in der Trendansicht von Director. • Vergewissern Sie sich, dass genügend Kapazität für die Sitzungslast verfügbar ist. • Fügen Sie neue Maschinen hinzu, falls erforderlich. • Melden Sie getrennte Sitzungen ab, falls erforderlich.
Verbindungsfehlerrate	Verbindungsfehler während der letzten Stunde in Prozent. Verhältnis der Summe aller Fehler zur Summe aller Verbindungsversuche. • Überprüfen in Director die Ansicht "Fehlertrends" auf Ereignisse aus dem Konfigurationsprotokoll. • Prüfen Sie, ob Anwendungen bzw. Desktops erreichbar sind.
Anzahl Verbindungsfehler	Zahl der Verbindungsfehler während der letzten Stunde Empfohlene Aktionen: • Überprüfen in Director die Ansicht "Fehlertrends" auf Ereignisse aus dem Konfigurationsprotokoll. • Prüfen Sie, ob Anwendungen bzw. Desktops erreichbar sind.
Fehlerhafte Maschinen (Desktop-OS)	Zahl fehlerhafter Desktopbetriebssystemmaschinen Empfohlene Aktionen: • Fehler können aus verschiedenen Gründen auftreten und werden entsprechend im Dashboard von Director oder in gefilterten Ansichten angezeigt. Führen Sie eine Ursachendiagnose mit Citrix Scout durch. Weitere Informationen finden Sie unter "Behandeln von Benutzerproblemen".
Fehlerhafte Maschinen (Server-OS)	Zahl fehlerhafter Serverbetriebssystemmaschinen Empfohlene Aktionen: • Fehler können aus verschiedenen Gründen auftreten und werden entsprechend im Dashboard von Director oder in gefilterten Ansichten angezeigt. Führen Sie eine Ursachendiagnose mit Citrix Scout durch.

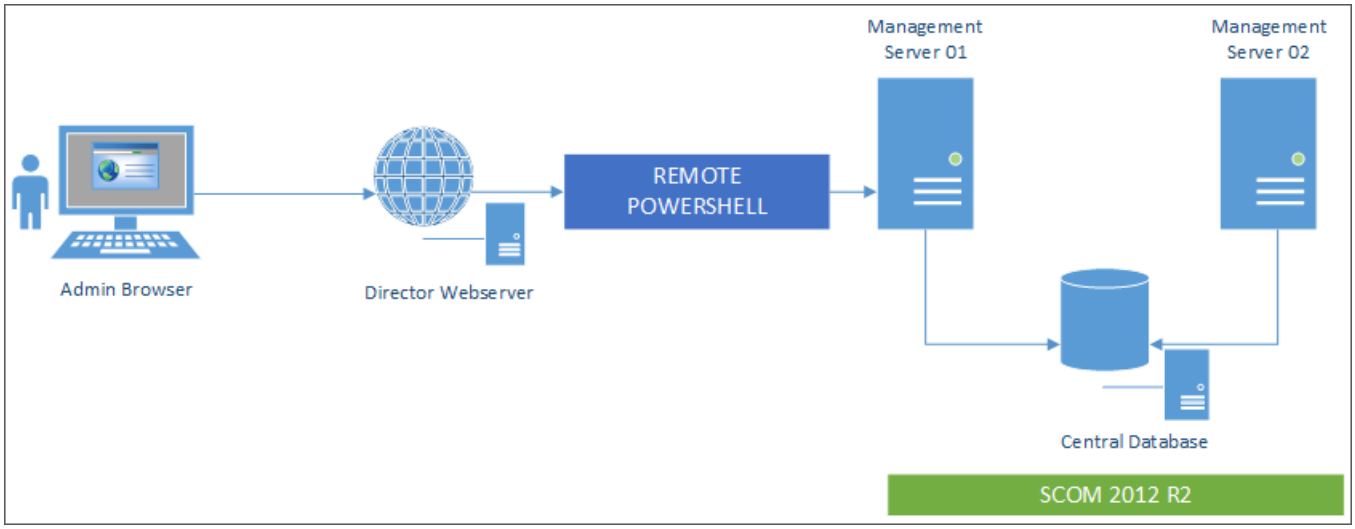
Durchschnittliche Anmeldedauer	Durchschnittliche Dauer der Anmeldungen in der letzten Stunde. Empfohlene Aktionen: • Überprüfen Sie die aktuellen Daten zur Anmeldedauer im Dashboard von Director. Melden sich viele Benutzer innerhalb kurzer Zeit an, kann die Anmeldung länger dauern. • Überprüfen Sie Baseline und Aufschlüsselung der Anmeldungen zur Ursachenfindung.
Lastauswertungsprogrammindex	Wert des Lastauswertungsprogrammindex der letzten 5 Minuten. Empfohlene Aktionen: • Prüfen Sie in Director auf Serverbetriebssystemmaschinen, die mit Spitzenlast ausgeführt werden. • Zeigen Sie das Dashboard (Fehler) und die Trendansicht für den Lastauswertungsprogrammindex an.

Wird Microsoft System Center 2012 Operations Manager in Director integriert, können Warnungen von SCOM im Dashboard und in anderen Ansichten der obersten Ebene in Director angezeigt werden.

SCOM-Warnungen werden parallel mit Citrix Warnungen angezeigt. Sie können auf SCOM-Warnungen über die SCOM-Registerkarte auf der Randleiste zugreifen und Details anzeigen.

Sie können Warnungen eines Alters von bis zu einem Monat anzeigen, sortieren und filtern und die gefilterten Informationen in CSV-, Excel- und PDF-Berichte exportieren.

Bei einer SCOM-Integration werden Daten mit Remote-PowerShell 3.0 oder höher beim SCOM-Verwaltungsserver abgefragt und es besteht eine beständige Runspace-Verbindung in der Director-Sitzung des Benutzers. Director und der SCOM-Server müssen über dieselbe PowerShell-Version verfügen.



Anforderungen für die SCOM-Integration:

- Windows Server 2012 R2
- System Center 2012 R2 Operations Manager
- PowerShell 3.0 oder höher (PowerShell-Versionen in Director und auf dem SCOM-Server müssen übereinstimmen)
- Quad-Core-CPU mit 16 GB RAM (empfohlen)
- Ein primärer Verwaltungsserver für SCOM muss in der web.config-Datei von Director konfiguriert werden. Dafür können Sie das Tool DirectorConfig verwenden.
- Citrix empfiehlt die Konfiguration des Director-Administratorkontos mit der SCOM-Rolle "Operator", damit die vollständigen Warnungsinformationen in Director abgerufen werden können. Ist das nicht möglich, kann mit dem DirectorConfig-Tool ein SCOM-Administratorkonto in der Datei web.config konfiguriert werden. Dies wird jedoch nicht empfohlen.
- Citrix empfiehlt, nicht mehr als 10 Director-Administratoren pro SCOM-Verwaltungsserver zu konfigurieren. Auf diese Weise wird der SCOM-Verwaltungsserver zur Gewährleistung der optimalen Leistung nur mäßig belastet.

Auf dem Director-Server

1. Geben Sie auf dem Director-Server **Enable-PSRemoting** ein, um das PowerShell-Remoting zu aktivieren.

2. Fügen Sie den SCOM-Verwaltungsserver der Liste "TrustedHosts" hinzu. Öffnen Sie eine PowerShell-Eingabeaufforderung mit erhöhten Rechten und führen Sie die folgenden Befehle aus:

a. Abrufen der aktuellen TrustedHosts-Liste

```
Get-Item WSMAN:\localhost\Client\TrustedHosts
```

b. Hinzufügen des FQDN des SCOM-Verwaltungsservers zur TrustedHosts-Liste. steht für die von dem Cmdlet "Get-Item" zurückgegebenen vorhandenen Einträge.

```
Set-Item WSMAN:\localhost\Client\TrustedHosts -Value "<FQDN SCOM Management Server>,<Old Values>"
```

Konfigurieren von SCOM mit dem Tool DirectorConfig

```
C:\inetpub\wwwroot\Director\tools\DirectorConfig.exe /configscom
```

Auf dem SCOM-Verwaltungsserver

1. Weisen Sie einer SCOM-Administratorrolle Director-Administratoren zu.

    a. Öffnen Sie die SCOM-Verwaltungskonsole und navigieren Sie zu **Verwaltung** > **Sicherheit** > **Benutzerrollen**.

    b. Unter "Benutzerrollen" können Sie Benutzerrollen erstellen und bearbeiten. Es gibt vier Kategorien von SCOM-Operatoren. Über diese Rollen wird die Art des Zugriffs auf SCOM-Daten festgelegt. Ein Operator der Kategorie "Schreibgeschützt" kann beispielsweise den Verwaltungsbereich nicht sehen und keine Regeln, Maschinen und Konten erkennen oder verwalten. Eine SCOM-Operatorrolle entspricht einer vollständigen Administratorrolle.

    Hinweis:

    Ist einem Director-Administrator eine andere Rolle als "Operator" zugewiesen, kann er die nachfolgend aufgeführten Arbeitsschritte nicht ausführen.

        i. Sind mehrere Verwaltungsserver konfiguriert und füllt der primäre Server aus, kann der Director-Administrator keine Verbindung mit dem sekundären Verwaltungsserver herstellen.
        Der primäre Verwaltungsserver ist der in der Director-Datei web.config konfigurierte Server und mit dem oben in Schritt 3 im DirectorConfig-Tool angegebenen identisch. Die sekundären Verwaltungsserver stehen mit dem primären Verwaltungsserver in einer Peerbeziehung.

        ii. Beim Filtern von Warnungen kann der Director-Administrator die Warnungsquelle nicht suchen. Dies erfordert Operator-Berechtigung.

    c. Zum Ändern einer Benutzerrolle klicken Sie mit der rechten Maustaste auf die Rolle und dann auf "Eigenschaften".

    d. In dem Dialogfeld mit den Benutzerrolleneigenschaften können Sie Director-Administratoren zu der angegebenen Benutzerrolle hinzufügen oder aus dieser entfernen.

2. Fügen Sie der Benutzergruppe "Remoteverwaltung" auf dem SCOM-Verwaltungsserver Director-Administratoren hinzu. Dadurch können Director-Administratoren eine Remote-PowerShell-Verbindung herstellen.

3. Geben Sie **Enable-PSRemoting** ein, um PowerShell-Remoting zu aktivieren.

4. Legen Sie die Limits für die Eigenschaften der WS-Verwaltung fest:

a. Ändern von MaxConcurrentUsers:

Befehlszeilenschnittstelle (CLI):

```
winrm set winrm/config/winrs @{MaxConcurrentUsers = "20"}
```

PS:

```
Set-Item WSMan:\localhost\Shell\MaxConcurrentUsers 20
```

b. Ändern von MaxShellsPerUser:

Befehlszeilenschnittstelle (CLI):

```
winrm set winrm/config/winrs @{MaxShellsPerUser="20"}
```

PS:

```
Set-Item WSMan:\localhost\Shell\MaxShellsPerUser 20
```

c. Ändern von MaxMemoryPerShellMB:

Befehlszeilenschnittstelle (CLI):

```
```

```
winrm set winrm/config/winrs @{MaxMemoryPerShellMB="1024"}
```

PS:

```
Set-Item WSMan:\localhost\Shell\MaxMemoryPerShellMB 1024
```

5. Um sicherzustellen, dass die SCOM-Integration in Umgebungen mit gemischten Domänen funktioniert, legen Sie folgenden Registrierungseintrag fest:

Pfad: HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

Schlüssel: LocalAccountTokenFilterPolicy

Typ: DWord

Wert: 1

> ## 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. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.

