StoreFront 3.15

Jun 04, 2018

StoreFront verwaltet die Bereitstellung von Desktops und Anwendungen von den XenApp-, XenDesktop- und XenMobile-Servern im Datenzentrum auf den Geräten der Benutzer. StoreFront enumeriert und aggregiert verfügbare Desktops und Anwendungen in Stores. Benutzer greifen auf StoreFront-Stores direkt über Citrix Receiver zu oder mit einem Browser über eine Citrix Receiver für Web-Site oder eine Desktopgerätesite. Darüber hinaus können Benutzer mit Thin Clients und anderen kompatiblen Geräten über eine XenApp Services-Site auf StoreFront zugreifen.

In StoreFront wird ein Datensatz der Anwendungen der Benutzer gespeichert und die Geräte werden automatisch aktualisiert. Die Benutzererfahrung beim Wechsel zwischen Smartphone, Tablet, Laptop und PC ist konsistent. StoreFront ist eine integrierte Komponente von XenApp 7.x und XenDesktop 7.x. Es kann aber auch mit anderen Versionen von XenApp und XenDesktop verwendet werden.

Sie können StoreFront unter https://www.citrix.com/downloads/storefront-web-interface/ herunterladen und installieren.

StoreFront 3.15 enthält eine Reihe von behobenen und bekannten Problemen.

Neue Features

Jun 04, 2018

StoreFront 3.15 enthält die folgende Funktionserweiterung und eine Reihe von behobenen und bekannten Problemen.

- **Passthrough von NetScaler Gateway - geringfügige Änderung des Abmeldeverhaltens**. Wenn Sie zur Authentifizierung ein Passthrough von NetScaler Gateway verwenden und Benutzer sich von der Receiver für Web-Site abmeldet, werden sie jetzt zur NetScaler-Abmeldeseite umgeleitet. Vorher sahen Benutzer möglicherweise ein Authentifizierungsdialogfeld. Das Verhalten der NetScaler-Abmeldeseite hängt von der NetScaler-Konfiguration ab. Beispielsweise kann die Umleitung den Benutzer zur Abmeldeseite des Identitätsanbieters führen oder zu einer Seite, auf der eine einfache Erfolgsmeldung für das Abmelden angezeigt wird.

Wir haben kleinere Updates an folgenden Artikeln vorgenommen:

- Systemanforderungen (Änderungen der Produkt- und Plattformunterstützung)

Behobene Probleme

Jun 04, 2018

Die folgenden Probleme wurden seit Version 3.14 behoben:

- Wenn die Einstellung "Desktop automatisch starten" aktiviert ist, funktioniert das Verhindern mehrfacher Anmeldungen möglicherweise nicht. Infolgedessen schlagen nachfolgende Anforderungen fehl, dieselbe Instanz des Desktops zu starten. [#LC7430]
- Wenn "TWIMode" für einige Anwendungen auf "Aus" gesetzt ist, werden alle Anwendungen im Fenstermodus gestartet, wenn Sie Citrix Receiver für Chrome verwenden. [# LC7558]
- Nach dem Upgrade von StoreFront 2.6, das auf einem nicht standardmäßigen Laufwerk installiert ist, werden die Anwendungsabonnementdaten der Benutzer möglicherweise nicht beibehalten. [#LC8046]
- Wenn zwei oder mehr Stores in StoreFront vorhanden sind, kann durch Klicken auf "Remotezugriffseinstellungen konfigurieren" im ersten oder zweiten Store der Storename des zuletzt hinzugefügten Stores dupliziert werden. [# LC8089]
- Wenn Sie Stores mit gemeinsamer Authentifizierung in StoreFront konfigurieren, können bei dem Versuch, ein neues NetScaler Gateway-Gerät mit einem Store zu verbinden, vorhandene, bereits verbundene NetScaler Gateway-Geräte entfernt werden. Wenn Sie versuchen, sich an den Stores anzumelden, wird die folgende Fehlermeldung angezeigt:

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

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

  "Ein Fehler ist beim Speichern der Änderungen aufgetreten." [#LC8370]
- Dieser Fix behebt ein Netzwerksocketproblem in einer Hintergrundkomponente. [#LC8514]
- Nach dem Neustart der StoreFront MMC-Konsole wird der Wert des Kontrollkästchens **Desktop Viewer anzeigen** möglicherweise nicht korrekt angezeigt. [#LC8520]
- Wenn Sie den Befehl **Set-STFWebReceiverSiteStyle** für ein PNG-Datei ausführen (Transparenz wird unterstützt), um StoreFront anzupassen, wird die PNG-Datei in eine JPEG-Datei konvertiert. Im JPEG-Dateiformat geht möglicherweise die Unterstützung für Transparenz verloren. [# LC8677]
- Wenn Sie den Befehl **Set-STFWebReceiverApplicationShortcuts** ausführen, um die vertrauenswürdigen URLs für Anwendungsverknüpfungen in Citrix Receiver für Web-Sites festzulegen, wird am Ende der URL möglicherweise ein Schrägstrich ("/") hinzugefügt. [# LC8761]

- Wenn Sie den Befehl **Set-STFWebReceiverSiteStyle**verwenden, um StoreFront anzupassen, wird die Datei style.css möglicherweise falsch im Custom-Ordner geändert. Daher kann die StoreFront-Konsole die Anpassung nicht lesen. [# LC8776]
- Auf den StoreFront-Servern kann ein Authentifizierungsfehler auftreten. Das Problem tritt auf, wenn die dynamischen TCP-Ports aufgebraucht sind. [#LC8795]
- Versuche, das StoreFront-Logo mit dem Befehl **Set-STFWebReceiverSiteStyle** zu ändern, schlagen möglicherweise fehl. [#LC8994]
- Wenn **OverrideIcaClientname** aktiviert ist, können Versuche fehlschlagen, eine Remotesitzung vom Remotedesktopclient herzustellen. Das Problem tritt auf, wenn die Lizenz nicht erneuert wird. Eine dieser Fehlermeldungen könnte erscheinen:

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

  ODER

  "The remote session could not be established from remote desktop client WR_XxXXxXXX because its temporary license has expired." [#LC9246]
- StoreFront kann möglicherweise nicht aktualisiert werden, wenn im benutzerdefinierten Dateiverzeichnis einer beliebigen Instanz von Citrix Receiver für Websites schreibgeschützte Dateien vorhanden sind. [#LC9252]
- Wenn Sie während der Einrichtung von XenDesktop eine konfigurierte Site auswählen, wird möglicherweise ein Standardstore in StoreFront erstellt, der den Standardauthentifizierungsdienst verwendet. Wenn Sie diesen Store entfernen, können Benutzer von Citrix Receiver für Windows keine anderen Stores hinzufügen und die folgende Fehlermeldung wird angezeigt:

  "Ein Protokollfehler ist bei der Kommunikation mit dem Authentifizierungsdienst aufgetreten." [#LC9404]
- Versuche, sich bei StoreFront anzumelden, führen möglicherweise zu dem Fehler **Ihre Anforderung kann nicht abgeschlossen werden**. [# LC9521]
- Wenn Sie das StoreFront SDK zum Anpassen bestimmter Funktionen verwenden und die Aggregation des Stores konfigurieren, führt die Anmeldung möglicherweise zu dem Fehler **Ihre Anforderung kann nicht abgeschlossen werden**. Das Problem tritt auf, wenn die veröffentlichten Anwendungen benutzerdefinierte Symbole mit minimalen Auflösungen haben. [# LC9561]

Bekannte Probleme

Feb 26, 2018

In diesem Release bestehen die folgenden Probleme.

- Das Verbinden von Servergruppen funktioniert nicht, wenn TLS 1.0 auf einem Server mit .NET 4.6.1 oder früher deaktiviert ist. Um dieses Problem zu umgehen, führen Sie ein Upgrade auf .NET 4.6.2 oder höher durch.

  [# STF-687]

- Wenn StoreFront ursprünglich über die ausführbare Datei auf dem Installationsmedium installiert wurde, wird es, wenn Sie später das Komplettinstallationsprogramm für eine neuere Version verwenden, nicht als aktualisierbar angezeigt. Aktualisieren Sie StoreFront als Workaround über die ausführbare Datei auf dem Installationsmedium.

  [# DNA-47816]

- Es ist ein bekanntes Drittanbieterproblem mit Smartcardauthentifizierung und Microsoft Edge. Zur Problemvermeidung verwenden Sie Internet Explorer.

  [# #DNA 47809]

- Gelegentlich (beobachtet, wenn der Windows CEIP-Prozess nachts ausgeführt wird) gibt es ein StoreFront-Upgradeproblem während eines Upgrades von Delivery Controller Version 7.12 oder höher. Die folgende Fehlermeldung wird angezeigt:

  > StoreFront kann nicht aktualisiert werden, weil das folgende Programm Dateien verwendet. Schließen Sie das Programm und versuchen Sie es erneut.
  > Programmname: CompatTelRunner

  Um dieses Problem zu umgehen, folgen Sie den Anweisungen auf dem Bildschirm.

  [# DNA-51341]

- Bei der Wiederverbindung stellt Workspace Control die Verbindung nur zu einer App-Sitzung und nicht zu allen Apps im Workspace wieder her. Dieses Problem tritt auf, wenn der Zugriff auf die Receiver für Web-Site in Chrome erfolgt. Um dieses Problem zu umgehen, klicken Sie für jede getrennte App auf "Verbinden".

  [# DNA-25140, # DNA-22561]

Hinweise zu Drittanbietern

Jun 04, 2018

StoreFront enthält ggf. Software von Drittanbietern, die gemäß den im folgenden Dokument aufgeführten Bestimmungen lizenziert ist:

PDF StoreFront Hinweise zu Drittanbietern

Systemanforderungen

Jun 04, 2018

Beim Planen der Installation empfiehlt Citrix, mindestens 2 GB zusätzlichen RAM für StoreFront über die Anforderungen aller anderen, auf dem Server installierten Produkte hinaus zu veranschlagen. Der Abonnementstoredienst erfordert mindestens 5 MB Speicherplatz und pro 1000 Anwendungsabonnements sind zusätzlich ca. 8 MB Speicherplatz erforderlich. Alle anderen Hardwareelemente müssen die Mindestanforderungen an die Hardware für das installierte Betriebssystem erfüllen.

Nach entsprechenden Tests bietet Citrix nun Unterstützung für StoreFront auf folgenden Plattformen:

- Windows Server 2016 (Datacenter- und Standard-Editionen)
- Windows Server 2012 R2 Datacenter- und Standard-Editionen

Das Aktualisieren des Betriebssystems eines Servers, auf dem StoreFront ausgeführt wird, wird nicht unterstützt. Citrix empfiehlt die Installation von StoreFront auf einer neuen Installation des Betriebssystems. Auf allen Servern in einer Multiserverbereitstellung muss die gleiche Betriebssystemversion mit den gleichen Gebietsschemaeinstellungen ausgeführt werden. StoreFront-Servergruppen mit unterschiedlichen Betriebssystemversionen und Gebietsschemas werden nicht unterstützt. Zwar kann eine Servergruppe maximal sechs Server enthalten, basierend auf Simulationen bieten Servergruppen mit mehr als drei Servern jedoch für die Kapazität keinen Vorteil. Alle Server in einer Servergruppe müssen sich am gleichen Ort befinden.

Microsoft Internetinformationsdienste (IIS) und Microsoft .NET Framework sind auf dem Server erforderlich. Wenn eine dieser beiden erforderlichen Komponenten installiert, aber nicht aktiviert ist, aktiviert das StoreFront-Installationsprogramm die Komponente, bevor das Produkt installiert wird. Windows PowerShell und Microsoft Management Console, beides Standardkomponenten von Windows Server, müssen auf dem Webserver installiert werden, bevor Sie StoreFront installieren können. Der relative Pfad zu StoreFront in IIS muss auf allen Servern in einer Gruppe identisch sein.

Das StoreFront-Installationsprogramm fügt die erforderlichen IIS-Features hinzu. Liste der Anforderungen, falls Sie diese Features vorinstallieren:

Alle Plattformen:

- Web-Static-Content
- Web-Default-Doc
- Web-Http-Errors
- Web-Http-Redirect
- Web-Http-Logging
- Web-Mgmt-Console
- Web-Scripting-Tools
- Web-Windows-Auth
- Web-Basic-Auth
- Web-AppInit

Unter Windows Server 2012 R2:

- Web-Asp-Net45
- Net-Wcf-Tcp-PortSharing45

Unter Windows Server 2016

- Web-Asp-Net45
- Net-Wcf-Tcp-PortSharing45

StoreFront verwendet die folgenden Ports für die Kommunikation. Stellen Sie sicher, dass Firewalls und andere Netzwerkgeräte den Zugriff auf diese Ports zulassen.

- Die TCP-Ports 80 und 443 werden für die Kommunikation über HTTP bzw. HTTPS verwendet und müssen von innerhalb und außerhalb des Unternehmensnetzwerks zugänglich sein.
- TCP-Port 808 wird für die Kommunikation zwischen StoreFront-Servern verwendet und muss von innerhalb des Unternehmensnetzwerks zugänglich sein.
- Ein nach dem Zufallsprinzip unter allen nicht reservierten Ports ausgewählter TCP-Port wird für die Kommunikation zwischen den StoreFront-Servern in eine Servergruppe verwendet. Wenn Sie StoreFront installieren, wird eine Windows-Firewallregel konfiguriert, die den Zugriff auf die ausführbare StoreFront-Datei gestattet. Da der Port jedoch nach dem Zufallsprinzip zugewiesen wird, müssen Sie sicherstellen, dass Firewalls oder andere Geräte im internen Netzwerk keinen Datenverkehr an einen der nicht zugewiesenen TCP-Ports blockieren.
- Wenn er aktiviert ist, wird TCP-Port 8008 von Citrix Receiver für HTML5 für die Kommunikation zwischen lokalen Benutzern im internen Netzwerk und den Servern, die die Desktops und Anwendungen bereitstellen, verwendet.

StoreFront unterstützt reine IPv6-Netzwerke und Umgebungen mit dualem Stapel (IPv4 und IPv6).

Anforderungen an die Infrastruktur

Citrix hat StoreFront mit den folgenden Citrix Produktversionen getestet und unterstützt sie.

Anforderungen für den Citrix Server

In StoreFront-Stores aggregierte Desktops und Anwendungen von den folgenden Produkten.

- XenApp und XenDesktop 7.18
- XenApp und XenDesktop 7.17
- XenApp und XenDesktop 7.16
- XenApp und XenDesktop 7.15
- XenApp und XenDesktop 7.14
- XenApp und XenDesktop 7.13
- XenApp und XenDesktop 7.12
- XenApp und XenDesktop 7.11
- XenApp und XenDesktop 7.9
- XenApp und XenDesktop 7.8
- XenApp und XenDesktop 7.7
- XenApp und XenDesktop 7.6
- XenApp und XenDesktop 7.5
- XenDesktop 7.1
- XenDesktop 7
- XenApp 6.5

Anforderungen für NetScaler Gateway

Die folgenden Versionen von NetScaler Gateway können verwendet werden, um Benutzern in öffentlichen Netzwerken

Zugriff auf StoreFront zu geben.

- NetScaler Gateway 12.0
- NetScaler Gateway 11.*x*
- NetScaler Gateway 10.5

Anforderungen für Citrix Receiver für HTML5

Wenn Sie beabsichtigen, Benutzern den Zugriff auf Desktops und Anwendungen mit Citrix Receiver für HTML5 auf Receiver für Web-Sites zu ermöglichen, gelten die folgenden zusätzlichen Anforderungen.

Bei internen Netzwerkverbindungen bietet Citrix Receiver für HTML5 den Zugriff auf Desktops und Anwendungen der folgenden Produkte.

- XenApp und XenDesktop 7.18
- XenApp und XenDesktop 7.17
- XenApp und XenDesktop 7.16
- XenApp und XenDesktop 7.15
- XenApp und XenDesktop 7.14
- XenApp und XenDesktop 7.13
- XenApp und XenDesktop 7.12
- XenApp und XenDesktop 7.11
- XenApp und XenDesktop 7.9
- XenApp und XenDesktop 7.8
- XenApp und XenDesktop 7.7
- XenApp und XenDesktop 7.6
- XenApp und XenDesktop 7.5
- XenDesktop 7.1
- XenDesktop 7
- XenApp 6.5 Feature Pack 2
- XenApp 6.5 Feature Pack 1 für Windows Server 2008 R2 (erfordert Hotfix XA650R01W2K8R2X64051, verfügbar unter http://support.citrix.com/article/CTX136293)

Remotebenutzern außerhalb des Unternehmensnetzwerks ermöglicht Citrix Receiver für HTML5 den Zugriff auf Desktops und Anwendungen über die folgenden NetScaler Gateway-Versionen.

- NetScaler Gateway 12.0
- NetScaler Gateway 11.*x*

Bei Verbindungen über NetScaler Gateway bietet Citrix Receiver für HTML5 den Zugriff auf Desktops und Anwendungen folgender Produkte.

- XenApp und XenDesktop 7.18
- XenApp und XenDesktop 7.17
- XenApp und XenDesktop 7.16
- XenApp und XenDesktop 7.15
- XenApp und XenDesktop 7.14
- XenApp und XenDesktop 7.13
- XenApp und XenDesktop 7.12

- XenApp und XenDesktop 7.11
- XenApp und XenDesktop 7.9
- XenApp und XenDesktop 7.8
- XenApp und XenDesktop 7.7
- XenApp und XenDesktop 7.6
- XenApp und XenDesktop 7.5
- XenDesktop 7.1
- XenDesktop 7
- XenApp 6.5

Anforderungen für Benutzergeräte

StoreFront bietet Benutzern verschiedene Optionen für den Zugriff auf Desktops und Anwendungen. Citrix Receiver-Benutzer können entweder über Citrix Receiver auf Stores zugreifen oder einen Webbrowser verwenden, um sich bei einer Citrix Receiver für Web-Site für den Store anzumelden. Benutzern, die Citrix Receiver nicht installieren können, jedoch einen HTML5-kompatiblen Webbrowser haben, können Sie direkten Zugriff auf Desktops und Anwendungen im Webbrowser ermöglichen, indem Sie Citrix Receiver für HTML5 für Ihre Citrix Receiver für Web-Site aktivieren.

Benutzer mit nicht domänengebundenen Desktopgeräten können auf ihre Desktops über ihren Webbrowser zugreifen, der für den Zugriff auf Desktopgerätesites konfiguriert ist. Benutzer von domänengebundenen Desktopgeräten und umfunktionierten PCs, auf denen Citrix Desktop Lock ausgeführt wird, sowie Benutzer mit älteren Citrix Clients, die nicht aktualisiert werden können, können über die XenApp-Services-URL direkt auf Stores zugreifen.

Wenn Sie Offlineanwendungen bereitstellen möchten, ist neben Citrix Receiver für Windows auch das Offline Plug-In erforderlich. Wenn Sie Microsoft Application Virtualization (App-V)-Sequenzen für Benutzer bereitstellen möchten, wird außerdem eine unterstützte Version von Microsoft Application Virtualization Desktop Client benötigt. Weitere Informationen hierzu finden Sie unter Verwalten gestreamter Anwendungen. Benutzer können nicht über Citrix Receiver für Web-Sites auf Offlineanwendungen oder App-V-Sequenzen zugreifen.

Es wird vorausgesetzt, dass alle Benutzergeräte die Mindestanforderungen an die Hardware für das installierte Betriebssystem erfüllen.

Anforderungen für Citrix Receiver-fähige Stores

Die folgenden Citrix Receiver-Versionen können für den Zugriff auf StoreFront-Stores über interne Netzwerkverbindungen und über NetScaler Gateway verwendet werden. Verbindungen über NetScaler Gateway können mit dem NetScaler Gateway Plug-In und/oder über clientlosen Zugriff hergestellt werden. Citrix Receiver für Windows 4.5 ist die mindestens erforderliche Version für die einheitliche Receiver-Benutzeroberfläche unter StoreFront. Siehe Unterstützung der einheitlichen Receiver-Benutzeroberfläche.

- Citrix Receiver für Chrome 2.x
- Citrix Receiver für HTML5 2.x
- Citrix Receiver für Mac 12.x
- Citrix Receiver für Windows 4.x
- Citrix Receiver für Linux 13.x

Anforderungen für den Zugriff auf Stores über Citrix Receiver für Web-Sites

Die folgenden Kombinationen aus Citrix Receiver, Betriebssystem und Webbrowser werden für den Zugriff auf Citrix

Receiver für Web-Sites über interne Netzwerkverbindungen und NetScaler Gateway empfohlen. Verbindungen über NetScaler Gateway können mit dem NetScaler Gateway Plug-In oder über clientlosen Zugriff hergestellt werden.

Sofern nicht anders angegeben, werden die neuesten Browserversionen empfohlen.

- Citrix Receiver für Windows 4.5 und höher bis Citrix Receiver für Windows 4.12
  - Windows 10 (32-Bit- und 64-Bit-Edition)
    - Microsoft Edge
    - Internet Explorer 11
    - Google Chrome
    - Mozilla Firefox
  - Windows 8.1 (32- und 64-Bit-Edition)
    - Internet Explorer 11 (32-Bit-Modus)
    - Google Chrome
    - Mozilla Firefox
  - Windows 8 (32-Bit- und 64-Bit-Edition)
    - Internet Explorer 10 (32-Bit-Modus)
    - Google Chrome
    - Mozilla Firefox
  - Windows 7 mit Service Pack 1 (32-Bit- und 64-Bit-Editionen)
    - Internet Explorer 11, 10, 9
    - Google Chrome
    - Mozilla Firefox
  - Windows Embedded Standard 7 Service Pack 1 oder Windows Thin PC
    - Internet Explorer 11, 10, 9
- Citrix Receiver für Mac 12.0
  - Mac OS X 10.11 El Capitan
    - Safari 9
    - Google Chrome
    - Mozilla Firefox
  - Mac OS X 10.10 Yosemite
    - Safari 8
    - Google Chrome
    - Mozilla Firefox
  - Mac OS X 10.9 Mavericks
    - Safari 7
    - Google Chrome
    - Mozilla Firefox
- Citrix Receiver für Linux 13.x
  - Ubuntu 12.04 (32-Bit) und 14.04 LTS (32-Bit)
    - Google Chrome
    - Mozilla Firefox

Anforderungen für den Zugriff auf Desktops und Anwendungen über Receiver für HTML5

Die folgenden Betriebssysteme und Webbrowser werden für den Zugriff auf Desktops und Anwendungen mit Receiver für HTML5 auf Receiver für Web-Sites empfohlen. Es werden sowohl interne Netzwerkverbindungen als auch Verbindungen über NetScaler Gateway unterstützt. Bei Verbindungen über das interne Netzwerk unterstützt Receiver für HTML5 allerdings nur den Zugriff auf Ressourcen, die von bestimmten Produkten bereitgestellt werden. Außerdem sind bestimmte Versionen von NetScaler Gateway erforderlich, um Verbindungen von außerhalb des Unternehmensnetzwerks zu ermöglichen. Weitere Informationen finden Sie unter Anforderungen an die Infrastruktur.

Sofern nicht anders angegeben, werden die neuesten Browserversionen empfohlen.

- Browser
  - Microsoft Edge
  - Internet Explorer 11
  - Safari 7
  - Google Chrome
  - Mozilla Firefox
- Betriebssysteme
  - Windows 10 (32-Bit- und 64-Bit-Edition)
  - Windows 8.1 (32- und 64-Bit-Edition)
  - Windows 8 (32-Bit- und 64-Bit-Edition)
  - Windows 7 mit Service Pack 1 (32-Bit- und 64-Bit-Editionen)
  - Windows Vista mit Service Pack 2 (32-Bit- und 64-Bit-Editionen)
  - Windows Embedded XP
  - Mac OS X 10.10 Yosemite
  - Mac OS X 10.9 Mavericks
  - Mac OS X 10.8 Mountain Lion
  - Google Chrome OS 48
  - Google Chrome OS 47
  - Ubuntu 12.04 (32 Bit)

Anforderungen für den Zugriff auf Stores über Desktopgerätesites

Die folgenden Kombinationen aus Citrix Receiver, Betriebssystem und Webbrowser werden für den Zugriff auf Desktopgerätesites über interne Netzwerkverbindungen empfohlen. Verbindungen über NetScaler Gateway werden nicht unterstützt.

- Citrix Receiver für Windows 4.5
  - Windows 8.1 (32- und 64-Bit-Edition)
    - Internet Explorer 11 (32-Bit-Modus)
  - Windows 8 (32-Bit- und 64-Bit-Edition)
    - Internet Explorer 10 (32-Bit-Modus)
  - Windows 7 Service Pack 1 (32-Bit- und 64-Bit-Edition), Windows Embedded Standard 7 Service Pack 1 oder Windows Thin PC
    - Internet Explorer 9 (32-Bit-Modus)
    - Internet Explorer 8 (32-Bit-Modus)
  - Windows Embedded XP
    - Internet Explorer 8 (32-Bit-Modus)

Anforderungen für den Zugriff auf Stores über XenApp Services-URLs

Alle o. g. Versionen von Citrix Receiver können für den Zugriff auf StoreFront-Stores mit reduziertem Funktionsumfang über XenApp Services-URLs verwendet werden. Verbindungen über NetScaler Gateway, sofern unterstützt, können mit dem NetScaler Gateway Plug-In oder über clientlosen Zugriff hergestellt werden.