Nach dem Einrichten der SCOM-Integration wird möglicherweise die Meldung "Die aktuellen SCOM-Warnmeldungen können nicht abgerufen werden" angezeigt. Suchen Sie in den Director-Serverereignisprotokollen weitere Informationen. Anhand der Informationen in den Serverereignisprotokollen können Sie das Problem identifizieren und beheben. Mögliche Ursachen:

- Unterbrechung der Netzwerkverbindung am Computer mit Director oder SCOM
- SCOM-Dienst nicht verfügbar oder überlastet
- Keine Autorisierung aufgrund einer Änderung an den Berechtigungen des Benutzers
- Fehler in Director beim Verarbeiten der SCOM-Daten
- Nicht übereinstimmende PowerShell-Version zwischen Director und SCOM-Server.

Delegierte Administration und Director

Feb 29, 2016

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 unter Delegierte Administration.

Durch die administrativen Berechtigungen wird festgelegt, wie die Director-Benutzeroberfläche für Administratoren dargestellt wird und welche Aufgaben sie ausführen können. Mit Berechtigungen wird Folgendes festgelegt:

- Die Seiten, auf die der Administrator zugreifen kann, kollektiv als "Ansicht" bezeichnet
- Die Desktops, Maschinen und Sitzungen, die der Administrator anzeigen und verwenden kann
- Die Befehle, die der Administrator ausführen kann, z. B. das Spiegeln einer Benutzersitzung oder das Aktivieren des Wartungsmodus

Über die integrierten Rollen und Berechtigungen wird außerdem gesteuert, wie Administratoren Director verwenden:

Administratorrolle	Berechtigungen in Director
Volladministrator	Hat vollständigen Zugriff auf alle Ansichten und kann alle Befehle ausführen, einschließlich Spiegeln einer Benutzersitzung, Aktivieren des Wartungsmodus und Exportieren von Trenddaten.
Bereitstellungsgruppenadministrator	Hat vollständigen Zugriff auf alle Ansichten und kann alle Befehle ausführen, einschließlich Spiegeln einer Benutzersitzung, Aktivieren des Wartungsmodus und Exportieren von Trenddaten.
Lesezugriffadministrator	Kann auf alle Ansichten zugreifen und alle Objekte in angegebenen Geltungsbereichen sowie globale Informationen anzeigen. Kann Berichte aus HDX-Kanälen herunterladen und Trenddaten mit der Exportoption in der Ansicht "Trends" exportieren. Kann keine anderen Befehle ausführen oder Daten in den Ansichten ändern.
Helpdeskadministrator	Kann nur auf die Ansichten "Helpdesk" und "Benutzerdetails" zugreifen und nur Objekte anzeigen, die dem Administrator zur Verwaltung übertragen wurden. Kann eine Benutzersitzung spiegeln und Befehle für diesen Benutzer ausführen. Kann Vorgänge im Wartungsmodus ausführen. Kann Energieoptionen auf Desktopbetriebssystemmaschinen verwenden. Kann nicht auf das Dashboard, Trends, Warnungen oder Filteransichten zugreifen. Kann keine Energieoptionen auf Serverbetriebssystemmaschinen verwenden.
Maschinenkatalogadministrator	Kein Zugriff. Dieser Administrator wird für Director nicht unterstützt und er kann keine Daten anzeigen. Dieser Benutzer kann auf die Seite "Maschinendetails" zugreifen (maschinenbasierte Suche).

Administratorrolle	Berechtigungen in Director
Hostadministrator	Kein Zugriff. Dieser Administrator wird für Director nicht unterstützt und er kann keine Daten anzeigen.

Konfigurieren von benutzerdefinierten Rollen für Director-Administratoren

In Studio können Sie auch Director-spezifische benutzerdefinierte Rollen konfigurieren, die den Anforderungen Ihrer Organisation besser gerecht werden und eine flexiblere Delegierung von Berechtigungen ermöglichen. Sie können beispielsweise die integrierte Helpdeskadministratorrolle einschränken, sodass dieser Administrator keine Sitzungen abmelden kann.

Wenn Sie eine benutzerdefinierte Rolle mit Director-Berechtigungen erstellen, müssen Sie dieser auch andere allgemeine Berechtigungen erteilen:

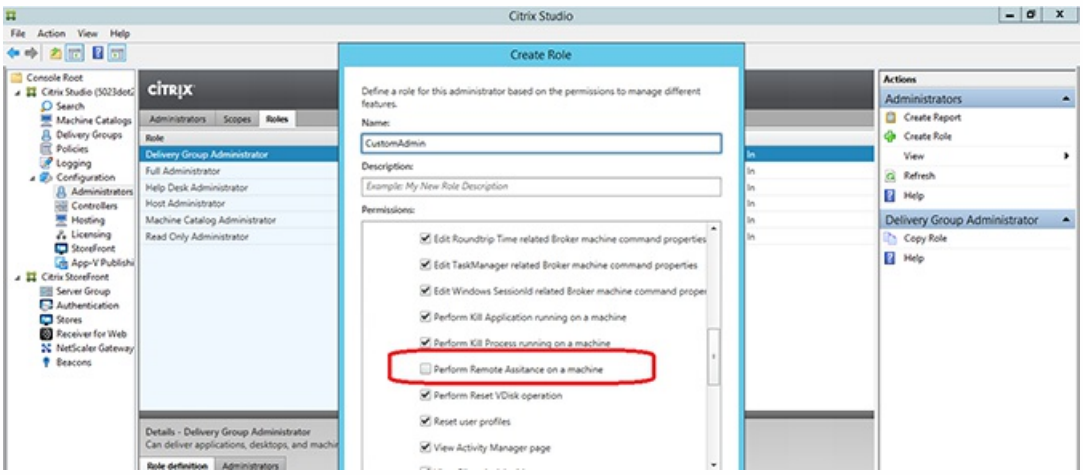
- Delivery Controller-Berechtigung zur Anmeldung bei Director.
- Berechtigungen für Bereitstellungsgruppen zum Anzeigen der zu diesen gehörigen Daten in Director.

Alternativ können Sie eine benutzerdefinierte Rolle erstellen, indem Sie eine vorhandene Rolle kopieren und dieser zusätzliche Berechtigungen für die verschiedenen Ansichten erteilen. Sie können beispielsweise die Rolle "Helpdesk" kopieren und Berechtigungen zum Anzeigen des Dashboards oder der Seiten "Filter" hinzufügen.

Wählen Sie die Director-Berechtigungen für die benutzerdefinierte Rolle, die Folgendes enthält:

- Abbrechen von auf Maschine ausgeführter Anwendung erzwingen
- Abbrechen von auf Maschine ausgeführtem Prozess erzwingen
- Remoteunterstützung für Maschine ausführen
- Vorgang zum Zurücksetzen von vDisk ausführen
- Benutzerprofile zurücksetzen
- Anzeigen der Seite "Clientdetails"
- Anzeigen der Seite "Dashboard"
- Anzeigen der Seite "Filter"
- Anzeigen der Seite "Maschinendetails"
- Anzeigen der Seite "Trends"
- Anzeigen der Seite "Benutzerdetails"

In diesem Beispiel ist das Spiegeln (Remoteunterstützung für Maschine ausführen) deaktiviert.



Aus der Liste der Berechtigungen für andere Komponenten sollten Sie zusätzlich folgende Berechtigungen berücksichtigen:

- Bereitstellungsgruppen:
  - 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

Konfigurieren von Berechtigungen für VDAs vor XenDesktop 7

Feb 29, 2016

Wenn Benutzer auf ihren Geräten VDAs einer Version vor XenDesktop 7 installiert haben, ergänzt Director Informationen aus der Bereitstellung durch Echtzeitstatus und -metrik über Windows-Remoteverwaltung (WinRM).

Darüber hinaus können Sie mit dem hier beschriebenen Verfahren WinRM für die Verwendung mit Remote PC in XenDesktop 5.6 Feature Pack1 konfigurieren.

Standardmäßig verfügen nur lokale Administratoren des Desktopcomputers (in der Regel Domänenadministratoren und andere privilegierte Benutzer) über die Berechtigungen, die zum Anzeigen der Echtzeitdaten erforderlich sind.

Informationen zum Installieren und Konfigurieren von WinRM finden Sie unter CTX125243.

Um anderen Benutzern das Anzeigen von Echtzeitdaten zu ermöglichen, müssen Sie diesen Berechtigungen erteilen. Beispiel: Angenommen, es gibt mehrere Director-Benutzer (HelpDeskUserA, HelpDeskUserB usw.), die zu einer Active Directory-Sicherheitsgruppe namens "HelpDeskUsers" gehören. Der Gruppe wurde in Studio die Helpdeskadministratorrolle mit den erforderlichen Delivery Controller-Berechtigungen zugewiesen. Die Gruppe benötigt jedoch auch Zugriff auf Informationen vom Desktopcomputer.

Sie haben zwei Möglichkeiten, die Berechtigungen für den erforderlichen Zugriff zu konfigurieren:

- Erteilen von Berechtigungen für die Director-Benutzer (Identitätswechselmodell)
- Erteilen von Berechtigungen für den Director-Dienst (Modell mit vertrauenswürdigem Subsystem)

Erteilen von Berechtigungen für die Director-Benutzer (Identitätswechselmodell)

Director verwendet standardmäßig ein Identitätswechselmodell: Die WinRM-Verbindung mit der Desktopmaschine wird mit der Identität des Director-Benutzers hergestellt. Aus diesem Grund muss der Benutzer über die erforderlichen Berechtigungen auf dem Desktop verfügen.

Sie können diese Berechtigungen mit einer der folgenden beiden Methoden konfigurieren (nachfolgend beschrieben):

1. Hinzufügen von Benutzern zur lokalen Administratorgruppe auf der Desktopmaschine.
2. Erteilen der von Director benötigten spezifischen Berechtigungen für Benutzer. Bei dieser Option wird vermieden, dass Director-Benutzer (beispielsweise die HelpDeskUsers-Gruppe) Volladministratorrechte auf der Maschine erhalten.

Erteilen von Berechtigungen für den Director-Dienst (Modell mit vertrauenswürdigem Subsystem)

Anstatt den Director-Benutzern Berechtigungen für die Desktopmaschinen zu erteilen, können Sie Director so konfigurieren, dass WinRM-Verbindungen mit einer Dienstidentität hergestellt werden, und ausschließlich dieser Dienstidentität die entsprechenden Berechtigungen erteilen.