Anforderungen für Smartcards

Anforderungen für die Verwendung von Citrix Receiver für Windows 4.X mit Smartcards

Citrix testet die Kompatibilität mit folgenden Smartcards: CAC (Common Access Card, US-Behörden), NIST PIV (National Institute of Standards and Technology Personal Identity Verification, USA) und diverse USB-Smartcardtoken. Sie können Kontaktkartenleser verwenden, die mit der Spezifikation "USB Chip/Smart Card Interface Devices" (CCID) übereinstimmen und vom deutschen Zentralen Kreditausschuss (ZKA) als Klasse 1-Smartcardleser klassifiziert wurden. Bei ZKA Klasse 1-Kontaktkartenlesern müssen Benutzer die Smartcards in den Leser einlegen. Andere Smartcardleser, einschließlich Klasse 2-Leser (mit Tastatur für die PIN-Eingabe), kontaktlose Leser und virtuelle TPM-Chip-basierte (Trusted Platform Module) Smartcards werden nicht unterstützt.

Für Windows-Geräte basiert die Smartcard-Unterstützung auf dem PC/SC-Standard (Personal Computer/Smart Card) von Microsoft. Als Mindestanforderung müssen Smartcards und Smartcardleser vom Betriebssystem unterstützt werden und über die Windows-Hardwarezertifizierung verfügen.

Weitere Informationen über Citrix-kompatible Smartcards und Middleware finden Sie unter Smartcards in der XenApp- und XenDesktop-Dokumentation und unter http://www.citrix.com/ready.

Anforderungen für die Authentifizierung über NetScaler Gateway

Die folgenden Versionen von NetScaler Gateway können verwendet werden, um Benutzern in öffentlichen Netzwerken den Zugriff auf StoreFront mit Smartcardauthentifizierung zu ermöglichen.

- NetScaler Gateway 12.0
- NetScaler Gateway 11.x
- NetScaler Gateway 10.5

Planen der StoreFront-Bereitstellung

Nov 27, 2017

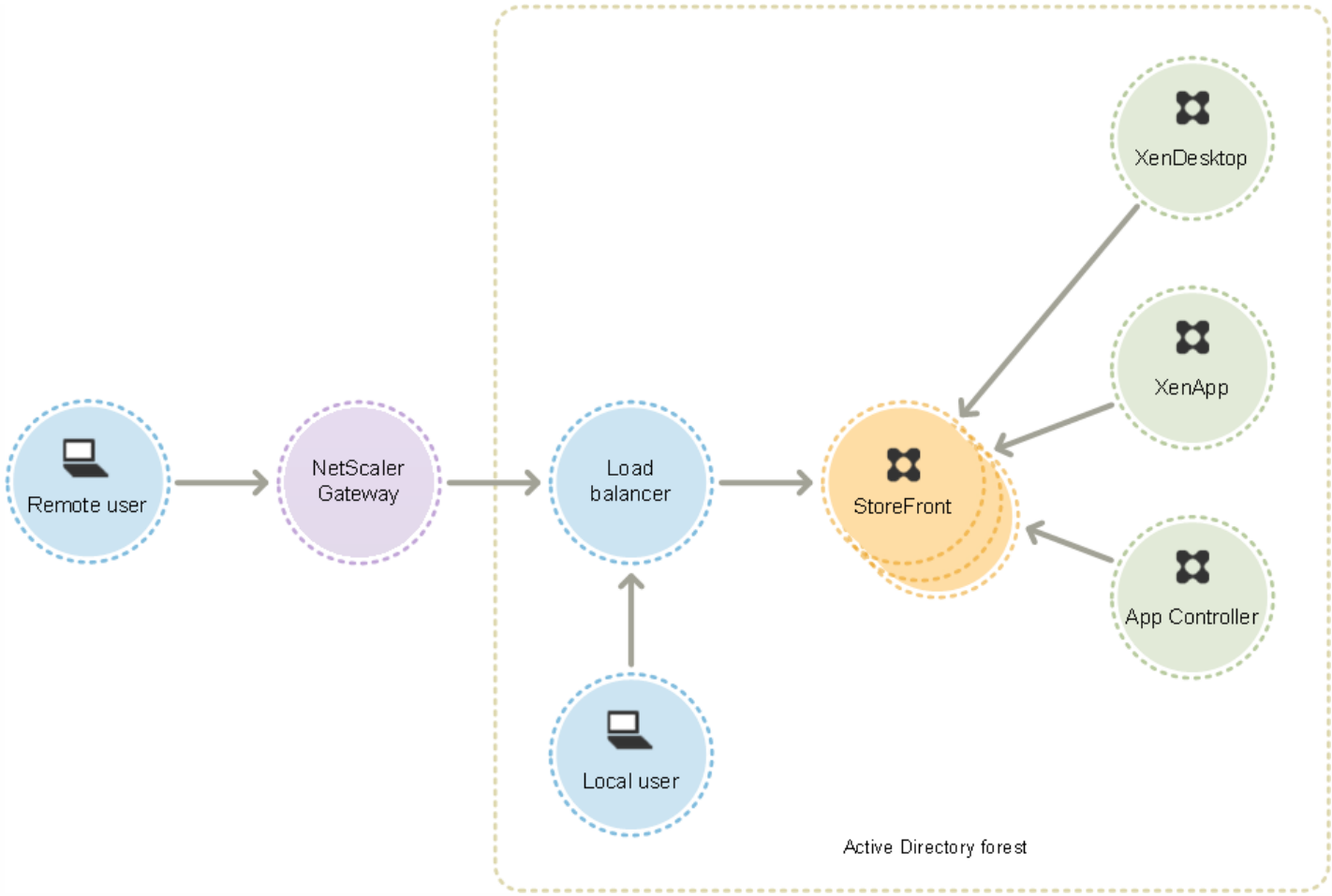
StoreFront nutzt Microsoft .NET-Technologie, die auf Microsoft Internetinformationsdienste (IIS) ausgeführt wird, zur Bereitstellung von Unternehmens-App-Stores, in denen Ressourcen zusammengefasst und Benutzern zur Verfügung gestellt werden. StoreFront kann in Ihre XenDesktop-, XenApp- und VDI-in-a-Box-Bereitstellungen integriert werden und bietet Benutzern einen zentralen Self-Service-Zugriffspunkt für ihre Desktops und Anwendungen.

StoreFront umfasst die folgenden Kernkomponenten:

- Der Authentifizierungsdienst authentifiziert Benutzer mit Microsoft Active Directory und stellt auf diese Weise sicher, dass Benutzer sich nicht erneut anmelden müssen, um auf ihre Desktops und Anwendungen zuzugreifen. Weitere Informationen finden Sie unter Benutzerauthentifizierung.
- In Stores werden Desktops und Anwendungen von XenDesktop, XenApp und App Controller aufgelistet und zusammengefasst. Benutzer greifen auf Stores über Citrix Receiver, Citrix Receiver für Web-Sites, Desktopgerätesites und XenApp Services-URLs zu. Weitere Informationen finden Sie unter Benutzerzugriffsoptionen.
- Vom Abonnementstoredienst werden Informationen zu Anwendungsabonnements von Benutzern aufgezeichnet und deren Geräte aktualisiert, damit ein konsistentes Roamingverhalten gewährleistet ist. Weitere Informationen zum Optimieren der Benutzererfahrung finden Sie unter Optimieren der Benutzererfahrung.

StoreFront kann auf einem einzelnen Server oder als Multiserverbereitstellung konfiguriert werden. Multiserverbereitstellungen bieten nicht nur zusätzliche Kapazität, sondern auch höhere Verfügbarkeit. Die modulare Architektur von StoreFront stellt sicher, dass die Konfigurationsinformationen und Details zu den Anwendungsabonnements der Benutzer auf allen Servern in einer Servergruppe gespeichert und repliziert werden. Wenn ein StoreFront-Server aus irgendeinem Grund nicht verfügbar ist, können Benutzer weiter auf ihre Stores auf den übrigen Servern zugreifen. Die Konfigurations- und Abonnementsdaten auf dem ausgefallenen Server werden automatisch aktualisiert, wenn er wieder mit der Servergruppe verbunden wird. Abonnementdaten werden aktualisiert, wenn der Server wieder online geht, Sie müssen jedoch Konfigurationsänderungen verteilen, die vom Server verpasst wurden. Falls aufgrund eines Hardwarefehlers der Server ersetzt werden muss, installieren Sie StoreFront auf einem neuen Server und fügen ihn der vorhandenen Servergruppe hinzu. Der neue Server wird automatisch konfiguriert und mit den Anwendungsabonnements der Benutzer aktualisiert, wenn er der Servergruppe beitritt.

Die Abbildung zeigt eine typische StoreFront-Bereitstellung.



Load Balancing

Bei Multiserverbereitstellungen ist ein externer Lastausgleich, z. B. über NetScaler oder Windows-Netzwerklastenausgleich erforderlich. Konfigurieren Sie die Lastausgleichsumgebung für Failover zwischen den Servern, um eine fehlertolerante Bereitstellung zu ermöglichen. Weitere Informationen über den Lastausgleich mit NetScaler finden Sie unter Lastausgleich. Weitere Informationen über den Windows-Netzwerklastenausgleich finden Sie unter http://technet.microsoft.com/de-de/library/hh831698.aspx.

Aktiver Lastausgleich von Anfragen, die von StoreFront an XenDesktop-Sites und XenApp-Farmen gesendet werden, ist für Bereitstellungen mit Tausenden von Benutzern empfehlenswert oder wenn hohe Lasten auftreten, z. B. wenn eine große Anzahl von Benutzern sich in kurzer Zeit anmeldet. Verwenden Sie einen Load Balancer mit integrierten XML-Monitoren und Sitzungspersistenz, z. B. NetScaler.

Wenn Sie einen Load Balancer mit SSL-Terminierung einsetzen oder zur Problembehandlung können Sie das PowerShell-Cmdlet **Set-STFWebReceiverCommunication** verwenden.

Syntax:

Set-STFWebReceiverCommunication [-WebReceiverService] [[-Loopback]] [[-LoopbackPortUsingHttp]]

Gültige Werte sind die Folgenden:

- **On**: Dies ist der Standardwert für neue Citrix Receiver für Web-Sites. Citrix Receiver für Web verwendet das Schema (HTTPS oder HTTP) und die Portnummer der Basis-URL, ersetzt jedoch den Host mit der Loopback-IP-Adresse, um mit den StoreFront-Diensten zu kommunizieren. Dieskann bei Einzelserverbereitstellungen und bei Bereitstellungen mit einem

Load Balancer ohne SSL-Terminierung eingesetzt werden.

- **OnUsingHttp**: Citrix Receiver für Web verwendet HTTP und die Loopback-IP-Adresse zum Kommunizieren mit den StoreFront-Diensten. Wenn Sie einen Load Balancer mit SSL-Terminierung verwenden, wählen Sie diesen Wert. Sie müssen zudem den HTTP-Port angeben, wenn nicht der Standardport 80 verwendet wird.
- **Off**: Dieser Wert deaktiviert Loopback, und Citrix Receiver für Web verwendet die StoreFront-Basis-URL für die Kommunikation mit den StoreFront-Diensten. Wenn Sie ein direktes Upgrade durchführen, ist dies der Standardwert, mit dem Unterbrechungen der bestehenden Bereitstellung verhindert werden.

Wenn Sie beispielsweise einen Load Balancer mit SSL-Terminierung verwenden, IIS zur Nutzung von Port 81 für HTTP konfiguriert ist und der Pfad der Citrix Receiver für Web-Site /Citrix/StoreWeb ist, können Sie die Citrix Receiver für Web-Site mit folgendem Befehl konfigurieren:

```
$wr = Get-STFWebReceiverService -VirtualPath /Citrix/StoreWeb
Set-STFWebReceiverCommunication -WebReceiverService $wr -Loopback OnUsingHttp -LoopbackPortUsingHttp 81
```

Sie müssen Loopback deaktivieren, wenn Sie ein Webproxy-Tool wie Fiddler verwenden, um den Netzwerkverkehr zwischen Citrix Receiver für Web und den StoreFront-Diensten zu erfassen.

Überlegungen zu Active Directory

Für Einzelserverbereitstellungen können Sie StoreFront auf einem Server installieren, der nicht in einer Domäne ist (bestimmte Funktionen stehen dann aber nicht zur Verfügung). Sonst müssen StoreFront-Server in der Active Directory-Domäne mit den Benutzerkonten residieren oder in einer Domäne, die mit dieser eine Vertrauensstellung hat, außer Sie aktivieren die Delegierung der Authentifizierung an die XenApp- und XenDesktop-Sites bzw. -Farmen. Alle StoreFront-Server einer Gruppe müssen in der gleichen Domäne sein.

Benutzerverbindungen

In einer Produktionsumgebung empfiehlt Citrix die Verwendung von HTTPS, um den Datenverkehr zwischen StoreFront und Benutzergeräten sicher zu gestalten. Damit HTTPS verwendet werden kann, müssen die IIS-Instanz, auf der der Authentifizierungsdienst gehostet wird, und zugeordnete Stores für HTTPS konfiguriert sein. Wenn die entsprechende IIS-Konfiguration nicht verfügbar ist, verwendet StoreFront HTTP für die Kommunikation. Sie können jederzeit von HTTP zu HTTPS wechseln, vorausgesetzt, die entsprechende IIS-Konfiguration ist vorhanden.

Wenn Sie beabsichtigen, Zugriff auf StoreFront von außerhalb des Unternehmensnetzwerks zu ermöglichen, ist NetScaler Gateway erforderlich, um sichere Verbindungen für Remotebenutzer zu gewährleisten. Stellen Sie NetScaler Gateway außerhalb des Unternehmensnetzwerks bereit und trennen Sie NetScaler Gateway vom öffentlichen und internen Netzwerk durch Firewalls. Stellen Sie sicher, dass NetScaler Gateway auf die Active Directory-Gesamtstruktur mit den StoreFront-Servern zugreifen kann.

Mehrere Internetinformationsdienste- (IIS)-Websites

StoreFront ermöglicht das Bereitstellen von unterschiedlichen Stores in verschiedenen IIS-Websites per Windows-Server, sodass jeder Store einen anderen Hostnamen und eine Zertifikatbindung haben kann.

Erstellen Sie zwei weitere Websites zusätzlich zur Standardwebsite. Wenn Sie mehrere Websites in IIS erstellt haben, können Sie mit dem PowerShell SDK eine StoreFront-Bereitstellung in jeder dieser IIS-Websites erstellen. Weitere Informationen über das Erstellen von Websites in IIS finden Sie unter How to set up your first IIS Website.

Hinweis: Die StoreFront- und PowerShell-Konsolen können nicht gleichzeitig geöffnet sein. Schließen Sie immer zuerst die

StoreFront-Verwaltungskonsole, bevor Sie die PowerShell-Konsole zum Verwalten der StoreFront-Konfiguration öffnen. Schließen Sie gleichermaßen immer alle Instanzen von PowerShell, bevor Sie die StoreFront-Konsole öffnen.

Beispiel: Erstellen von zwei IIS-Websitebereitstellungen - eine für Anwendungen und eine für Desktops.

1. Add-STFDeployment -SiteID 1 -HostBaseURL "https://www.storefront.app.com"
2. Add-STFDeployment -SiteID 2 -HostBaseURL "https://www.storefront.desktop.com"

StoreFront deaktiviert die Verwaltungskonsole, wenn mehrere Sites erkannt werden, und zeigt eine entsprechende Meldung an.

Weitere Informationen finden Sie unter Vorbereiten der Installation.

Skalierbarkeit

Die Anzahl der Citrix Receiver-Benutzer, die von einer StoreFront-Servergruppe unterstützt werden, hängt von der verwendeten Hardware und dem Grad der Benutzeraktivität ab. Annahme: Benutzer melden sich an, enumerieren 100 veröffentlichte Anwendungen und starten eine Ressource. In diesem Szenario kann ein einzelner StoreFront-Server mit der mindestens empfohlenen Ausstattung von zwei virtuellen CPUs, die auf einem Server mit Dual Intel Xeon L5520 2.27Ghz-Prozessor ausgeführt werden, bis zu 30.000 Benutzerverbindungen pro Stunde ermöglichen.

Sie können erwarten, dass eine Servergruppe mit zwei ähnlich konfigurierten Servern in der Gruppe bis zu 60.000 Benutzerverbindungen pro Stunde ermöglichen kann; drei Knoten bis zu 90.000 Verbindungen pro Stunde; vier Knoten bis zu 120.000 Verbindungen pro Stunde; fünf Knoten bis zu 150.000 Verbindungen pro Stunde; sechs Knoten bis zu 175.000 Knoten pro Stunde.

Der Durchsatz eines einzelnen StoreFront-Servers kann auch dadurch erhöht werden, dass dem System mehr virtuelle CPUs zugewiesen werden. Wobei vier virtuelle CPUs bis zu 55.000 Benutzerverbindungen pro Stunde ermöglichen und acht virtuelle CPUs bis zu 80.000 Verbindungen pro Stunde.

Die mindestens empfohlene Speichermenge für jeden Server ist 4 GB. Wenn Sie Citrix Receiver für Web verwenden, sollten Sie zusätzlich zu der Basisspeichermenge 700 Byte pro Benutzer pro Ressource zuweisen.Wie bei Web Receiver sollten Sie für Citrix Receiver beim Entwerfen von Umgebungen zusätzlich zu der Basisspeichermenge von 4 GB für diese Version von StoreFront weitere 700 Bytes pro Benutzer pro Ressource einplanen.

Da sich Ihr Nutzungsmuster von den Simulationen ggf. unterscheidet, unterstützen Ihre Server u. U. mehr oder weniger Benutzerverbindungen pro Stunde.

Wichtig: Alle Server in einer Servergruppe müssen sich am gleichen Ort befinden. StoreFront-Servergruppen mit unterschiedlichen Betriebssystemversionen und Gebietsschemas werden nicht unterstützt.

Überlegungen zu Timeouts

Netzwerk- oder andere Probleme zwischen StoreFront und den von StoreFront angesprochenen Servern können Verzögerungen oder Fehler für Benutzer verursachen. Sie können die Timeouteinstellungen für einen Store verwenden, um dieses Verhalten zu steuern. Wenn Sie ein kurzes Timeout festlegen, verlässt StoreFront einen Server schnell und versucht es mit einem anderen. Dies ist nützlich, wenn Sie z. B. mehrere Server für Failoverzwecke konfiguriert haben.

Wenn Sie ein längeres Timeout festlegen, wartet StoreFront länger auf eine Antwort von einem Server. Dies ist nützlich in Umgebungen, in denen Netzwerk oder Server unzuverlässig sind und Verzögerungen häufig vorkommen.

Citrix Receiver für Web hat auch eine Timeouteinstellung, die festlegt, wie lange eine Citrix Receiver für Web-Site auf eine Antwort vom Store wartet. Legen Sie für dieses Einstellung ein Timeout fest, das mindestens so lang ist, wie das

Storetimeout. Ein längerer Timeoutwert bietet eine bessere Fehlertoleranz, kann aber für Benutzer lange Verzögerungen bedeuten. Ein kürzeres Timeout verringert Verzögerungen für Benutzer, kann aber mehr Fehler bedeuten.

Weitere Informationen zur Einstellung von Timeouts finden Sie Kommunikationstimeoutdauer und Serverwiederholungsversuche und Kommunikationstimeoutdauer und Wiederholungsversuche.

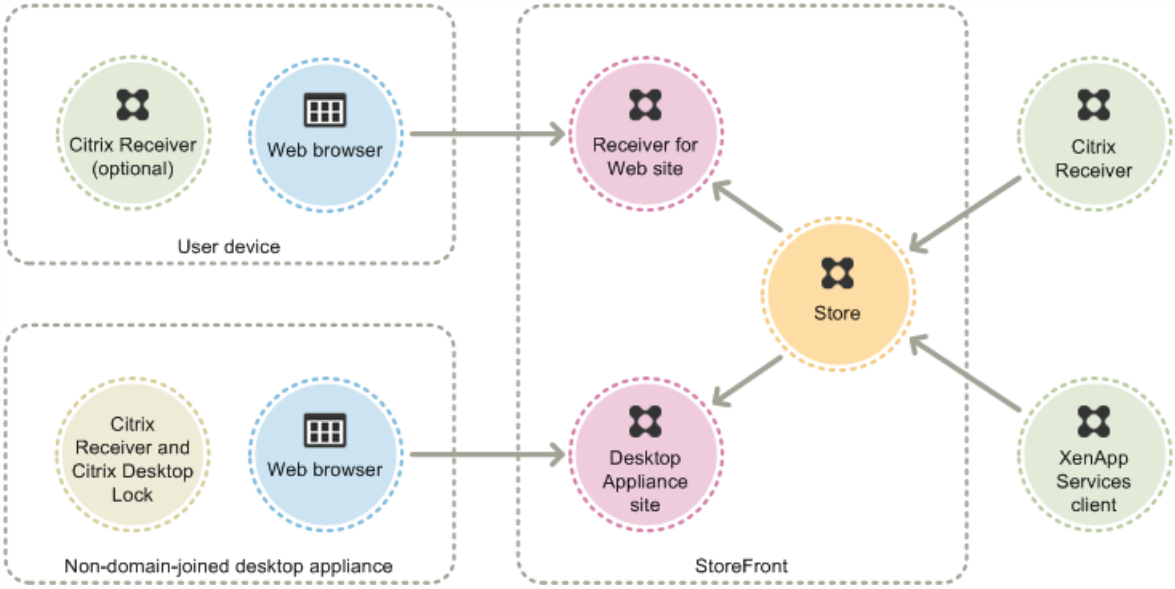
Benutzerzugriffsoptionen

Jun 04, 2018

Es gibt vier verschiedene Methoden, wie Benutzer auf StoreFront-Stores zugreifen können.

- Citrix Receiver: Benutzer mit kompatiblen Versionen von Citrix Receiver können direkt von der Citrix Receiver-Benutzeroberfläche auf StoreFront-Stores zugreifen. Direkter Zugriff auf Stores innerhalb von Citrix Receiver bietet die beste Benutzererfahrung und den größten Funktionsumfang.
- Citrix Receiver für Web-Sites: Benutzer mit kompatiblen Webbrowsern können auf StoreFront-Stores zugreifen, indem sie zu Citrix Receiver für Web-Sites navigieren. Benutzer benötigen standardmäßig auch eine kompatible Version von Citrix Receiver, um auf ihre Desktops und Anwendungen zuzugreifen. Sie können Citrix Receiver für Web-Sites jedoch so konfigurieren, dass Benutzer mit HTML5-kompatiblen Browsern auf ihre Ressourcen zugreifen können, ohne Citrix Receiver zu installieren. Bei der Erstellung eines neuen Stores wird standardmäßig eine Citrix Receiver für Web-Site für den Store erstellt.
- Desktopgerätesites: Benutzer mit nicht domänengebundenen Desktopgeräten können auf ihre Desktops über Webbrowser auf ihren Geräten zugreifen, die so konfiguriert sind, dass sie Desktopgerätesites im Vollbildmodus anzeigen. Wenn Sie mit Citrix Studio einen neuen Store für eine XenDesktop-Bereitstellung erstellen, wird standardmäßig eine Desktopgerätesite für den Store erstellt.
- XenApp Services-URLs: Benutzer domänengebundener Desktopgeräte und umfunktionierter PCs, auf denen Citrix Desktop Lock ausgeführt wird, sowie Benutzer mit älteren Citrix Clients, die nicht aktualisiert werden können, können über die XenApp Services-URL auf Stores zugreifen. Wenn Sie einen neuen Store erstellen, wird die XenApp Services-URL standardmäßig aktiviert.

Die Abbildung zeigt die Optionen für den Zugriff auf StoreFront-Stores:



Citrix Receiver

Zugriff auf Stores von innerhalb der Citrix Receiver-Benutzeroberfläche aus bietet die beste Benutzererfahrung und den größten Funktionsumfang. Informationen dazu, mit welchen Citrix Receiver-Versionen Sie so auf Stores zugreifen können, finden Sie unter Systemanforderungen.

Citrix Receiver verwendet interne und externe URLs als Beacons. Anhand des Versuchs, diese Beacons zu kontaktieren, kann Citrix Receiver ermitteln, ob ein Benutzer mit dem lokalen oder einem öffentlichen Netzwerk verbunden ist. Wenn ein

Benutzer auf einen Desktop oder eine Anwendung zugreift, werden die Standortinformationen an den Server mit der Ressource weitergegeben, sodass die entsprechenden Verbindungsinformationen an Citrix Receiver zurückgegeben werden können. Dadurch kann Citrix Receiver sicherstellen, dass Benutzer nicht aufgefordert werden, sich neu anmelden, wenn sie auf einen Desktop oder eine Anwendung zugreifen. Weitere Informationen finden Sie unter Konfigurieren von Beacons.

Nach der Installation müssen in Citrix Receiver die Verbindungsinformationen für die Stores konfiguriert werden, über die Benutzern Desktops und Anwendungen bereitgestellt werden. Sie können Benutzern die Konfiguration erleichtern, indem Sie die erforderlichen Informationen über eine der folgenden Methoden bereitstellen.

Wichtig: Standardmäßig erfordert Citrix Receiver HTTPS-Verbindungen zu Stores. Wenn StoreFront nicht für HTTPS konfiguriert ist, müssen Benutzer zusätzliche Konfigurationsschritte ausführen, um HTTP-Verbindungen zu verwenden. Citrix empfiehlt dringend, keine ungeschützten Benutzerverbindungen mit StoreFront in einer Produktionsumgebung zu aktivieren. Weitere Informationen finden Sie unter *Konfigurieren und Installieren von Receiver für Windows mit Befehlszeilenparametern* in der Dokumentation von Receiver für Windows.