Bei diesem Modell sind die Benutzer von Director nicht berechtigt, selbst WinRM-Aufrufe zu tätigen. Sie können nur mit Director auf die Daten zugreifen.

Der Director-Anwendungspool in IIS ist für die Ausführung als Dienstidentität konfiguriert. Dies ist standardmäßig das virtuelle Konto "APPPOOL\Director". Beim Herstellen von Remoteverbindungen wird dieses Konto als das Active Directory-Computerkonto des Servers angezeigt, z. B. MyDomain\DirectorServer$. Sie müssen dieses Konto mit den entsprechenden

Berechtigungen konfigurieren.

Wenn mehrere Director-Websites bereitgestellt werden, müssen Sie das Computerkonto jedes Webservers in eine Active Directory-Sicherheitsgruppe setzen, die entsprechende Berechtigungen hat.

Um Director so einzustellen, dass anstelle der Benutzeridentität die Dienstidentität für WinRM verwendet wird, konfigurieren Sie die folgende Einstellung, wie unter Erweiterte Konfiguration beschrieben:

Service.Connector.WinRM.Identity = Service
Sie haben zwei Möglichkeiten, diese Berechtigungen zu konfigurieren:

1. Hinzufügen des Dienstkontos zur lokalen Administratorgruppe auf der Desktopmaschine.
2. Erteilen Sie dem Dienstkonto die für Director erforderlichen Berechtigungen (siehe weiter unten). So kann eine Erteilung von Volladministratorrechten für das Dienstkonto auf der Maschine vermieden werden.

Zuweisen von Berechtigungen für einen bestimmten Benutzer oder eine bestimmte Gruppe

Die folgenden Berechtigungen sind erforderlich, damit Director auf die von der Desktopmaschine benötigten Informationen über WinRM zugreifen kann:

- Lese- und Ausführberechtigungen in WinRM RootSDDL
- WMI-Namespace-Berechtigungen:
  - root/cimv2 – Remotezugriff
  - root/citrix – Remotezugriff
  - root/RSOP – Remotezugriff und Ausführen
- Zugehörigkeit zu diesen lokalen Gruppen:
  - Systemmonitorbenutzer
  - Ereignisprotokollleser

Das ConfigRemoteMgmt.exe-Tool, das zum automatischen Erteilen dieser Berechtigungen verwendet wird, befindet sich auf dem Installationsmedium in den Ordnern x86\Virtual Desktop Agent und x64\Virtual Desktop Agent und auf dem Installationsmedium im Ordner "tools". Sie müssen allen Director-Benutzern Berechtigungen erteilen.

Um einer Active Directory-Sicherheitsgruppe, einem Benutzer oder einem Computerkonto Berechtigungen zu erteilen, oder um Aktionen auszuführen wie "Anwendung beenden und "Prozess beenden", führen Sie das Tool mit Administratorrechten an einer Eingabeaufforderung mit den folgenden Argumenten aus:

ConfigRemoteMgmt.exe /configwinrmuser domain\name
wobei name eine Sicherheitsgruppe, ein Benutzer oder ein Computerkonto ist.

Erteilen der erforderlichen Berechtigungen für eine Benutzersicherheitsgruppe:

ConfigRemoteMgmt.exe /configwinrmuser domain\HelpDeskUsers
Erteilen von Berechtigungen für ein bestimmtes Computerkonto:

ConfigRemoteMgmt.exe /configwinrmuser domain\DirectorServer$
Für die Aktionen "Prozess beenden", "Anwendung beenden" und "Spiegeln":

ConfigRemoteMgmt.exe /configwinrmuser domain\name /all
Erteilen von Berechtigungen für eine Benutzergruppe:

ConfigRemoteMgmt.exe /configwinrmuser domain\HelpDeskUsers /all

Anzeigen der Hilfe für das Tool:

ConfigRemoteMgmt.exe

Konfigurieren von HDX Insight

Feb 29, 2016

Hinweis: Die Verfügbarkeit dieser Funktion richtet sich nach der Lizenzierung der Organisation und den Administratorberechtigungen.

HDX Insight ist die Integration der EdgeSight-Netzwerkanalyse und der EdgeSight-Leistungsverwaltung in Director:

- Die EdgeSight-Netzwerkanalyse nutzt HDX Insight und stellt eine kontextbezogene Ansicht der Anwendungen und Desktops im Netzwerk bereit. Mit diesem Feature bietet Director eine erweiterte Analyse des ICA-Datenverkehrs in der Bereitstellung.
- Die EdgeSight-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, liefert HDX Insight zusätzliche Informationen an Director:

- Auf der Seite Trends werden bereitstellungsübergreifend Auswirkungen auf Latenz und Bandbreite für Anwendungen, Desktops und Benutzer angezeigt.
- Auf der Seite Benutzerdetails werden Latenz- und Bandbreiteninformationen zu spezifischen Benutzersitzungen angezeigt.

Einschränkungen

- Die Roundtripzeitdaten für die ICA-Sitzung werden in Receiver für Windows 3.4 oder höher und Receiver für Mac 11.8 oder höher richtig angezeigt. Bei früheren Versionen von Receiver werden die Daten nicht richtig angezeigt.
- In der Trendansicht werden Anmeldedaten für HDX-Verbindungen für VDAs vor Version 7 nicht gesammelt. Für frühere VDAs werden die Diagrammdaten als 0 angezeigt.

Konfigurieren der EdgeSight-Netzwerkanalyse in Director

EdgeSight bietet eine Netzwerkanalyse unter Nutzung von NetScaler HDX Insight, anhand derer Administratoren der Citrix Anwendungen und Desktops Probleme behandeln und korrelieren können, die auf eine schlechte Netzwerkleistung zurückzuführen sind.

NetScaler Insight Center muss in Director installiert und konfiguriert sein, damit die EdgeSight-Netzwerkanalyse aktiviert werden kann. Insight Center ist eine virtuelle Maschine (Gerät), die von Citrix.com heruntergeladen wird. Mit der EdgeSight-Netzwerkanalyse sammelt Director Daten zur Bereitstellung. Diese Informationen werden aus HDX Insight verwendet, das eine stabile Analyse des Citrix ICA-Protokolls zwischen dem Client und der Citrix Back-End-Infrastruktur bietet.

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, konfigurieren Sie den Maschinennamen (FQDN oder IP-Adresse) für NetScaler Insight Center sowie den Benutzernamen, das Kennwort und den HTTP- oder HTTPS-Verbindungstyp.
3. Melden Sie sich zum Prüfen der Änderungen ab und wieder an.

Behandeln von Benutzerproblemen

Feb 29, 2016

In der Ansicht **Helpdesk** (Seite **Aktivitäts-Manager**) in Director zeigen Sie Informationen über den Benutzer an:

- Überprüfen Sie die Details zur Anmeldung des Benutzers, zur Verbindung und zu den Anwendungen.
- Spiegeln Sie die Maschine des Benutzers.
- Behandeln Sie das Problem mit den in der folgenden Tabelle empfohlenen Aktionen und eskalieren Sie das Problem ggf. an den entsprechenden Administrator.

Tipps zur Problembehandlung

Problem des Benutzers	Lösungsvorschläge:
Anmeldung dauert lange oder schlägt periodisch oder wiederholt fehl	Diagnose von Benutzeranmeldeproblemen
Anwendung ist langsam oder reagiert nicht mehr	Beheben von Anwendungsfehlern
Verbindung ist fehlgeschlagen	Wiederherstellen von Desktopverbindungen
Sitzung ist langsam oder reagiert nicht	Wiederherstellen von Sitzungen
Video ist langsam oder von schlechter Qualität	Ausführen von Systemberichten für HDX-Kanäle

Hinweis: Um sicherzustellen, dass der Computer nicht im Wartungsmodus ist, überprüfen Sie in der Ansicht Benutzerdetails den Bereich Maschinendetails.

Suchtipps

Wenn Sie den Namen des Benutzers im Suchfeld eingeben, sucht Director in Active Directory nach Benutzern in allen Sites, die für Director konfiguriert wurden.

Wenn Sie den Namen einer Maschine, die von mehreren Benutzern verwendet wird, in ein Suchfeld eingeben, zeigt Director die Maschinendetails für die angegebene Maschine an.

Wenn Sie einen Endpunktnamen in ein Suchfeld eingeben, verwendet Director die nicht authentifizierten (anonymen) und die authentifizierten Sitzungen, die mit einem bestimmten Endpunkt verbunden sind, sodass Probleme in nicht authentifizierten Sitzungen behandelt werden können. Stellen Sie sicher, dass Endpunktnamen eindeutig sind, damit die Problembehandlung von nicht authentifizierten Sitzungen durchgeführt werden kann.

Die Suchergebnisse schließen auch Benutzer ein, die derzeit keine Maschine verwenden bzw. keiner Maschine zugewiesen sind.

- Bei der Suche wird die Groß- und Kleinschreibung nicht beachtet.
- Teileinträge ergeben eine Liste möglicher Übereinstimmungen.
- Nachdem Sie einige Buchstaben eines zweiteiligen Namens (Benutzername, Nachname und Vorname oder Anzeigename)

durch Leerzeichen getrennt eingegeben haben, enthalten die Ergebnisse Übereinstimmungen für beide Zeichenfolgen. Wenn Sie beispielsweisejo robeingeben, werden Zeichenfolgen wie "John Robertson" oder "Robert, Jones" als Ergebnisse angezeigt.

Klicken Sie auf das Director-Logo, um zur Startseite zurückzukehren.

Hochladen von Problembehandlungsinformationen zum technischen Support von Citrix

Führen Sie Citrix Scout auf einem Delivery Controller oder VDA aus, um wichtige Datenpunkte und CDF-Traces (Citrix Diagnosis Facility) für die Fehlerbehebung auf ausgewählten Computern zu erfassen. Mit Scout können Sie Daten sicher an Citrix Insight Services (CIS) hochladen, um den technischen Support von Citrix bei der Problembehandlung zu unterstützen. Der technische Support von Citrix nutzt die CIS-Plattform, um von Kunden gemeldete Probleme schneller zu lösen.

Scout wird mit XenApp- bzw. XenDesktop-Komponenten installiert. Je nach Windows-Version erscheint Scout im Startmenü bzw. Startbildschirm nach der Installation von (bzw. einem Upgrade auf) XenDesktop 7.1, XenDesktop 7.5, XenApp 7.5, XenDesktop 7.6, XenApp 7.6, XenDesktop 7.7 oder XenApp 7.7.

Zum Starten von Scout über das Startmenü oder den Startbildschirm wählen Sie **Citrix** > **Citrix Scout**.

Weitere Informationen zum Verwenden und Konfigurieren von Scout und häufig gestellte Fragen finden Sie unter CTX130147.

Spiegeln von Benutzern

Feb 29, 2016

Mit dem Feature Benutzer spiegeln in Director können Sie die virtuelle Maschine oder Sitzung eines Benutzers direkt anzeigen und damit arbeiten. Der Benutzer muss mit der zu spiegelnden Maschine verbunden sein. Wenn der Benutzer verbunden ist, wird der Name der verbundenen Maschine in der Titelleiste des Benutzers angezeigt.

1. Wählen Sie in der Ansicht Details die Benutzersitzung aus.
2. Aktivieren Sie die Spiegelung für die ausgewählte Benutzersitzung:
   - Klicken Sie zur Maschinenüberwachung in der Ansicht Aktivitäts-Manager auf Spiegeln.
   - Klicken Sie zur Sitzungsüberwachung in der Ansicht Benutzerdetails im Bereich Sitzungsdetails auf Spiegeln.
3. Nach Initialisierung der Verbindung werden Sie in einem Dialogfeld aufgefordert, die Datei .msrcincident zu öffnen oder zu speichern.
4. Öffnen Sie die Vorfalldatei mit dem Remoteunterstützung-Viewer, wenn er nicht standardmäßig ausgewählt ist. Auf dem Benutzergerät wird eine Bestätigungsaufforderung angezeigt.
5. Weisen Sie die Benutzer an, auf Ja zu klicken, um die Maschinen- oder die Sitzungsfreigabe zu starten.

Fordern Sie den Benutzer auf, die Tastatur- und Maussteuerung freizugeben, damit Sie die Steuerung übernehmen können.

Richten Sie den Microsoft Internet Explorer-Browser so ein, dass die heruntergeladene Datei zur Microsoft-Remoteunterstützung (.msra) automatisch mit dem Remoteunterstützungsclient geöffnet wird.

Hierzu müssen Sie die Einstellung Automatische Eingabeaufforderung für Dateidownloads im Gruppenrichtlinien-Editor aktivieren:

Computerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Internet Explorer > Internetsystemsteuerung > Sicherheitsseite > Internetzone > Automatische Eingabeaufforderung für Dateidownloads.

Diese Option ist standardmäßig für Sites in der lokalen Intranetzone aktiviert. Wenn die Director-Site nicht zur lokalen Intranetzone gehört, sollten Sie die Site manuell dieser Zone hinzufügen.

Senden von Nachrichten an Benutzer

Feb 29, 2016

Sie können über Director eine Nachricht an einen Benutzer senden, der mit einer oder mehreren Maschinen verbunden ist. Sie können beispielsweise mit dieser Funktion sofortige Benachrichtigungen über administrative Aktionen senden, wie bevorstehende Desktopwartung, Abmeldungen bzw. Neustarts von Maschinen und die Rücksetzung von Profilen.

1. Wählen Sie in der Ansicht Aktivitäts-Manager den Benutzer aus und klicken Sie auf Details.
2. Klicken in der Ansicht Benutzerdetails im Bereich Sitzungsdetails auf Nachricht senden.
3. Füllen Sie die Felder Betreff und Nachricht aus und klicken Sie auf Senden.

Wenn die Nachricht gesendet wird, wird in Director eine Bestätigungsmeldung angezeigt. Wenn die Maschine des Benutzers verbunden ist, wird dort eine entsprechende Nachricht angezeigt.

Wenn die Nachricht nicht gesendet wird, wird in Director eine Fehlermeldung angezeigt. Gehen Sie bei der Problembehandlung gemäß der Anweisungen in der Fehlermeldung vor. Geben Sie abschließend den Betreff und Text der Nachricht erneut ein und klicken Sie auf Noch einmal versuchen.

Diagnose von Benutzeranmeldeproblemen

Feb 29, 2016

Führen Sie diese allgemeinen Schritte aus:

1. Überprüfen Sie in der Ansicht Benutzerdetails im Bereich Anmeldedauer, welcher Anmeldezustand vorliegt.
   - Wenn Benutzer sich anmelden, wird der Anmeldeprozess in der Ansicht widergespiegelt.
   - Wenn der Benutzer bereits angemeldet ist, wird im Bereich Anmeldedauer angezeigt, wie viel Zeit für die Anmeldung des Benutzers an der aktuellen Sitzung benötigt wurde.
2. Fordern Sie die Benutzer auf, sich abmelden und neu anzumelden, damit Sie die Daten für Anmeldedauer beobachten können. Der Bereich wird ungefähr alle drei Minuten aktualisiert, es kann jedoch länger dauern, abhängig von der Dauer, die für den Abschluss der Anmeldung benötigt wird.
3. Untersuchen Sie die Phasen des Anmeldeprozess:
   - **Brokering**: zur Zuweisung des Desktops zum Benutzer benötigte Zeit.
   - **VM-Start**: zum Starten des Desktops benötigte Zeit.
   - **HDX-Verbindung**: je nach Netzwerk zum Herstellen der HDX-Verbindung benötigte Zeit.
   - **Gruppenrichtlinienobjekte**: zum Anwenden der Gruppenrichtlinienobjekte benötigte Zeit.
   - **Anmeldeskripts**: für die Skripts benötigte Zeit.
   - **Profilladezeit**: zum Laden des Benutzerprofils benötigte Zeit.
   - **Interaktive Sitzung**: zum Einrichten einer interaktiven Benutzersitzung benötigte Zeit.

   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.

   Tipp: 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 der 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 Brokeringdauer zu lang ist, können Sie das Problem dem Siteadministrator melden, damit der Lastausgleich auf dem Delivery Controller überprüft wird.

Tipps zur Problembehandlung: 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.
- Große Abweichung zwischen den Anmeldewerten des Benutzers (aktuelle und durchschnittliche Dauer) und der durchschnittlichen Dauer der Bereitstellungsgruppe.

Klicken Sie u. U. auf Neu starten, um den Anmeldeprozess des Benutzers zu beobachten und Probleme zu beheben, z. B. VM-Start oder Brokering.

Beheben von Anwendungsfehlern

Feb 29, 2016

Klicken Sie in der Ansicht Aktivitäts-Manager auf die Registerkarte Anwendungen. Sie können alle Anwendungen auf allen Maschinen anzeigen, auf die dieser Benutzer zugreifen kann, einschließlich der lokalen und der gehosteten Anwendungen für die derzeit verbundene Maschine und den aktuellen Status der einzelnen Maschine.
Hinweis: Wenn die Registerkarte Anwendungen abgeblendet ist, wenden Sie sich an einen Administrator, der die Berechtigung hat, die Registerkarte zu aktivieren.
Die Liste enthält nur die Anwendungen, die in der Sitzung gestartet wurden.

Für Serverbetriebssystemmaschinen und Desktopbetriebssystemmaschinen werden Anwendungen für jede getrennte Sitzung angezeigt. Wenn der Benutzer nicht verbunden ist, werden keine Anwendungen angezeigt.

Aktion	Beschreibung
Beenden Sie die 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 erneut zu starten.
Beenden Sie Prozesse, 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.
Starten Sie die Maschine des Benutzers neu.	Nur Desktopbetriebssystemmaschinen: Klicken Sie für die ausgewählte Sitzung auf Neu starten. Sie können auch in der Ansicht Maschinendetails die Maschine mit den Energiesteuerelementen neu starten oder herunterfahren. Fordern Sie den Benutzer auf, sich neu anzumelden, sodass Sie die Anwendung überprüfen können. Für Serverbetriebssystemmaschinen steht die Option "Neu starten" nicht zur Verfügung. Melden Sie stattdessen den Benutzer ab und fordern Sie ihn auf, sich neu anzumelden.
Setzen Sie die Maschine in den Wartungsmodus.	Wenn das Image einer Maschine gewartet werden muss, z. B. mit Patches oder anderen Updates, setzen Sie die Maschine in den Wartungsmodus und eskalieren Sie das Problem an den entsprechenden Administrator. Klicken Sie in der Ansicht Maschinendetails auf Details und aktivieren Sie die Option "Wartungsmodus". Eskalieren Sie an den entsprechenden Administrator.

Wiederherstellen von Desktopverbindungen

Feb 29, 2016

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.
Starten Sie die Maschine des Benutzers neu.	Wählen Sie die Maschine aus und klicken Sie auf Neu starten. Verwenden Sie diese Option, wenn die Maschine des Benutzers nicht mehr reagiert oder keine Verbindung herstellen kann, z. B. wenn die Maschine sehr viele CPU-Ressourcen verbraucht und dies die CPU unbrauchbar macht.

Wiederherstellen von Sitzungen

Feb 29, 2016

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 machen Sie in der Ansicht Benutzerdetails im Bereich Sitzungsdetails. Sie können die Details der aktuellen Sitzung (durch die Sitzungs-ID gekennzeichnet) anzeigen.

Aktion	Beschreibung
Beenden Sie Anwendungen und Prozesse, 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 entsprechenden Prozess auswählen, der nicht reagiert, und auf Prozess beenden. Beenden Sie auch Prozesse, die ungewöhnlich viel Speicher oder CPU-Ressourcen verbrauchen, da sie die CPU unbrauchbar machen können.
Trennen Sie die Windows-Sitzung.	Klicken Sie auf Sitzungssteuerung und wählen Sie dann Trennen. Diese Option steht nur für vermittelte Serverbetriebssystemmaschinen zur Verfügung. Für nicht vermittelte Sitzungen ist die Option deaktiviert.
Melden Sie den Benutzer von der Sitzung ab.	Klicken Sie auf Sitzungssteuerung und wählen Sie dann Abmelden.

Zum Testen der Sitzung kann der Benutzer versuchen, sich neu anzumelden. Sie können den Benutzer auch spiegeln, um diese Sitzung genauer zu beobachten.

Hinweis: Wenn VDAs vor XenDesktop 7 auf Benutzergeräten ausgeführt werden, kann Director keine vollständigen Informationen über die Sitzung anzeigen. Stattdessen wird in einer Meldung angezeigt, dass die Informationen nicht verfügbar sind. Diese Meldungen werden möglicherweise auf der Seite Benutzerdetails und im Aktivitäts-Manager angezeigt.

Ausführen von Systemberichten für HDX-Kanäle

Feb 29, 2016

Prüfen Sie in der Ansicht Benutzerdetails im Bereich HDX den Status der HDX-Kanäle auf der Maschine des Benutzers. Dieser Bereich ist nur verfügbar, wenn die Maschine des Benutzers mit HDX verbunden ist.
Wenn eine Meldung angibt, dass die Informationen zurzeit nicht verfügbar sind, warten Sie eine Minute, bis die Seite aktualisiert ist, oder klicken Sie auf die Schaltfläche Aktualisieren. Die Aktualisierung von HDX-Daten kann etwas länger dauern als bei anderen Daten.

Klicken Sie zur Anzeige weiterer Informationen auf das Fehler- oder Warnsymbol.

Tipp: Sie können Informationen über andere Kanäle in demselben Dialogfeld einblenden, indem Sie in der linken Ecke der Titelleiste auf den Pfeil nach links oder rechts klicken.
Systemberichte über die HDX-Kanäle werden hauptsächlich vom Citrix Support für die weitere Problembehandlung verwendet.