Provisioningdateien

Sie können Provisioningdateien mit den Verbindungsinformationen für die Stores der Benutzer bereitstellen. Nach der Installation von Citrix Receiver öffnen Benutzer die CR-Datei, um Konten für die Stores automatisch zu konfigurieren. Citrix Receiver für Web-Sites bieten Benutzern standardmäßig eine Provisioningdatei für den einen Store, für den die Site konfiguriert ist. Sie könnten die Benutzer auffordern, die Receiver für Web-Sites für die Stores zu besuchen, auf die sie zugreifen möchten, und von dort Provisioningdateien herunterzuladen. Für eine größere Kontrolle können Sie alternativ die Citrix StoreFront-Verwaltungskonsole zum Generieren von Provisioningdateien verwenden, die Verbindungsdetails für einen oder mehrere Stores enthalten. Sie können dann diese Dateien an die entsprechenden Benutzer verteilen. Weitere Informationen finden Sie unter Exportieren der Store-Provisioningdateien für Benutzer.

Automatisch generierte Setup-URLs

Für Mac OS-Benutzer können Sie mit dem Citrix Receiver für Mac Setup URL Generator eine URL mit den Verbindungsinformationen für einen Store erstellen. Nach der Installation von Citrix Receiver klicken Benutzer auf die URL, um ein Konto für den Store automatisch zu konfigurieren. Geben Sie die Bereitstellungsinformationen in das Tool ein und generieren Sie eine URL, die Sie an die Benutzer senden können.

Manuelle Konfiguration

Fortgeschrittene Benutzer können neue Konten erstellen, indem sie Store-URLs in Citrix Receiver eingeben. Weitere Informationen finden Sie in der Citrix Receiver-Dokumentation.

E-Mail-basierte Kontenermittlung:

Wenn Benutzer Citrix Receiver auf einem Gerät zum ersten Mal installieren, können sie ihr Konto durch Eingabe ihrer E-Mail-Adresse einrichten, sofern sie Citrix Receiver von der Citrix Website oder einer im internen Netzwerk gehosteten Citrix Receiver-Downloadseite herunterladen. Sie konfigurieren die Locator-Ressourceneinträge der Dienstidentifizierung (SRV) für NetScaler Gateway oder StoreFront auf dem Microsoft Active Directory-DNS-Server (Domain Name System). Benutzer müssen die Zugriffsinformationen für ihre Stores nicht kennen. Stattdessen geben sie während der Citrix Receiver-Erstkonfiguration ihre E-Mail-Adresse an. Citrix Receiver kontaktiert den DNS-Server der Domäne, die in der E-Mail-Adresse angegeben ist, und ruft die Details ab, die Sie dem Ressourceneintrag für Dienste (SRV) hinzugefügt haben. Daraufhin wird den Benutzern eine Liste der Stores angezeigt, auf die sie über Citrix Receiver zugreifen können.

Konfigurieren der e-mail-basierten Kontenermittlung

Konfigurieren Sie die e-mail-basierte Kontenermittlung, sodass Benutzer, die Citrix Receiver auf einem Gerät zum ersten Mal installieren, ihr Konto durch Eingabe ihrer E-Mail-Adresse einrichten können. Sofern sie Citrix Receiver von der Citrix Website oder einer im internen Netzwerk gehosteten Citrix Receiver-Downloadseite herunterladen, müssen Benutzer bei der Installation und Konfiguration von Citrix Receiver die Details für den Zugriff auf Stores nicht kennen. Die e-mail-basierte Kontenermittlung ist verfügbar, wenn Citrix Receiver von einem anderen Speicherort heruntergeladen wird (z. B. einer Citrix Receiver für Website). Bei Download von ReceiverWeb.exe oder ReceiverWeb.dmg über Citrix Receiver für Web werden Benutzer nicht zum Konfigurieren eines Stores aufgefordert. Die Benutzer können weiterhin "Konto hinzufügen" verwenden und ihre E-Mail-Adresse eingeben.

Während der Erstkonfiguration fordert Citrix Receiver Benutzer auf, eine E-Mail-Adresse oder eine Store-URL einzugeben. Wenn ein Benutzer eine E-Mail-Adresse eingibt, ruft Citrix Receiver vom Microsoft Active Directory-DNS-Server (Domain Name System) für die Domäne, die in der E-Mail-Adresse angegeben ist, eine Liste der verfügbaren Stores ab, aus der der Benutzer auswählen kann.

Damit Citrix Receiver verfügbare Stores auf Grundlage der E-Mail-Adressen von Benutzern finden kann, konfigurieren Sie die Ressourceneinträge für den Dienstidentifizierungslocator (SRV) für NetScaler Gateway oder StoreFront auf dem DNS-Server. Als Fallback können Sie StoreFront auch auf einem Server namens "discoverReceiver.Domäne ist die Domäne, die die E-Mail-Konten Ihrer Benutzer enthält. Wenn kein SRV-Eintrag in der angegebene Domäne gefunden wird, sucht Citrix Receiver nach einer Maschine mit dem Namen "discoverReceiver", um einen StoreFront-Server zu finden.

Sie müssen ein gültiges Serverzertifikat auf dem NetScaler Gateway-Gerät oder dem StoreFront-Server installieren, um die e-mail-basierte Kontenermittlung zu aktivieren. Des Weiteren muss die vollständige Kette zum Stammzertifikat gültig sein. Um optimale Benutzerfreundlichkeit zu erzielen, installieren Sie ein Zertifikat, das für "Antragsteller" oder "Alternativer Antragstellername" den Eintrag "discoverReceiver" verwendet.Domäne ist die Domäne, die die E-Mail-Konten Ihrer Benutzer enthält. Obwohl Sie ein Zertifikat mit Platzhalterzeichen für die Domäne verwenden können, die die E-Mail-Konten der Benutzer enthält, müssen Sie zunächst sicherstellen, dass die Bereitstellung solcher Zertifikate von den Sicherheitsrichtlinien Ihres Unternehmens zugelassen wird. Sie können andere Zertifikate für die Domäne mit den Benutzer-E-Mail-Konten verwenden, den Benutzern wird jedoch bei der ersten Verbindungsherstellung von Citrix Receiver mit dem StoreFront-Server eine Warnung bezüglich des Zertifikats angezeigt. Die e-mail-basierte Kontenermittlung kann nicht mit anderen Zertifikatidentitäten verwendet werden.

Um die e-mail-basierte Kontenermittlung für Benutzer zu aktivieren, die sich von außerhalb des lokalen Netzwerks anmelden, müssen Sie außerdem die StoreFront-Verbindungsinformationen auf dem NetScaler Gateway konfigurieren. Weitere Informationen finden Sie unter Verbinden mit StoreFront über die e-mail-basierte Kontoermittlung.

Hinzufügen eines SRV-Eintrags zum DNS-Server

1. Klicken Sie auf der **Windows-Startseite** auf **Verwaltung** und klicken Sie dann im Ordner **Verwaltung** auf **DNS**.
2. Wählen Sie im linken Bereich von **DNS-Manager** Ihre Domäne in der Forward- und Reverse-Lookupzone aus. Klicken Sie mit der rechten Maustaste auf die Domäne und wählen Sie **Weitere neue Einträge** aus.
3. Wählen Sie im Dialogfeld **Ressourceneintragstyp** die Option **Dienstidentifizierung (SRV)** aus und klicken Sie dann auf **Eintrag erstellen**.
4. Klicken Sie im Dialogfeld **Neuen Eintrag erstellen** in das Feld **Dienst** und geben Sie den Hostwert **_citrixreceiver** ein.
5. Geben Sie in das Feld **Protokoll** den Wert **_tcp** ein.
6. Geben Sie im Feld **Host, der diesen Dienst anbietet** den vollqualifizierten Domänennamen (FQDN) und den Port für das NetScaler Gateway-Gerät (Unterstützung lokaler und Remotebenutzer) oder den StoreFront-Server (nur Unterstützung von Benutzern im lokalen Netzwerk) im Format *servername.domäne:port* an.
   Wenn es in der Umgebung interne und externe DNS-Server gibt, können Sie einen SRV-Eintrag mit Angaben zum FQDN

des StoreFront-Servers auf dem internen DNS-Server und einen weiteren Eintrag zum externen Server unter Angabe des NetScaler Gateway-FQDNs hinzufügen. Mit dieser Konfiguration erhalten lokale Benutzer die StoreFront-Details, Remotebenutzer dagegen NetScaler Gateway-Verbindungsinformationen.

7. Wenn Sie einen SRV-Eintrag für das NetScaler Gateway-Gerät konfiguriert haben, fügen Sie NetScaler Gateway die StoreFront-Verbindungsinformationen in einem Sitzungsprofil oder einer globalen Einstellung hinzu.

Citrix Receiver für Web-Sites

Benutzer mit kompatiblen Webbrowsern können auf StoreFront-Stores zugreifen, indem sie zu Citrix Receiver für Web-Sites navigieren. Bei der Erstellung eines neuen Stores wird standardmäßig eine Citrix Receiver für Web-Site für den Store erstellt. Die Standardkonfiguration für Citrix Receiver für Web-Sites erfordert, dass Benutzer eine kompatible Version von Citrix Receiver installieren, um auf ihre Desktops und Anwendungen zuzugreifen. Weitere Informationen über die Kombinationen von Citrix Receiver und Webbrowsern, mit denen auf Citrix Receiver für Web-Sites zugegriffen werden kann, finden Sie unter Anforderungen für Benutzergeräte.

Standardmäßig versucht die Site zu ermitteln, ob Citrix Receiver auf dem Benutzergerät installiert ist, wenn ein Benutzer über einen Computer unter Windows oder Mac OS X auf Receiver für Web-Sites zugreift. Wenn Citrix Receiver nicht erkannt wird, wird der Benutzer aufgefordert, die entsprechende Citrix Receiver-Version für seine Plattform herunterzuladen und zu installieren. Der Standardort für den Download ist die Citrix Website; Sie können jedoch auch die Installationsdateien auf den StoreFront-Server kopieren und Benutzern diese lokalen Dateien anbieten. Bei lokaler Speicherung der Citrix Receiver-Installationsdateien können Sie die Site auch so konfigurieren, dass Benutzer älterer Clients ein Upgrade auf die Version auf dem Server durchführen können. Weitere Informationen zum Konfigurieren der Bereitstellung von Citrix Receiver für Windows und Citrix Receiver für Mac finden Sie unter Konfigurieren von Citrix Receiver für Web-Sites.

Citrix Receiver für HTML5

Citrix Receiver für HTML5 ist eine StoreFront-Komponente, die standardmäßig in Citrix Receiver für Web-Sites integriert ist. Sie können Citrix Receiver für HTML5 auf den Citrix Receiver für Web-Sites aktivieren, sodass Benutzer, die Citrix Receiver nicht installieren können, weiterhin Zugriff auf ihre Ressourcen haben. Mit Citrix Receiver für HTML5 können Benutzer auf Desktops und Anwendungen direkt über einen HTML5-kompatiblen Webbrowser zugreifen, ohne dass Citrix Receiver installiert werden muss. Wenn Sie eine Site erstellen, ist Citrix Receiver für HTML5 standardmäßig deaktiviert. Weitere Informationen zum Aktivieren von Citrix Receiver für HTML5 finden Sie unter citrix-receiver-download-page-template.html.

Fürden Zugriff auf Desktops und Anwendungen mit Citrix Receiver für HTML5 müssen die Benutzer auf die Citrix Receiver für Web-Site mit einem HTML5-kompatiblen Browser zugreifen. Weitere Informationen über die Betriebssysteme und Webbrowser, die mit Citrix Receiver für HTML5 verwendet werden können, finden Sie unter Anforderungen für Benutzergeräte.

Citrix Receiver für HTML5 kann von Benutzern im internen Netzwerk und von Remotebenutzern, die eine Verbindung über NetScaler Gateway herstellen, verwendet werden. Für Verbindungen über das interne Netzwerk unterstützt Citrix Receiver für HTML5 den Zugriff auf Desktops und Anwendungen nur von einer Teilmenge der Produkte, die von Citrix Receiver für Web-Sites unterstützt werden. Benutzer, die die Verbindung über NetScaler Gateway herstellen, können auf Ressourcen zugreifen, die über eine breitere Produktpalette bereitgestellt werden, wenn Sie beim Konfigurieren von StoreFront Citrix Receiver für HTML5 als Option wählen. Bestimmte Versionen von NetScaler Gateway sind für Citrix Receiver für HTML5 erforderlich. Weitere Informationen finden Sie unter Anforderungen an die Infrastruktur.

Für lokale Benutzer im internen Netzwerk ist der Zugriff über Citrix Receiver für HTML5 auf Ressourcen, die von XenDesktop und XenApp bereitgestellt werden, standardmäßig deaktiviert. Sie aktivieren den lokalen Zugriff auf Desktops

und Anwendungen über Citrix Receiver für HTML5, indem Sie die Richtlinie für ICA-WebSockets-Verbindungen auf den XenDesktop- und XenApp-Servern aktivieren. Stellen Sie sicher, dass die Firewalls und anderen Netzwerkgeräte den Zugriff auf den in der Richtlinie festgelegten Port für Citrix Receiver für HTML5 zulassen. Weitere Informationen finden Sie unter Einstellungen der Richtlinie "WebSockets".