1. Klicken Sie im Bereich HDX auf Systembericht herunterladen.
2. Sie können die XML-Berichtdatei anzeigen oder speichern.
   - Klicken Sie zur Ansicht der XML-Datei auf Öffnen. Die XML-Datei wird in demselben Fenster wie die Anwendung Director angezeigt.
   - Klicken Sie zum Speichern der XML-Datei auf Speichern. Das Dialogfeld Speichern unter wird angezeigt, in dem Sie angeben, an welchem Speicherort auf der Director-Maschine die Datei heruntergeladen wird.

Zurücksetzen von Personal vDisk

Feb 29, 2016

Achtung: Beim Zurücksetzen der Disk werden die Einstellungen auf die werksseitigen Standardwerte zurückgesetzt und alle Daten, einschließlich der Anwendungen, werden gelöscht. Die Profildaten bleiben gespeichert, es sei denn, Sie haben den Personal vDisk-Standard geändert (d. h. das Umleiten der Profile vom Laufwerk C:) oder Sie verwenden keine Profillösung eines Drittanbieters.

Zum Zurücksetzen muss die Maschine mit Personal vDisk ausgeführt werden, der Benutzer muss aber nicht angemeldet sein.

Diese Option steht nur für Desktopbetriebssystemmaschinen zur Verfügung, sie ist für Serverbetriebssystemmaschinen deaktiviert.

1. Wählen Sie in der Ansicht Helpdesk die gewünschte Desktopbetriebssystemmaschine aus.
2. Klicken Sie in dieser Ansicht oder im Bereich Personalisierung der Ansicht Benutzerdetails auf Personal vDisk zurücksetzen.
3. Klicken Sie auf Zurücksetzen. Eine Warnmeldung gibt an, dass der Benutzer abgemeldet wird. Wenn der Benutzer abgemeldet ist (falls er angemeldet war), wird die Maschine neu gestartet.

Wenn das Zurücksetzen erfolgreich ist, wird im Feld Status im Bereich Personalisierung der Ansicht Benutzerdetails der Wert Wird ausgeführt angezeigt. Wenn das Zurücksetzen fehlgeschlagen ist, wird rechts neben Wird ausgeführt ein rotes X angezeigt. Wenn Sie auf dieses X zeigen, werden Informationen zu dem Fehler angezeigt.

Zurücksetzen eines Benutzerprofils

Feb 29, 2016

Achtung: Wenn ein Profil zurückgesetzt wird, werden die Ordner und Dateien des Benutzers zwar gespeichert und in das neue Profil kopiert, aber die meisten Benutzerdaten werden gelöscht (z. B. wird die Registrierung zurückgesetzt und die Anwendungseinstellungen werden möglicherweise gelöscht).

1. Suchen Sie in Director den Benutzer, dessen Profil Sie zurücksetzen möchten, und wählen Sie seine Benutzersitzung aus.
2. Klicken Sie auf **Profil zurücksetzen**.
3. Fordern Sie den Benutzer auf, sich von allen Sitzungen abzumelden.
4. Fordern Sie den Benutzer auf, sich erneut anzumelden. Der Ordner und Dateien, die aus dem Profil des Benutzers gespeichert wurden, werden in das neue Profil kopiert.
   Wichtig: Wenn der Benutzer Profile auf mehreren Plattformen (z. B. Windows 8 und Windows 7) hat, fordern Sie den Benutzer auf, sich zuerst bei dem gleichen Desktop oder bei der gleichen App anzumelden, bei dem bzw. der dieser Benutzer Probleme hatte. Dies stellt sicher, dass das richtige Profil zurückgesetzt wird.
   Wenn das Profil ein Citrix Benutzerprofil ist, ist es zum Zeitpunkt der Benutzerdesktopanzeige bereits zurückgesetzt. Bei Microsoft-Roamingprofilen dauert die Ordnerwiederherstellung möglicherweise noch kurze Zeit an. Der Benutzer muss angemeldet bleiben, bis die Wiederherstellung abgeschlossen ist.

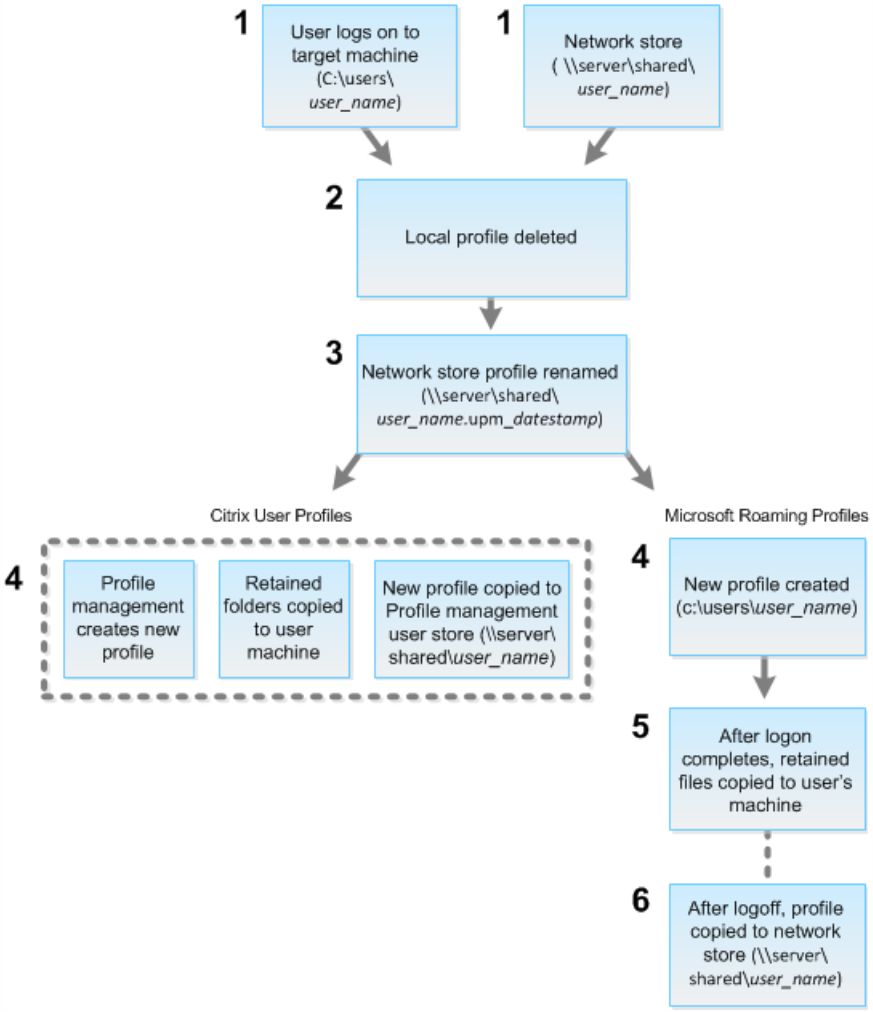
Hinweis: Bei den zuvor erläuterten Schritten wird davon ausgegangen, dass Sie XenDesktop (Desktop-VDA) verwenden. Wenn Sie XenApp (Server-VDA) verwenden, müssen Sie angemeldet sein, um das Profil zurückzusetzen. Der Benutzer muss sich dann abmelden und neu anmelden, um das Zurücksetzen des Profils abzuschließen.
Wenn das Profil nicht erfolgreich zurückgesetzt wird (z. B. der Benutzer kann sich nicht wieder anmelden oder einige der Dateien fehlen), müssen Sie das ursprüngliche Profil manuell wiederherstellen.
Die Ordner (und die Dateien) des Benutzerprofils werden gespeichert und in das neue Profil kopiert. Dabei gilt folgende Kopierreihenfolge:

- Desktop
- Cookies
- Favoriten
- Dokumente
- Bilder
- Musik
- Videos

Hinweis: In Windows 8 und höheren Versionen werden Cookies beim Zurücksetzen des Profils nicht kopiert.

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.

In diesem Diagramm wird die Verarbeitung dargestellt, die bei der nächsten Benutzeranmeldung ausgeführt wird.



1. Der Befehl zum Zurücksetzen von Director gibt den Profiltyp an. Der Profilverwaltungsdienst versucht dann, ein Profil dieses Typs zurückzusetzen und sucht die entsprechende Netzwerkfreigabe (Benutzerspeicher). Wenn der Benutzer von der Profilverwaltung verarbeitet wird, aber einen Roamingprofilbefehl erhält, wird er abgelehnt (oder umgekehrt).
2. Wenn ein lokales Profil vorhanden ist, wird es gelöscht.
3. Das Netzwerkprofil wird umbenannt.
4. Die nächste Aktion hängt davon ab, ob es sich bei dem Profil, das zurückgesetzt wird, um ein Citrix Benutzerprofil oder ein Microsoft Roamingprofil handelt.
   - Für Citrix Benutzerprofile wird das neue Profil mit den Importregeln der Profilverwaltung erstellt, die Ordner werden in das Netzwerkprofil zurückkopiert und der Benutzer kann die Anmeldung wie gewohnt fortsetzen. Wenn ein Roamingprofil für das Zurücksetzen verwendet wird, bleiben alle Registrierungseinstellungen im Roamingprofil im zurückgesetzten Profil gespeichert.
     Hinweis: Sie können in der Profilverwaltung konfigurieren, dass das Roamingprofil ggf. von einem Vorlagenprofil überschrieben wird.
   - Für Microsoft Roamingprofile wird ein neues Profil von Windows erstellt, und die Ordner werden bei Anmeldung des Benutzers auf das Benutzergerät zurückkopiert. Bei der nächsten Benutzerabmeldung wird das neue Profil in den Netzwerkspeicher kopiert.

1. Fordern Sie den Benutzer auf, sich von allen Sitzungen abzumelden.
2. Löschen Sie das lokale Profil, falls vorhanden.
3. Suchen Sie den archivierten Ordner auf der Netzwerkfreigabe, bei dem das Datum und die Uhrzeit dem Ordnernamen

angehängt wurden, also den Ordner mit der Erweiterung .upm_Datumsstempel.

4. Löschen Sie den aktuellen Profilnamen, d. h. die Datei ohne die Erweiterung upm_Datumsstempel.
5. Benennen Sie den archivierten Ordner in den ursprünglichen Profilnamen um (entfernen Sie den Datumsstempel). Sie haben das Profil auf den ursprünglichen Zustand zurückgesetzt.

SDKs und APIs

Feb 29, 2016

Das aktuelle Release enthält mehrere SDKs und APIs.

SDK für XenApp und XenDesktop: Dieses basiert auf zahlreichen Microsoft Windows PowerShell 3.0-Snap-Ins, mit dem Sie die gleichen Tasks wie mit der Citrix Studio-Konsole und andere Tasks ausführen können, die in Studio allein nicht möglich sind.

Weitere Informationen finden Sie unter Citrix Developer.

Citrix Group Policy SDK: Mit diesem SDK können Sie Einstellungen und Filter für Gruppenrichtlinien anzeigen und konfigurieren. Es verwendet einen PowerShell-Anbieter, um einen virtuellen Datenträger zu erstellen, der mit den Maschinen- und Benutzereinstellungen und -filtern übereinstimmt. Der Anbieter wird als Erweiterung zu New-PSDrive angezeigt. Für die Verwendung des Group Policy SDKs muss Studio oder das XenApp- bzw. XenDesktop-SDK installiert sein. Weitere Informationen finden Sie Abschnitt Group Policy SDK weiter unten.

Überwachungsdienst-OData-API: Diese API können Sie für Folgendes verwenden:

- Analysieren historischer Trends für die Planung
- Durchführen einer eingehenden Problembehandlung bei Verbindungs- und Maschinenfehlern
- Extrahieren von Informationen für die Eingabe in andere Tools und Prozesse, z. B. wenn PowerPivot-Tabellen in Microsoft Excel für die Anzeige von Daten auf verschiedene Weise verwendet werden
- Erstellen einer benutzerdefinierten Benutzeroberfläche auf der Basis der von der API bereitgestellten Daten

Weitere Informationen finden Sie in den Artikeln zur Überwachungsdienst-OData-API.

XenApp- und XenDesktop-SDK

Ab Version 7.x bieten XenApp und XenDesktop mit FlexCast Management Architecture eine einheitliche Architektur und Verwaltung. Daher stehen nun in XenApp viele Features bereit, die es zuvor nur in XenDesktop gab. Elemente des SDKs für gemeinsame Features gelten also nun sowohl für XenApp als auch für XenDesktop, selbst wenn die Befehle sich nur auf XenDesktop beziehen.

In der folgenden Liste werden die Unterschiede zwischen Version 5 und 7.x des SDKs für XenApp und XenDesktop aufgeführt.

- **Neues SDK auf höherer Ebene**: XenDesktop 7 umfasst ein neues SDK auf höherer Ebene, mit dem Sie schnell und mühelos ein Skript erstellen und die Siteerstellung und -wartung automatisieren. Das SDK auf höherer Ebene isoliert Sie von der Komplexität der SDKs auf niedrigerer Ebene, sodass Sie für das Erstellen einer neuen Site nur zwei Cmdlets ausführen müssen.
- **Neue SDKs auf niedriger Ebene**: Einzelne SDKs auf niedriger Ebene werden für die neuen XenDesktop 7-Dienste bereitgestellt, u. a. ein dediziertes und verbessertes SDK für den Dienst für die delegierte Administration (DAS), das vorher Teil des Broker-SDKs in XenDesktop 5 war. Es gibt auch SDKs für neue Features, u. a. Überwachungsdienst, Umgebungstest und Konfigurationsprotokollierung.
- **Kataloge und Bereitstellungsgruppen für Windows-Serverbetriebssystemmaschine**: Mit dem XenDesktop 7-

SDK stellen Sie kostengünstig Anwendungen und Desktops bereit, die auf Serverbetriebssystemen gehostet werden.

- **Anwendungen für Desktopbetriebssystemmaschinen**: Anwendungen für Desktopbetriebssystemmaschinen haben sich auf der SDK-Ebene wesentlich geändert. Wenn Sie vorhandene Skripts für die Ausführung von Anwendungen auf Desktopbetriebssystemen haben, müssen Sie diese Skripts für XenDesktop 7 aktualisieren, da es fast keine Rückwärtskompatibilität gibt.
- **Anwenden von Einstellungen auf Maschinen in Bereitstellungsgruppen**: In XenDesktop 7 können Sie mit Konfigurationsslots Einstellungen auf Maschinen in einer bestimmten Bereitstellungsgruppe statt auf alle Maschinen in einer Site anwenden. So können Sie für eine bestimmte Bereitstellungsgruppe konfigurieren, welche Einstellungen für diese Gruppe gelten. Zahlreiche vordefinierte Konfigurationsslots werden bereitgestellt, die unterschiedliche Typen von Einstellungen enthalten, u. a. Einstellungen für StoreFront-Adressen, die mit Speicherorten von Receiver- oder App-V-Veröffentlichungserver verwendet werden. Eine Sammlung von Einstellungen kann sich nur auf eine bestimmte Bereitstellungsgruppe auswirken, und eine andere Sammlung von Einstellungen von dem gleichen Slot wirkt sich auf eine andere Bereitstellungsgruppe aus. Sie können Namen verwenden, die für Ihre Bereitstellung geeignet sind, z. B. "Vertriebsabteilungsrichtlinie".
- **Ersetzte Katalogtypen**: In XenDesktop 7 wurden Katalogtypen durch Kataloge mit individuellen Eigenschaften ersetzt. Für die Rückwärtskompatibilität können Sie weiterhin vorhandene Skripts nutzen, die Katalogtypen verwenden, z. B. ein Image (gepoolt) und Thin Clone (dediziert) usw., intern werden diese jedoch in Gruppen von Eigenschaften konvertiert.
  Achtung: Die Rückwärtskompatibilität mit XenDesktop 5-Katalogtypen wurde beibehalten, wenn es praktikabel war. Verwenden Sie beim Schreiben neuer Skripts jedoch keine Katalogtypen sondern geben Sie Kataloge mit individuellen Eigenschaften an.

- **Ersetztes Desktopobjekte**: In XenDesktop 5 ist das Desktopobjekt einer der Haupttypen des SDK-Objekts, das in Broker-SDK-Skripts verwendet wird. Das Desktopobjekt beschreibt sowohl die Maschine als auch die Sitzung auf der Maschine. In XenDesktop 7 wird dieses Objekt durch das Sitzungsobjekt und das Maschinenobjekt ersetzt, die beide erweitert wurden und jetzt die Funktion des Desktopobjekts übernehmen. Für die Rückwärtskompatibilität können Sie jedoch weiterhin vorhandene Skripts verwenden, die das Desktopobjekt nutzen.
  Achtung: Die Rückwärtskompatibilität mit XenDesktop 5 wurde beibehalten, wenn es praktikabel war. Verwenden Sie beim Schreiben neuer Skripts jedoch nicht das Desktopobjekt, sondern geben Sie Sitzungs- und Maschinenobjekte an.

Die Richtlinienregeln im SDK und der Studio-Konsole sind nicht identisch. Anspruchs- und Zuordnungsrichtlinienregeln sind unabhängige Entitäten im SDK, und in der Konsole. Diese Entitäten sind nicht sichtbar, da sie nahtlos mit der Bereitstellungsgruppe zusammengeführt werden. Weiterhin sind Richtlinienregeln im SDK weniger restriktiv.

Das SDK enthält mehrere PowerShell-Snap-Ins, die automatisch vom Installationsassistenten installiert werden, wenn Sie den Delivery Controller oder Studio installieren.

Berechtigungen: Sie müssen die Shell oder das Skript mit einer ID ausführen, die über Citrix Administratorrechte verfügt. Obwohl die Mitglieder der lokalen Administratorgruppe auf dem Controller automatisch über Volladministratorprivilegien verfügen, um XenApp bzw. XenDesktop zu installieren, empfiehlt Citrix, dass Sie für den normalen Betrieb Citrix Administratoren mit den entsprechenden Rechten erstellen und nicht das lokale Administratorkonto verwenden. Wenn Sie Windows Server 2008 R2 ausführen, müssen Sie die Shell oder das Skript als Citrix Administrator und nicht als Mitglied der lokalen Administratorgruppe ausführen.

Zugreifen auf die Cmdlets:

1. Starten einer Shell in PowerShell 3.0: Öffnen Sie Studio, wählen Sie die Registerkarte **PowerShell** und klicken Sie auf **PowerShell starten**.
2. Legen Sie die Ausführungsrichtlinie in PowerShell fest, um SDK-Cmdlets in Skripts zu verwenden. Weitere Informationen zur PowerShell-Ausführungsrichtlinie finden Sie in der Dokumentation von Microsoft.
3. Fügen Sie mit dem Cmdlet **Add -PSSnapin** in der Windows PowerShell-Konsole die Snap-Ins hinzu, die Sie in der PowerShell-Umgebung benötigen.

    V1 und V2 beziehen sich auf die Version des Snap-Ins. (XenDesktop 5-Snap-Ins sind Version 1; XenDesktop 7-Snap-Ins sind Version 2. Zum Installieren von XenDesktop 7-Snap-Ins geben Sie beispielsweise "Add-PSSnapin Citrix.ADIdentity.Admin.V2" ein.) Geben Sie zum Importieren aller Cmdlets "Add-PSSnapin Citrix.*.Admin.V*" ein.

Nach dem Hinzufügen der Snap-Ins, können Sie auf die Cmdlets und die zugehörige Hilfe zugreifen.

Group Policy SDKs

Für die Verwendung des Group Policy SDKs muss Studio oder das XenApp- bzw. XenDesktop-SDK installiert sein.

Zum Hinzufügen des Group Policy SDKs geben Sie **Add-PSSnapin citrix.common.grouppolicy** ein. (Zum Aufrufen der Hilfe geben Sie **help New-PSDrive -path localgpo:/** ein.)

Zum Erstellen einer virtuellen Festplatte und Laden dieser Festplatte mit Einstellungen geben Sie Folgendes ein: **New-PSDrive <*Standard Parameters*> [-PSProvider] CitrixGroupPolicy -Controller <*Zeichenfolge*>**, wobei die Controller-Zeichenfolge der vollqualifizierte Domänenname eines Controllers in der Site ist, aus der die Einstellungen geladen werden sollen.

Überwachungsdienst-OData-API

Feb 29, 2016

Zusätzlich zur Anzeige von historischen Daten in der Citrix Director-Konsole können Sie Daten mit der Überwachungsdienst-OData-API abfragen. Sie können die API für Folgendes verwenden:

- Analysieren historischer Trends für die Planung
- Durchführen einer eingehenden Problembehandlung bei Verbindungs- und Maschinenfehlern
- Extrahieren von Informationen für die Eingabe in andere Tools und Prozesse, z. B. wenn PowerPivot-Tabellen in Microsoft Excel für die Anzeige von Daten auf verschiedene Weise verwendet werden
- Erstellen einer benutzerdefinierten Benutzeroberfläche auf der Basis der von der API bereitgestellten Daten

Die Überwachungsdienst-OData-API verwendet das Open Data-Protokoll (OData), ein Webprotokoll für die Abfrage und Aktualisierung von Daten, das auf Webtechnologien wie HTTP aufbaut. Weitere Informationen über das OData-Protokoll finden Sie unter http://www.odata.org.

Die Überwachungsdienst-API setzt mit den Windows Communication Foundation (WCF) Data Services auf SQL Server-Datenbanken auf, die während der Verarbeitung und Konsolidierung aufgefüllt werden. Bei Verwendung von WCF mit wsHttpBinding werden zwei Endpunkte verfügbar gemacht. Die Basisadresse ist http:// {dc-host}/Citrix/Monitor/OData/v2. Sie können Endpunkte auch mit TLS schützen (weitere Informationen finden Sie unter Schützen von Endpunkten mit TLS).