Standardmäßig werden Desktops und Anwendungen in Citrix Receiver für HTML5 auf einer neuen Browserregisterkarte gestartet. Beim Start von Ressourcen über Verknüpfungen mit Citrix Receiver für HTML5 ersetzt der Desktop bzw. die Anwendung jedoch die Citrix Receiver für Web-Site in der geöffneten Browserregisterkarte anstatt eine neue Registerkarte anzuzeigen. Sie können Citrix Receiver für HTML5 so konfigurieren, dass Ressourcen immer auf der gleichen Registerkarte wiedie Receiver für Web-Site gestartet werden. Weitere Informationen finden Sie unter Konfigurieren der Verwendung der Browserregisterkarten für Citrix Receiver für HTML5.

Ressourcenverknüpfungen

Sie können URLs für den Zugriff auf Desktops und Anwendungen, die über Citrix Receiver für Web-Sites verfügbar sind, generieren. Betten Sie diese Links in Websites ein, die im internen Netzwerk gehostet werden, damit Benutzer schnell auf Ressourcen zugreifen können. DieBenutzer klicken auf einen Link und werden an die Receiver für Web-Site weitergeleitet, wo sie sich anmelden, wenn sie dies nicht bereits getan haben. Die Citrix Receiver für Web-Site startet automatisch die Ressource. Im Fall von Anwendungen wird zudem ein Abonnement für die Benutzer erstellt, wenn diese eine Anwendung noch nicht abonniert haben. Weitere Informationen zum Erstellen von Ressourcenverknüpfungen finden Sie unter Konfigurieren von Citrix Receiver für Web-Sites.

Wie bei allen Desktops und Anwendungen, auf die über Citrix Receiver für Web-Sites zugegriffen wird, müssen Benutzer entweder Citrix Receiver installiert haben oder Citrix Receiver für HTML5 für den Zugriff auf Ressourcen über Verknüpfungen verwenden können. Die für eine Citrix Receiver für Web-Site verwendete Methode hängt von der Sitekonfiguration ab, d. h. davon, ob Citrix Receiver auf Benutzergeräten erkannt werden kann und ob ein HTML5-kompatibler Browser verwendet wird. Aus Sicherheitsgründen werden Benutzer von Internet Explorer möglicherweise aufgefordert, zu bestätigen, dass sie Ressourcen über Verknüpfungen starten möchten. WeisenSie die Benutzer an, die Receiver für Web-Site in die Zone "Lokales Intranet" oder "Vertrauenswürdige Sites" in Internet Explorer einzufügen, um diesen zusätzlichen Schritt zu vermeiden. Standardmäßig sind Workspace Control und der automatische Start von Desktops beim Zugriff auf Citrix Receiver für Web-Sites über Verknüpfungen deaktiviert.

Wenn Sie eine Anwendungsverknüpfung erstellen, stellen Sie sicher, dass keine andere über die Citrix Receiver für Web-Site verfügbare Anwendung denselben Namen hat. Verknüpfungen können nicht zwischen mehreren Instanzen einer Anwendung mit dem gleichen Namen unterscheiden. Gleichermaßen können Sie, wenn Sie mehrere Instanzen eines Desktops in einer Desktopgruppe über eine Citrix Receiver für Web-Site verfügbar machen, keine separate Verknüpfung für jede Instanz erstellen. Verknüpfungen können keine Befehlszeilenparameter an Anwendungen weitergeben.

Zum Erstellen von Anwendungsverknüpfungen konfigurieren Sie StoreFront mit den URLs der internen Websites, von denen die Verknüpfungen gehostet werden. Wenn ein Benutzer auf eine Anwendungsverknüpfung auf einer Website klickt, prüft StoreFront diese Website anhand der von Ihnen eingegebenen Liste der URLs, um sicherzustellen, dass die Anforderung von einer vertrauenswürdigen Website stammt. Für Benutzer, die eine Verbindung über NetScaler Gateway herstellen, werden Websites, die Verknüpfungen hosten, jedoch nicht validiert, da die URLs nicht an StoreFront übergeben werden. Um sicherzustellen, dass Benutzer nur Zugriff auf Anwendungsverknüpfungen von vertrauenswürdigen internen Websites haben, konfigurieren Sie NetScaler Gateway so, dass der Zugriff auf diese Websites beschränkt wird. Weitere Informationen finden Sie unter http://support.citrix.com/article/CTX123610

Anpassen der Sites

Citrix Receiver für Web-Sites bieten einen Mechanismus zum Anpassen der Benutzeroberfläche. Sie können Zeichenfolgen anpassen, das Cascading Stylesheet und die JavaScript-Dateien. Sie können außerdem einen benutzerdefinierten Bildschirm vor oder nach der Anmeldung hinzufügen, ebenso wie Sprachpakete.

Wichtige Hinweise

Benutzer, die über eine Citrix Receiver für Web-Site auf Stores zugreifen, profitieren von vielen der Features, die bei Storezugriff in Citrix Receiver verfügbar sind, z. B. Anwendungssynchronisierung. Bei der Entscheidung, ob Sie Benutzern Zugriff auf Stores über Citrix Receiver für Web-Sites gewähren möchten, berücksichtigen Sie die folgenden Einschränkungen.

- Über jede Citrix Receiver für Web-Site kann nur auf jeweils einen einzigen Store zugegriffen werden.
- Citrix Receiver für Web-Sites können keine SSL-VPN-Verbindungen (Secure Sockets Layer, virtuelles privates Netzwerk) initiieren. Benutzer, die sich ohne VPN-Verbindung über NetScaler Gateway anmelden, können nicht auf Webanwendungen zugreifen, für die App Controller eine solche Verbindung erfordert.
- Abonnierte Anwendungen sind nicht auf der Windows-Startseite verfügbar, wenn über eine Citrix Receiver für Web-Site auf einen Store zugegriffen wird.
- Es ist keine Dateitypzuordnung zwischen lokalen Dokumenten und gehosteten Anwendungen verfügbar, die über Citrix Receiver für Web-Sites aufgerufen werden.
- Auf Offlineanwendungen kann über Citrix Receiver für Web-Sites nicht zugegriffen werden.
- Citrix Receiver für Web-Sites unterstützen keine in Stores integrierten Citrix Online-Produkte. Citrix Online-Produkte müssen mit App Controller bereitgestellt oder als gehostete Anwendungen verfügbar gemacht werden, um den Zugriff über Citrix Receiver für Web-Sites zu ermöglichen.
- Citrix Receiver für HTML5 kann mit HTTPS-Verbindungen verwendet werden, wenn der VDA XenApp 7.6 oder XenDesktop 7.6 mit aktiviertem SSL ist oder wenn der Benutzer eine Verbindung über NetScaler Gateway herstellt.
- Wenn Benutzer Citrix Receiver für HTML5 mit Mozilla Firefox über HTTPS-Verbindungen verwenden möchten, müssen sie about:config in die Adressleiste von Firefox eingeben und die Einstellung network.websocket.allowInsecureFromHTTPS auf true setzen.

Desktopgerätesites

Benutzer nicht domänengebundener Desktopgeräte können auf ihre Desktops über Desktopgerätesites zugreifen. In diesem Zusammenhang ist die Nichteinbindung der Geräte in eine Domäne in der Active Directory-Gesamtstruktur gemeint, die die StoreFront-Server enthält.

Wenn Sie mit Citrix Studio einen neuen Store für eine XenDesktop-Bereitstellung erstellen, wird standardmäßig eine Desktopgerätesite für den Store erstellt. Desktopgerätesites werden nur standardmäßig erstellt, wenn StoreFront installiert und als Teil der XenDesktop-Installation konfiguriert ist. Sie können Desktopgerätesites manuell über Windows PowerShell erstellen. Weitere Informationen finden Sie unter Konfigurieren von Desktopgerätesites.

Desktopgerätesites bieten eine ähnliche Benutzererfahrung wie bei der Anmeldung bei einem lokalen Desktop. Die Webbrowser auf Desktopgeräten sind so konfiguriert, dass sie im Vollbildmodus starten und den Anmeldebildschirm für eine Desktopgerätesite anzeigen. Wenn ein Benutzer sich bei einer Site anmeldet, wird standardmäßig automatisch der Desktop in dem für die Site konfigurierten Store gestartet, der dem Benutzer als erster (in alphabetischer Reihenfolge) zur Verfügung steht. Wenn Sie Benutzern Zugriff auf mehrere Desktops in einem Store bereitstellen, können Sie die Desktopgerätesite so konfigurieren, dass die verfügbaren Desktops angezeigt werden, damit Benutzer einen auswählen können. Weitere Informationen finden Sie unter Konfigurieren von Desktopgerätesites.

Wenn der Desktop eines Benutzers gestartet wird, wird er im Vollbildmodus angezeigt und verdeckt den Webbrowser. Der

Benutzer wird automatisch von der Desktopgerätesite abgemeldet. Wenn sich der Benutzer vom Desktop abmeldet, wird der Webbrowser, der den Anmeldebildschirm der Desktopgerätesite anzeigt, wieder sichtbar. Eine Meldung wird angezeigt, wenn ein Desktop gestartet wird, die einen Link für den Benutzer enthält, mit dem er den Desktop neu starten kann, wenn der Zugriff darauf nicht möglich ist. Zum Aktivieren dieser Funktion müssen Sie die Bereitstellungsgruppe so konfigurieren, dass Benutzer ihre Desktops neu starten können. Weitere Informationen finden Sie unter Bereitstellungsgruppen.

Damit Zugriff auf Desktops möglich ist, ist eine kompatible Version von Citrix Receiver auf dem Desktopgerät erforderlich. Normalerweise integrieren Hersteller XenDesktop-kompatibler Geräte Citrix Receiver in ihren Produkten. Bei Windows-Geräten muss außerdem Citrix Desktop Lock installiert und mit der URL für die Desktopgerätesite konfiguriert sein. Wird Internet Explorer verwendet, muss die Desktopgerätesite der Zone "Lokales Intranet" oder "Vertrauenswürdige Sites" hinzugefügt werden. Weitere Informationen zu Citrix Desktop Lock finden Sie unter Verhindern des Benutzerzugriffs auf den lokalen Desktop.

Wichtige Hinweise

Desktopgerätesites sind für lokale Benutzer im internen Netzwerk vorgesehen, die auf Desktops von nicht domänengebundenen Desktopgeräten aus zugreifen. Bei der Entscheidung, ob Sie Benutzern Zugriff auf Stores über Desktopgerätesites gewähren möchten, sollten Sie die folgenden Einschränkungen berücksichtigen.

- Wenn Sie domänengebundene Desktopgeräte und umfunktionierte PCs bereitstellen möchten, konfigurieren Sie diese nicht für den Zugriff auf Stores über Desktopgerätesites. Sie können Citrix Receiver zwar mit der XenApp Services-URL für den Store konfigurieren, Citrix empfiehlt jedoch die Verwendung des neuen Desktop Lock für domänengebundene und nicht domänengebundene Desktopgeräte. Weitere Informationen finden Sie unter Citrix Receiver Desktop Lock.
- Desktopgerätesites unterstützen keine Verbindungen von Remotebenutzern außerhalb des Unternehmensnetzwerks. Benutzer, die sich an NetScaler Gateway anmelden, können nicht auf Desktopgerätesites zugreifen.

XenApp Services-URLs

Benutzer älterer Citrix Clients, die nicht aktualisiert werden können, können auf Stores zugreifen, indem sie ihren Client mit der XenApp Services-URL für den Store konfigurieren. Sie können auch Zugriff auf Stores über XenApp Services-URLs von domänengebundenen Desktopgeräten und umfunktionierten PCs, auf denen Citrix Desktop Lock ausgeführt wird, aktivieren. In diesem Zusammenhang ist die Einbindung der Geräte in eine Domäne in der Active Directory-Gesamtstruktur gemeint, die die StoreFront-Server enthält.

StoreFront unterstützt die Passthrough-Authentifizierung mit Proximitykarten über Citrix Receiver bei XenApp Services-URLs. Citrix Ready-Partnerprodukte verwenden die Citrix Fast Connect-API zur Leitung von Benutzeranmeldungen über Citrix Receiver für Windows für die Verbindung mit Stores mit der XenApp Services-URL. Die Benutzer authentifizieren sich bei Arbeitsstationen mit Proximitykarten und werden schnell mit per XenDesktop und XenApp bereitgestellten Desktops und Anwendungen verbunden. Weitere Informationen finden Sie in der aktuellen Dokumentation zu Citrix Receiver für Windows.