1. Der Endpunkt "Data" gestattet direkten Lesezugriff auf die Datenbankentitäten, Zugriff ist mit der Abfragesprache OData möglich. Dieser Endpunkt gestattet einen sehr flexiblen Zugriff im Hinblick auf Filter- und Spaltenauswahl. Die URI der Data-API ist: http://{dc-host}/Citrix/Monitor/OData/v2/Data. Weitere Informationen über den Zugriff auf Monitor Service-Daten finden Sie unter Zugriff auf Daten mit der API.
2. Der Endpunkt "Methods" macht Dienstvorgänge verfügbar, die von Citrix Director für das Abrufen von Daten verwendet werden, die eine komplexe Gruppierung und hohe Leistungsstandards erfordern (z. B. Abfragen für das Dashboard und Trend-Seiten). Die URI der Methods-API ist: http://{dc-host}/Citrix/Monitor/OData/v2/Methods. Methoden werden nur in Director selbst verwendet, d. h. nicht von der Mehrheit der Citrix Kunden. Sie werden daher hier nicht dokumentiert.

Die in XenApp und XenDesktop 7.6 enthaltene API-Version bietet die folgenden neuen Features:

- **Hotfix-Bestand** In der Ansicht "Benutzerdetails" oder „Maschine“ in Director können Sie eine Liste aller Citrix Hotfixes anzeigen, die auf einer Maschine installiert wurden. Sie können mit der API diese Daten extrahieren und benutzerdefinierte Berichte erstellen (z. B. Status der installierten Hotfixes über eine ganze Site) oder sie in eine Analyticsengine ziehen. Neue Klassen wurden eingeführt und die Maschinenklasse unterstützt nun die Nachverfolgung von auf dem Controller und VDAs installierten Citrix Hotfixes.
- **Anonyme Sitzungsproblembehandlung.** Sitzungen können in Form gepoolter lokaler Benutzerkonten ausgeführt werden. Die API hat eine neue IsAnonymous-Eigenschaft für die Sitzungsklasse (Standardwert = FALSE).
- **Bericht über die Verwendung gehosteter Anwendungen.** Director bietet neue Kapazitätsberichte zur Verwendung gehosteter Anwendungen über bestimmte Zeiträume. Mit der API können Sie Berichte zu den Details jeder in einer Benutzersitzung ausgeführten Anwendungsinstanz erstellen.

Alle die Daten betreffenden Updates sind in der API-Referenz unter http://support.citrix.com/help/monitorserviceapi/7.6/ vollständig dokumentiert.

Die Methode "GetSessionSummary" ist seit diesem Release veraltet.

Zugriff auf Daten mit der API

Feb 29, 2016

Die folgenden Datentypen sind über die Überwachungsdienst-API verfügbar:

- Daten zu Verbindungsfehlern
- Maschinen in fehlerhaftem Zustand
- Sitzungsnutzung
- Anmeldedauer
- Daten zum Lastausgleich
- Auf eine Maschine angewendete Hotfixes
- Verwendung gehostete Anwendung

Eine komplette Beschreibung der Datenobjekte finden Sie unter http://blogs.citrix.com/2013/08/27/xendesktop-7-monitor-service-what-data-is-available/.

Zur Verwendung der Überwachungsdienst-OData-API müssen Sie XenApp- bzw. XenDesktop-Administrator sein. Zum Aufrufen der API ist Lesezugriff erforderlich. Welche Daten zurückgegeben werden, hängt von den Rollen und Berechtigungen des XenApp- bzw. XenDesktop-Administrators ab. Administratoren von Bereitstellungsgruppen können beispielsweise die Überwachungsdienst-API aufrufen, aber die zurückgegebenen Daten hängen von dem mit Citrix Studio eingerichteten Bereitstellungsgruppenzugriff ab. Weitere Informationen über XenApp-/XenDesktop-Administratorrollen und -berechtigungen finden Sie unter Delegierte Administration.

Abfragen der Daten

Die Überwachungsdienst-API ist eine REST-basierte API, auf die mit einem OData-Consumer zugegriffen werden kann. OData-Consumer sind Anwendungen, die mit dem OData-Protokoll verfügbar gemachte Daten nutzen. OData-Consumer reichen vom einfachen Webbrowser bis zur benutzerdefinierten Anwendung, die sämtliche Features des OData-Protokolls nutzt. Weitere Informationen über OData-Consumer finden Sie unter http://www.odata.org/ecosystem#consumers.

Jeder Teil des Überwachungsdienst-Datenmodells ist zugänglich und kann über die URL gefiltert werden. OData bietet eine Abfragesprache im URL-Format zum Abrufen von Einträgen aus einem Dienst. Weitere Informationen finden Sie unter http://msdn.microsoft.com/en-us/library/ff478141.aspx.

Die Abfrage wird serverseitig verarbeitet und kann clientseitig mit dem OData-Protokoll weiter gefiltert werden.

Die modellierten Daten fallen in drei Hauptkategorien: Aggregierte Daten (die Zusammenfassungstabellen), aktueller Zustand von Objekten (Maschinen, Sitzungen usw.) und Protokolldaten, wobei es sich um historische Ereignisse handelt (z. B. Verbindungen).

Hinweis: Enumerationen werden vom OData-Protokoll nicht unterstützt, stattdessen werden ganze Zahlen verwendet. Weitere Informationen zum Bestimmen der von der Überwachungsdienst-OData-API zurückgegebenen Werte finden Sie unter http://support.citrix.com/help/monitorserviceapi/7.6/.

Aggregation der Datenwerte

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 in einem bestimmten Zeitraum auf und werden daher als Höchstwerte in einem Zeitraum verfügbar gemacht.
- Die Anmeldedauer ist ein Zeitlängenwert und wird daher als Durchschnitt in einem Zeitraum verfügbar gemacht.
- Die Anzahl der Anmeldungen und Verbindungsfehler repräsentieren eine Anzahl von Vorkommen in einem bestimmten Zeitraum und werden als Summen in einem Zeitraum gemacht.

Auswertung gleichzeitiger Daten

Sitzungen müssen sich überschneiden, um als gleichzeitig angesehen zu werden. Bei einem Zeitintervall von 1 Minute werden jedoch alle Sitzungen in dieser Minute (mit oder ohne Überschneidung) als gleichzeitig angesehen, d. h. das Intervall ist so klein, dass sich der Mehraufwand für die Berechnung der Genauigkeit nicht lohnt. Finden die Sitzungen in der gleichen Stunde, aber nicht in der gleichen Minute statt, werden sie als einander nicht überschneidend angesehen.

Korrelation der Zusammenfassungstabellen mit Rohdaten

Das Datenmodell stellt Metriken auf zwei verschiedene Arten dar:
- Die Zusammenfassungstabellen zeigen aggregierte Ansichten der Metriken in Granularitäten pro Minute, Stunde und Tag an.
- Die Rohdaten stehen für einzelne Ereignisse oder den aktuellen Zustand, der bzw. die für eine Sitzung, Verbindung, Anwendung und andere Objekte protokolliert werden.

Wenn Sie versuchen, Daten über API-Aufrufe hinweg oder innerhalb des Datenmodells selbst zu korrelieren, sollten Sie die folgenden Konzepte und Einschränkungen kennen:

- **Keine Zusammenfassungsdaten für Teilintervalle:** Die Zusammenfassungen von Metriken erfüllen die Anforderungen von historischen Trends über lange Zeiträume hinweg. Diese Metriken werden für vollständige Intervalle in der Zusammenfassungstabelle aggregiert. Für Teilintervalle am Anfang (die ältesten verfügbaren Daten) und am Ende der Datensammlung gibt es keine Zusammenfassungsdaten. Beim Anzeigen der Aggregation eines Tages (Intervall=1440) bedeutet dies, dass der erste Tag und der aktuelle unvollständige Tag keine Daten aufweisen. Obwohl für diese Teilintervalle u. U. Rohdaten vorhanden sind, werden sie nie zusammengefasst. Sie können das früheste und letzte Aggregationsintervall für eine bestimmte Datengranularität festlegen, indem Sie die Mindest- und Höchstwerte für "SummaryDate" aus einer bestimmten Zusammenfassungstabelle nehmen. Die Spalte "SummaryDate" stellt den Start des Intervalls dar. Die Spalte "Granularity" steht für die Länge des Intervalls der aggregierten Daten.
- **Korrelation nach Zeit:** Metriken werden, wie oben beschrieben, für vollständige Intervalle in der Zusammenfassungstabelle aggregiert. Sie können für historische Trends verwendet werden, aber rohe Ereignisdaten stellen möglicherweise einen aktuelleren Zustand dar als die Zusammenfassung für die Trendanalyse. Bei zeitbasierten Vergleichen zwischen der Zusammenfassung und den Rohdaten muss beachtet werden, dass es keine Zusammenfassungsdaten für Teilintervalle gibt, die am Anfang und Ende des Zeitraums auftreten.
- **Verpasste und latente Ereignisse:** Wenn Ereignisse verpasst werden oder während des Aggregationszeitraums latent sind, sind die für die Zusammenfassungstabelle aggregierten Metriken möglicherweise ungenau. Obwohl der Überwachungsdienst versucht, einen genauen aktuellen Zustand zu erhalten, wird die Aggregation für verpasste oder latente Ereignisse nicht im Nachhinein neu für die Zusammenfassungstabellen berechnet.
- **Hochverfügbare Verbindungen:** Bei hoher Verfügbarkeit von Verbindungen entstehen in den Zusammenfassungsdaten für aktuelle Verbindungen Lücken, aber die Sitzungsinstanzen werden dennoch in den Rohdaten ausgeführt.
- **Beibehaltungszeitraum für Daten:** Daten werden in den Zusammenfassungstabellen basierend auf einem anderen Bereinigungszeitplan beibehalten als Rohdaten von Ereignissen. Daten fehlen möglicherweise, weil die Zusammenfassungstabellen oder die unformatierten Tabellen bereinigt wurde. Beibehaltungszeiträume können

unterschiedliche Granularitäten für Zusammenfassungsdaten aufweisen. Daten basierend auf niedrigerer Granularität (Minuten) werden schneller bereinigt als Daten, die auf höherer Granularität (Tage) basieren. Wenn Daten bereinigt wurden und in einer Granularitätskategorie fehlen, sind sie möglicherweise in einer höheren Granularitätskategorie. API-Aufrufe geben nur Daten für die angeforderte Granularität zurück. Wenn für eine Granularität keine Daten zurückgegeben werden, sind möglicherweise für den gleichen Zeitraum Daten für eine höhere Granularität vorhanden.

- **Zeitzonen:** Metriken werden mit UTC-Zeitstempeln gespeichert. Zusammenfassungstabellen werden basierend auf stündlichen Zeitzonengrenzen aggregiert. Bei Zeitzonen, die nicht in diese stündlichen Grenzen fallen, gibt es möglicherweise Unstimmigkeiten beim Ort der Datenaggregation.

Datengranularität und -beibehaltung

Die Granularität der aggregierten Daten, die von Director abgerufen werden, ist eine Funktion des angeforderten Zeitraums (T). Folgende Regeln gelten:

- 0 < T <= 1 Stunde: minutengenaue Granularität wird verwendet
- 0 <=30 Tage: stundengenaue Granularität wird verwendet
- T > 31 Tage: tagesgenaue Granularität wird verwendet

Angeforderte Daten, die nicht von aggregierten Daten stammen, stammen von den rohen Sitzungs- und Verbindungsinformationen. Diese Menge dieser Daten nimmt schnell zu, daher haben sie eine eigene Bereinigungseinstellung. Bereinigung gewährleistet, dass nur relevante Daten langfristig gespeichert werden. Damit wird eine bessere Leistung sichergestellt, während die für die Berichterstellung erforderliche Granularität beibehalten werden kann. Bei Kunden, die keine Lizenz für die Platinum Edition haben, beginnt die Bereinigung am 8. Tag, unabhängig vom Standardbereinigungszeitraum. Platinum-Kunden können den Beibehaltungszeitraum auf die gewünschte Anzahl an Tagen einstellen, sonst wird der Standardwert verwendet.

Mit den folgenden Einstellungen wird die Bereinigung gesteuert:

Einstellungsname	Betroffene Bereinigung	Standardwert (Tage)	Zugriff mit
GroomSessionsRetentionDays	Sitzungs- und Sitzungsdetaileinträge	7 für Nicht-Platinum-Benutzer, 90 für Platinum	Cmdlet (set/get-monitorconfiguration)
GroomSummariesRetentionDays	Einträge für DesktopGroupSummary, FailureLogSummary und LoadIndexSummary. Aggregierte Daten, tägliche Granularität	7 für Nicht-Platinum-Benutzer, 90 für Platinum	Cmdlet (set/get-monitorconfiguration)
GroomHourlyRetentionDays	Aggregierte Daten - stundengenaue Granularität	32 Tage	Monitor.Configuration Database Table. Siehe Hinweis unten.
GroomMinuteRetentionDays	Aggregierte Daten - minutengenaue Granularität	3 Tage	Monitor.Configuration Database Table. Siehe Hinweis unten.

Einstellungsname	Betroffene Bereinigung	Standardwert (Tage)	Zugriff mit
GroomFailuresRetentionDays	Einträge für MachineFailureLog und ConnectionFailureLog	7 für Nicht-Platinum-Benutzer, 90 für Platinum	Cmdlet (set/get-monitorconfiguration)
GroomLoadIndexesRetentionDays	Einträge für LoadIndex	7 für Nicht-Platinum-Benutzer, 90 für Platinum	Cmdlet (set/get-monitorconfiguration)
GroomDeletedRetentionDays	Maschinen-, Katalog-, Desktopgruppen- und Hypervisorentitäten, die einen LifecycleState von "Deleted" haben. Dadurch werden auch zugehörige Einträge für Sitzung, Sitzungsdetail, Zusammenfassung, Fehler oder LoadIndex gelöscht.	7 für Nicht-Platinum-Benutzer, 90 für Platinum	Cmdlet (set/get-monitorconfiguration)
GroomMachineHotfixHistoryRetentionDays	Auf VDA und Controllermaschinen angewendete Hotfixes	90 für Nicht-Platinum- und Platinum-Benutzer	Cmdlet (set/get-monitorconfiguration)

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.

Das Beibehalten von Daten über lange Zeiträume hinweg hat die folgenden Auswirkungen auf die Größe von Tabellen:

- **Stundengenaue Daten:** Wenn Sie stundengenaue Daten bis zu zwei Jahre lang in der Datenbank speichern, wächst die Datenbank einer Site mit 1000 Bereitstellungsgruppen ungefähr wie folgt an:
  1000 Bereitstellungsgruppen x 24 Stunden/Tag x 365 Tage/Jahr x 2 Jahre = 17.520.000 Datenreihen. Diese große Datenmenge in den Aggregationstabellen hat beträchtliche Auswirkungen auf die Leistung. Wenn man bedenkt, dass die Dashboarddaten aus dieser Tabelle gezogen werden, sind die Anforderungen an den Datenbankserver möglicherweise riesig. Übermäßig viele Daten können dramatische Auswirkungen auf die Leistung haben.

- **Sitzungs- und Ereignisdaten:** Diese Daten werden jedes Mal gesammelt, wenn eine Sitzung gestartet und eine Verbindung/Wiederverbindung hergestellt wird. Bei einer großen Site (100.000 Benutzer) nimmt die Menge dieser Daten sehr schnell zu. Beispielsweise entsprechen die über zwei Jahre gespeicherten Tabellen mehr als 1 TB Daten und erfordern eine High-End-Unternehmensdatenbank.

Securing endpoints using TLS

Feb 29, 2016

This document explains how to use TLS to secure the Monitor Service OData API endpoints. If you choose to use TLS, you must configure TLS on all Delivery Controllers in the site; you cannot use a mixture of TLS and non-TLS.

To secure Monitor Service endpoints using TLS, you must perform the following configuration. Some steps need to be done only once per site, others must be run from every machine hosting the Monitor Service in the site. The steps are described below.

Part 1: Certificate registration with the system

1. Create a certificate using a trusted certificate manager. The certificate must be associated with the port on the machine that you wish to use for OData TLS.
2. Configure the Monitor Service to use this port for TLS communication. The steps depend on your environment and how this works with certificates. The following example shows how to configure port 449:

- Associate the certificate with a port:
  netsh http add sslcert ipport=0.0.0.0:449 certhash=97bb629e50d556c80528f4991721ad4f28fb74e9
  appid='{00000000-0000-0000-0000-000000000000}'
  Tip: In a PowerShell command window, ensure you put single quotes around the GUID in the appID, as shown above, or the command will not work. Note that a line break has been added to this example for readability only.

Part 2: Modify the Monitor Service configuration settings

1. From any Delivery Controller in the site, run the following PowerShell commands once. This removes the Monitor Service registration with the Configuration Service.
   asnp citrix.*

   $serviceGroup = get-configregisteredserviceinstance -servicetype Monitor | Select -First 1 ServiceGroupUid

   remove-configserviceGroup -ServiceGroupUid $serviceGroup.ServiceGroupUid
2. Do the following on all Controllers in the site:
   - Using a cmd prompt, locate the installed Citrix Monitor directory (typically in C:\Program Files\Citrix\Monitor\Service). Within that directory run:
     Citrix.Monitor.Exe -CONFIGUREFIREWALL -ODataPort 449 -RequireODataSsl
   - Run the following PowerShell commands:

   asnp citrix.* (if not already run within this window)

   get-MonitorServiceInstance | register-ConfigServiceInstance

   Get-ConfigRegisteredServiceInstance -ServiceType Config | Reset-MonitorServiceGroupMembership

Beispiele

Feb 29, 2016

Die folgenden Beispiele zeigen, wie Daten mit der Überwachungsdienst-OData-API exportiert werden.

Beispiel 1 – unformatiertes XML

1. Geben Sie die URL für jede Datengruppe in einen Webbrowser ein, der mit den für die XenApp- bzw. XenDesktop-Site erforderlichen Administratorrechten ausgeführt wird. Citrix empfiehlt die Verwendung des Chrome-Browsers mit dem Add-In Advanced Rest Client.
2. Zeigen Sie die Quelle an.

Beispiel 2 - PowerPivot für Excel

Bei diesen Anweisungen wird davon ausgegangen, dass Sie Microsoft Excel und PowerPivot bereits installiert haben.

Öffnen Sie Excel mit den für die XenApp- bzw. XenDesktop-Site erforderlichen Administratorrechten.

Bei Verwendung von Excel 2010:

1. Klicken Sie auf der Registerkarte "PowerPivot".
2. Klicken Sie auf "PowerPivot-Fenster".
3. Klicken Sie im Menüband auf **Aus Datenfeeds**.
4. Wählen Sie einen Anzeigenamen für die Verbindung aus (z. B. XenDesktop-Überwachungsdaten) und geben Sie die Datenfeed-URL ein: http://{dc-host}/Citrix/Monitor/OData/v1/Data (oder "https:", falls Sie TLS verwenden).
5. Klicken Sie auf **Next**.
6. Wählen Sie die Tabellen aus, die Sie in Excel importieren möchten, und klicken Sie auf **Fertig stellen**. Die Daten werden abgerufen.
7. Sie können die Daten jetzt über PowerPivot mit PivotTables und PivotCharts anzeigen und analysieren. Weitere Informationen finden Sie im Learning Center: http://www.microsoft.com/en-us/bi/LearningCenter.aspx.

Bei Verwendung von Excel 2013:

1. Klicken Sie auf die Registerkarte "Daten".
2. Wählen Sie "Aus anderen Quellen > Aus OData-Datenfeed".
3. Geben Sie die URL des Datenfeeds ein: http://{dc-host}/Citrix/Monitor/OData/v1/Data (oder "https:", wenn Sie TLS verwenden) und klicken Sie auf **Weiter**.
4. Wählen Sie die Tabellen aus, die Sie in Excel importieren möchten, und klicken Sie auf **Weiter**.
5. Akzeptieren Sie die Standardnamen oder passen Sie Namen an und klicken Sie auf **Fertig stellen**.
6. Wählen Sie **Nur Verbindung** oder **Pivot Report**. Die Daten werden abgerufen.
7. Sie können die Daten jetzt über PowerPivot mit PivotTables und PivotCharts anzeigen und analysieren. Weitere Informationen finden Sie im Learning Center: http://www.microsoft.com/en-us/bi/LearningCenter.aspx.

Beispiel 3 – LINQPad

Bei diesen Anweisungen wird davon ausgegangen, dass Sie LINQPad bereits installiert haben.

1. Führen Sie LinqPad mit den für die XenApp- bzw. XenDesktop-Site erforderlichen Administratorrechten aus.
   Tipp: Die einfachste Methode ist Download, Installation und Ausführung auf dem Delivery Controller.
2. Klicken Sie auf den Link "Add connection".

3. Wählen Sie "WCF Data Services 5.1 (OData 3)" und klicken Sie auf **Weiter**.
4. Geben Sie die URL des Datenfeeds ein: http://{dc-host}/Citrix/Monitor/OData/v2/Data (oder "https:", wenn Sie TLS verwenden). Falls erforderlich, geben Sie den Benutzernamen und das Kennwort für den Zugriff auf den Delivery Controller ein. Klicken Sie auf **OK**.
5. Sie können jetzt LINQ-Abfragen für den Datenfeed ausführen und die Daten nach Bedarf exportieren. Beispiel: Klicken Sie mit der rechten Maustaste auf "Catalogs" und wählen Sie **Catalogs.Take(100)** aus. Damit werden die ersten 100 Kataloge in der Datenbank zurückgegeben. Wählen Sie "Export > Export to Excel with formatting" aus.

Weitere funktionierende Beispiele für die Verwendung der API mit LINQPad finden Sie unter http://blogs.citrix.com/2014/01/14/creating-director-custom-reports-for-monitoring-xendesktop/.