Wenn Sie einen neuen Store erstellen, wird die XenApp Services-URL für den Store standardmäßig aktiviert. Die XenApp Services-URL für den Store hat das Format http[s]://serveraddress/Citrix/storename/PNAgent/config.xml, wobei serveraddressder vollqualifizierte Domänenname des Servers oder der Lastausgleichsumgebung für die StoreFront-Bereitstellung ist und storenameist der Name, den Sie beim Erstellen für den Store angegeben haben. Dies ermöglicht die Verwendung von Citrix Receiver-Instanzen, die nur über das PNAgent-Protokoll eine Verbindung mit StoreFront herstellen können. Eine Liste der Clients, mit denen Sie über XenApp Services-URLs auf Stores zugreifen können, finden Sie unter Anforderungen für Benutzergeräte.

Wichtige Hinweise

XenApp Services-URLs dienen zur Unterstützung von Benutzern, die nicht auf Citrix Receiver aktualisieren können, und für Szenarien, in denen alternative Zugriffsmethoden nicht verfügbar sind. Bei der Entscheidung, ob Sie Benutzern Zugriff auf Stores über XenApp Services-URLs gewähren möchten, sollten Sie die folgenden Einschränkungen berücksichtigen.

- Die XenApp Services-URL für einen Store kann nicht geändert werden.
- Sie können die Einstellungen einer XenApp Services-URL nicht durch Bearbeiten der Konfigurationsdatei config.xml ändern.
- XenApp Services-URLs unterstützen die explizite, Domänen-Passthrough-Authentifizierung mit Smartcards und die Passthrough-Authentifizierung mit Smartcards. Die explizite Authentifizierung ist standardmäßig aktiviert. Nur eine Authentifizierungsmethode kann für jede XenApp Services-URL konfiguriert werden und pro Store ist nur eine URL verfügbar. Wenn Sie mehrere Authentifizierungsmethoden benötigen, müssen Sie separate Stores mit einer XenApp Services-URL für jede Authentifizierungsmethode erstellen. Die Benutzer müssen dann eine Verbindung mit dem für ihre Authentifizierungsmethode geeigneten Store herstellen. Weitere Informationen finden Sie unter XML-basierte Authentifizierung.
- Workspace Control ist standardmäßig für XenApp Services-URLs aktiviert und kann nicht konfiguriert oder deaktiviert werden.
- Benutzeranforderungen zum Ändern von Kennwörtern werden direkt über die XenDesktop- oder XenApp-Server, die Desktops und Anwendungen für den Store bereitstellen, an den Domänencontroller geleitet. Der StoreFront-Authentifizierungsdienst wird dabei umgangen.

Benutzerauthentifizierung

Jun 04, 2018

StoreFront unterstützt verschiedene Authentifizierungsmethoden für den Zugriff auf Stores durch Benutzer, die jedoch, abhängig von der Zugriffsmethode und dem Netzwerkstandort des Benutzers, nicht alle verfügbar sind. Aus Sicherheitsgründen werden Authentifizierungsmethoden standardmäßig deaktiviert, wenn Sie den ersten Store erstellen. Weitere Informationen zum Aktivieren und Deaktivieren von Benutzerauthentifizierungsmethoden finden Sie unter Erstellen und Konfigurieren des Authentifizierungsdiensts.

Benutzername und Kennwort

Benutzer geben ihre Anmeldeinformationen ein und werden authentifiziert, wenn sie auf ihre Stores zugreifen. Die explizite Authentifizierung ist standardmäßig aktiviert. Alle Benutzerzugriffsmethoden unterstützen die explizite Authentifizierung.

Wenn ein Benutzer NetScaler Gateway verwendet, um auf Citrix Receiver für Web zuzugreifen, verwaltet NetScaler Gateway die Anmelde- und Kennwortänderung beim Ablauf. Benutzer können wahlweise das Kennwort mit der Citrix Receiver für Web-Benutzeroberfläche ändern. Nachdem das Kennwort geändert wurde, wird die NetScaler Gateway-Sitzung beendet und der Benutzer muss sich neu anmelden. Benutzer von Citrix Receiver für Linux können nur abgelaufene Kennwörter ändern.

SAML-Authentifizierung

Benutzer authentifizieren sich beim SAML-Idenditätsanbieter und werden beim Zugriff auf ihre Stores automatisch angemeldet. StoreFront unterstützt eine direkte SAML-Authentifizierung über ein Unternehmensnetzwerk ohne NetScaler.

SAML (Security Assertion Markup Language) ist ein offener Standard, der in Identitäts- und Authentifizierungsprodukten wie etwa Microsoft AD FS (Active Directory-Verbunddienste) verwendet wird. Durch die Integration der SAML-Authentifizierung über StoreFront können Administratoren u. a. Benutzern gestatten, sich ein Mal beim Unternehmensnetzwerk anzumelden und dann Single Sign-On für ihre veröffentlichten Anwendungen zu nutzen.

Anforderungen:

- Implementierung des Citrix Verbundauthentifizierungsdiensts
- SAML 2.0-konforme Identitätsanbieter:
  - Microsoft AD FS 4.0 (Windows Server 2016) unter ausschließlicher Nutzung von SAML-Bindungen (keine WS-Verbundbindungen)Weitere Informationen finden Sie unter AD FS 2016-Bereitstellung und AD FS 2016 Vorgänge.
  - Microsoft AD FS v3.0 (Windows Server 2012 R2)
  - NetScaler Gateway (als IdP konfiguriert)
- Konfigurieren Sie die SAML-Authentifizierung in StoreFront über die StoreFront-Verwaltungskonsole in einer neuen Bereitstellung (siehe Neue Bereitstellung erstellen) oder in einer bestehenden Bereitstellung (siehe Konfigurieren des Authentifizierungsdiensts). Sie können die SAML-Authentifizierung auch mit PowerShell-Cmdlets konfigurieren (siehe StoreFront SDK).
- Citrix Receiver für Windows (4.6 und höher) oder Citrix Receiver für Web.

Die Verwendung der SAML-Authentifizierung mit Netscaler wird zurzeit für Receiver für Web-Sites unterstützt.

Domänen-Passthrough

Benutzer authentifizieren sich bei ihrem domänengebundenen Computer und ihre Anmeldeinformationen werden für eine

automatische Anmeldung beim Zugriff auf ihre Stores verwendet. Wenn Sie StoreFront installieren, wird die Domänen-Passthrough-Authentifizierung standardmäßig deaktiviert. Die Domänen-Passthrough-Authentifizierung kann für Benutzer aktiviert werden, die über Citrix Receiver und XenApp Services-URLs eine Verbindung mit Stores herstellen. Citrix Receiver für Web-Sites unterstützen die Domänen-Passthrough-Authentifizierung nur für Internet Explorer. Aktivieren Sie die Domänen-Passthrough-Authentifizierung in dem Citrix Receiver für Web-Site Knoten in der Verwaltungskonsole. Sie müssen auch die einmalige Anmeldung in Citrix Receiver für Windows konfigurieren. Citrix Receiver für HTML5 unterstützt keine Passthrough-Authentifizierung für Domänen. Zur Verwendung der Domänen-Passthrough-Authentifizierung benötigen Benutzer Citrix Receiver für Windows oder das Online Plug-In für Windows. Die Passthrough-Authentifizierung muss aktiviert werden, wenn Citrix Receiver für Windows oder das Online Plug-In für Windows auf den Benutzergeräten installiert ist.

Passthrough-Authentifizierung von NetScaler Gateway

Benutzer authentifizieren sich bei NetScaler Gateway und werden beim Zugriff auf ihre Stores automatisch angemeldet. Die Passthrough-Authentifizierung von NetScaler Gateway ist standardmäßig aktiviert, wenn Sie eine erste Konfiguration des Remotezugriffs auf den Store durchführen. Benutzer können mit Citrix Receiver oder Citrix Receiver für Web-Sites über NetScaler Gateway eine Verbindung mit Stores herstellen. Desktopgerätesites unterstützen keine Verbindungen über NetScaler Gateway. Weitere Informationen zum Konfigurieren von StoreFront für NetScaler Gateway finden Sie unter Hinzufügen einer NetScaler Gateway-Verbindung.

StoreFront unterstützt Passthrough mit den folgenden NetScaler Gateway-Authentifizierungsmethoden.

- **Sicherheitstoken:** Benutzer melden sich bei NetScaler Gateway mit Passcodes an, die von durch Sicherheitstoken generierten Tokencodes abgeleitet sind und in manchen Fällen mit einer PIN kombiniert werden. Wenn Sie zur Passthrough-Authentifizierung ausschließlich Sicherheitstoken aktivieren, stellen Sie sicher, dass die von Ihnen bereitgestellten Ressourcen keine zusätzlichen oder alternativen Authentifizierungsformen erfordern, wie Microsoft Active Directory-Domänenanmeldeinformationen.
- **Domäne und Sicherheitstoken:** Benutzer, die sich an NetScaler Gateway anmelden, müssen ihre Domänenanmeldeinformationen und ihre Sicherheitstoken-Passcodes eingeben.
- **Clientzertifikat:** Benutzer melden sich bei NetScaler Gateway an und werden auf Grundlage der Attributen im Clientzertifikat, das NetScaler Gateway übergeben wird, authentifiziert. Konfigurieren Sie die Clientzertifikat-Authentifizierung, damit Benutzer sich an NetScaler Gateway mit Smartcards anmelden können. Die Clientzertifikat-Authentifizierung kann zusammen mit anderen Authentifizierungstypen verwendet werden, um Zweiquellenauthentifizierung bereitzustellen.

StoreFront bietet Passthrough-Authentifizierung für Remotebenutzer über den NetScaler Gateway-Authentifizierungsdienst, damit diese Benutzer ihre Anmeldeinformationen nur einmal eingeben müssen. Standardmäßig ist die Passthrough-Authentifizierung jedoch nur für Benutzer aktiviert, die sich an NetScaler Gateway mit einem Kennwort anmelden. Zum Konfigurieren der Passthrough-Authentifizierung von NetScaler Gateway bei StoreFront für Smartcardbenutzer delegieren Sie die Validierung der Anmeldeinformationen an NetScaler Gateway. Weitere Informationen finden Sie unter Erstellen und Konfigurieren des Authentifizierungsdiensts.

Benutzer können eine Verbindung mit Stores in Citrix Receiver mit Passthrough-Authentifizierung über einen SSL-VPN-Tunnel (Secure Sockets Layer, virtuelles privates Netzwerk) mit dem NetScaler Gateway Plug-In herstellen. Remotebenutzer, die das NetScaler Gateway Plug-In nicht installieren können, können über den clientlosen Zugriff eine Verbindung mit Stores in Citrix Receiver mit Passthrough-Authentifizierung herstellen. Zur Verwendung des clientlosen Zugriffs für eine Verbindung mit Stores benötigen Benutzer eine Version von Citrix Receiver, die den clientlosen Zugriff unterstützt.

Darüber hinaus können Sie clientlosen Zugriff mit Passthrough-Authentifizierung zu Citrix Receiver für Web-Sites aktivieren. Konfigurieren Sie dazu NetScaler Gateway als sicheren Remoteproxy. Benutzer melden sich direkt bei NetScaler Gateway

an und verwenden die Citrix Receiver für Web-Site, um auf ihre Anwendungen zuzugreifen, ohne sich neu authentifizieren zu müssen.

Benutzer, die über den clientlosen Zugriff eine Verbindung zu App Controller-Ressourcen herstellen, können nur auf externe SaaS-Anwendungen (Software-as-a-Service) zugreifen. Für den Zugriff auf interne Webanwendungen müssen Remotebenutzer das NetScaler Gateway Plug-In verwenden.

Wenn Sie die Zweiquellenauthentifizierung bei NetScaler Gateway für Remotebenutzer konfigurieren, die von Citrix Receiver aus auf Stores zugreifen, müssen Sie zwei Authentifizierungsrichtlinien für NetScaler Gateway erstellen. Konfigurieren Sie RADIUS (Remote Authentication Dial-In User Service) als primäre Authentifizierungsmethode und LDAP (Lightweight Directory Access Protocol) als sekundäre Methode. Ändern Sie den Anmeldeinformationsindex zur Verwendung der sekundären Authentifizierungsmethode im Sitzungsprofil, sodass LDAP-Anmeldeinformationen an StoreFront übergeben werden. Beim Hinzufügen des NetScaler Gateway-Geräts in der StoreFront-Konfiguration legen Sie für Logon type die Einstellung Domain and security token fest. Weitere Informationen finden Sie unter http://support.citrix.com/article/CTX125364.

Zum Aktivieren der Multidomänenauthentifizierung über NetScaler Gateway bei StoreFront setzen Sie in der NetScaler Gateway-LDAP-Authentifizierungsrichtlinie für jede Domäne SSO Name Attribute auf userPrincipalName. Sie können festlegen, dass die Benutzer auf der NetScaler Gateway-Anmeldeseite eine Domäne angeben müssen, sodass die richtige zu verwendende LDAP Richtlinie ermittelt werden kann. Geben Sie beim Konfigurieren der NetScaler Gateway-Sitzungsprofile für Verbindungen mit StoreFront keine Single Sign-On-Domäne an. Sie müssen Vertrauensstellungen zwischen allen Domänen konfigurieren. Stellen Sie sicher, dass Benutzer sich von allen Domänen aus an StoreFront anmelden können, indem Sie den Zugriff nicht auf explizit vertrauenswürdige Domänen beschränken.

Wenn die NetScaler Gateway-Bereitstellung dies unterstützt, können Sie SmartAccess zur Steuerung des Benutzerzugriffs auf XenDesktop- und XenApp-Ressourcen auf der Basis von NetScaler Gateway-Sitzungsrichtlinien verwenden. Weitere Informationen über SmartAccess finden Sie unter How SmartAccess works for XenApp and XenDesktop.

Smartcards

Benutzer authentifizieren sich mit Smartcards und PINs beim Zugriff auf ihre Stores. Wenn Sie StoreFront installieren, wird die Smartcardauthentifizierung standardmäßig deaktiviert. Die Smartcardauthentifizierung kann für Benutzer aktiviert werden, die über Citrix Receiver, Citrix Receiver für Web, Desktopgerätesites und XenApp Services-URLs eine Verbindung mit Stores herstellen.

Verwenden Sie die Smartcardauthentifizierung zur Vereinfachung der Anmeldung für Ihre Benutzer und zur gleichzeitigen Erhöhung der Sicherheit von deren Zugriff auf Ihre Infrastruktur. Der Zugriff auf das interne Unternehmensnetzwerk ist durch die zertifikatbasierte Zweifaktorauthentifizierung mit der Public Key-Infrastruktur geschützt. Private Schlüssel werden über die Hardware geschützt und verlassen nie die Smartcard. Die Benutzer können auf ihre Desktops und Anwendungen von unterschiedlichen Geräten des Unternehmens aus bequem mit Smartcard und PIN zugreifen.

Sie können Smartcards für die Benutzerauthentifizierung über StoreFront bei von XenDesktop und XenApp bereitgestellten Desktops und Anwendungen verwenden. Benutzer von Smartcard, die sich bei StoreFront anmelden, können auch auf von App Controller bereitgestellte Anwendungen zugreifen. Für den Zugriff auf App Controller-Webanwendungen, für die Clientzertifikatauthentifizierung verwendet wird, müssen sich Benutzer jedoch neu authentifizieren.

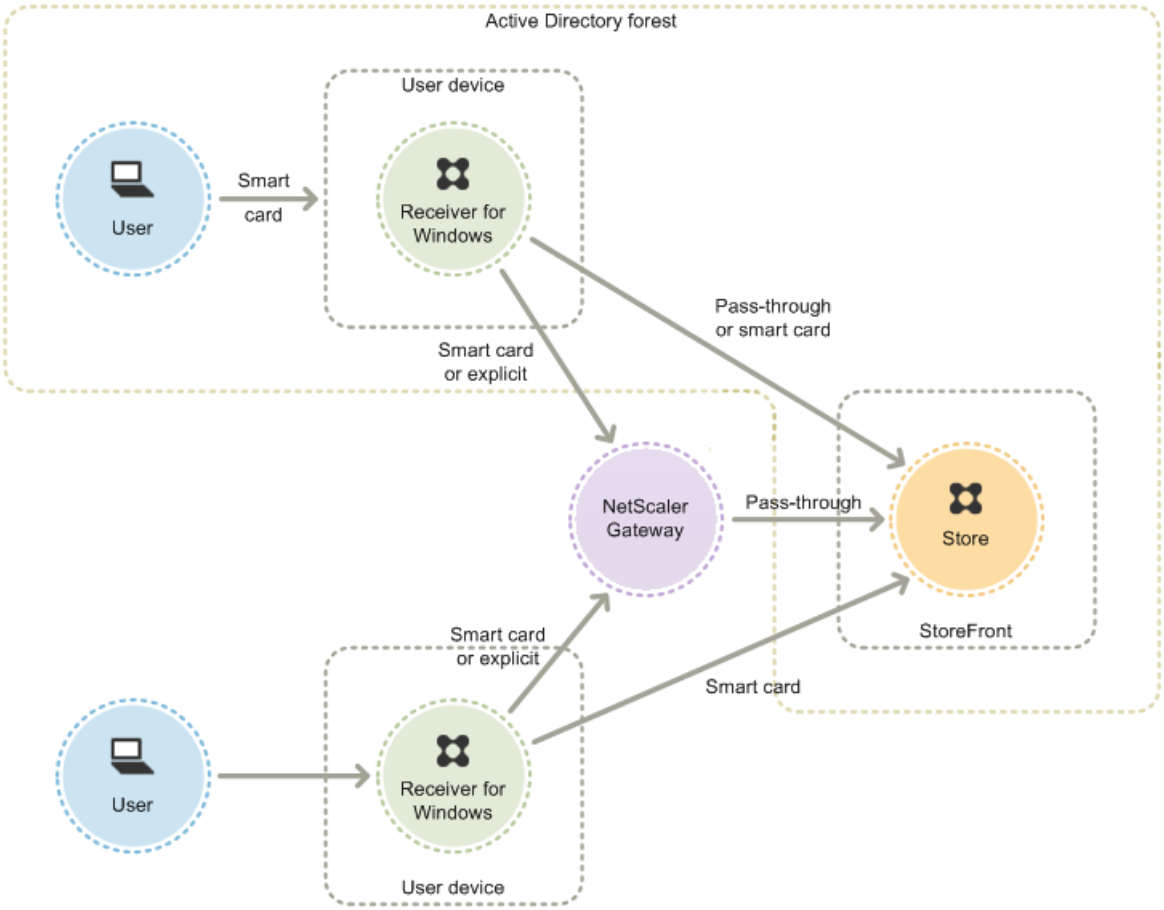
Zum Aktivieren der Smartcardauthentifizierung müssen Benutzerkonten entweder in der Microsoft Active Directory-Domäne der StoreFront-Server konfiguriert werden oder in einer Domäne, die über eine direkte bidirektionale Vertrauensstellung mit der StoreFront-Serverdomäne verfügt. Bereitstellungen mit mehreren Gesamtstrukturen und bidirektionalen Vertrauensstellungen werden unterstützt.

Die Konfiguration der Smartcardauthentifizierung bei StoreFront hängt von den Benutzergeräten, den installierten Clients und davon ab, ob die Geräte in die Domäne eingebunden sind. In diesem Zusammenhang bedeutet in die Domäne eingebunden, das die Geräte in eine Domäne in der Active Directory-Gesamtstruktur eingebunden sind, die die StoreFront-Server enthält.

Verwenden von Smartcards mit Citrix Receiver für Windows

Benutzer mit Geräten, die Citrix Receiver für Windows ausführen, können sich mit Smartcards direkt oder über NetScaler Gateway authentifizieren. Es können domänengebundene und nicht domänengebundene Geräte verwendet werden, allerdings bei einer geringfügig anderen Benutzererfahrung.

Die Abbildung zeigt die Optionen für die Smartcardauthentifizierung über Citrix Receiver für Windows.



Sie können Smartcardauthentifizierung für lokale Benutzer mit in Domänen eingebundenen Geräten konfigurieren, sodass Benutzer nur einmal zur Eingabe ihrer Anmeldeinformationen aufgefordert werden. Benutzer melden sich bei ihren Geräten mit ihrer Smartcard und PIN an und werden bei entsprechender Konfiguration nicht noch einmal zur Eingabe ihrer PIN aufgefordert. Benutzer werden automatisch bei StoreFront authentifiziert und auch, wenn sie auf ihre Desktops und Anwendungen zugreifen. Hierzu konfigurieren Sie Citrix Receiver für Windows für Passthrough-Authentifizierung und aktivieren Domänen-Passthrough-Authentifizierung für StoreFront.

Benutzer melden sich beim Gerät an und authentifizieren sich dann bei Citrix Receiver für Windows mit ihrer PIN. Beim Starten von Apps und Desktops werden keine weiteren Aufforderungen zur PIN-Eingabe angezeigt.

Da Benutzer nicht domänengebundener Geräte sich direkt bei Citrix Receiver für Windows anmelden, können Sie für diese

Benutzer ein Fallback auf die explizite Authentifizierung aktivieren. Wenn Sie Smartcard- und explizite Authentifizierung konfigurieren, werden Benutzer zunächst aufgefordert, sich mit der Smartcard und PIN anzumelden, können aber bei Problemen mit der Smartcard die explizite Authentifizierung auswählen.

Benutzer, die eine Verbindung über NetScaler Gateway herstellen, müssen sich mindestens zwei Mal mit Smartcard und PIN anmelden, um auf ihre Desktops und Anwendungen zugreifen zu können. Dies gilt sowohl für in Domänen eingebundene Geräte als auch für Geräte, die nicht in Domänen eingebunden sind. Benutzer authentifizieren sich mit ihrer Smartcard und PIN und werden bei entsprechender Konfiguration nur dann noch einmal zur Eingabe ihrer PIN aufgefordert, wenn sie auf ihre Desktops und Anwendungen zugreifen. Dazu aktivieren Sie die Passthrough-Authentifizierung mit NetScaler Gateway bei StoreFront und delegieren die Anmeldeinformationenvalidierung an NetScaler Gateway. Erstellen Sie dann einen weiteren virtuellen NetScaler Gateway-Server und leiten Sie über ihn die Benutzerverbindungen zu Ressourcen. Für in Domänen eingebundene Geräte müssen Sie zudem Citrix Receiver für Windows für Passthrough-Authentifizierung konfigurieren.

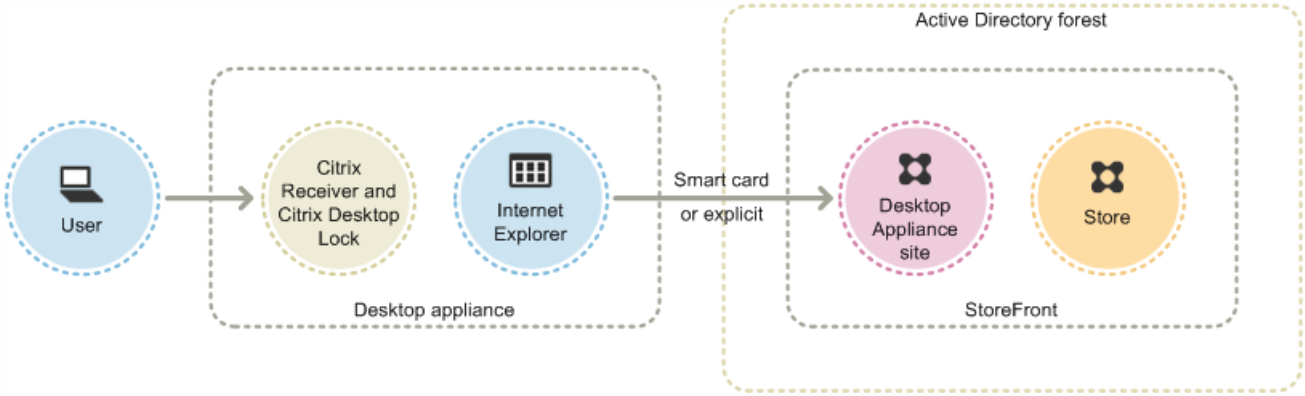
Hinweis: Wenn Sie Citrix Receiver für Windows 4.5 oder höher verwenden, können Sie einen zweiten virtuellen Server einrichten und durch Verwendung des optimalen Gateway-Routings die PIN-Eingabeaufforderungen beim Starten von Apps und Desktops vermeiden.

Benutzer können sich bei NetScaler Gateway mit Smartcard und PIN oder mit expliziten Anmeldeinformationen anmelden. Sie erhalten so die Möglichkeit, für die Anmeldung bei NetScaler Gateway auf die explizite Authentifizierung zurückzugreifen. 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.

Verwenden von Smartcards mit Desktopgerätesites

Nicht domänengebundene Windows-Desktopgeräte können so konfiguriert werden, dass Benutzer sich mit einer Smartcard an ihren Desktops anmelden können. Citrix Desktop Lock ist auf dem Gerät erforderlich und Internet Explorer muss für den Zugriff auf die Desktopgerätesite verwendet werden.

Die Abbildung zeigt die Smartcardauthentifizierung von einem nicht domänengebundenen Desktopgerät aus.



Wenn Benutzer auf Desktopgeräte zugreifen, startet Internet Explorer im Vollbildmodus und zeigt den Anmeldebildschirm für eine Desktopgerätesite an. Die Benutzer authentifizieren sich bei der Site mit ihrer Smartcard und PIN. Wenn die Desktopgerätesite für die Passthrough-Authentifizierung konfiguriert ist, werden die Benutzer automatisch authentifiziert, wenn sie auf ihre Desktops und Anwendungen zugreifen. Benutzer werden nicht aufgefordert, die PIN neu einzugeben. Ohne Passthrough-Authentifizierung müssen Benutzer ihre PIN ein zweites Mal eingeben, wenn sie einen Desktop oder

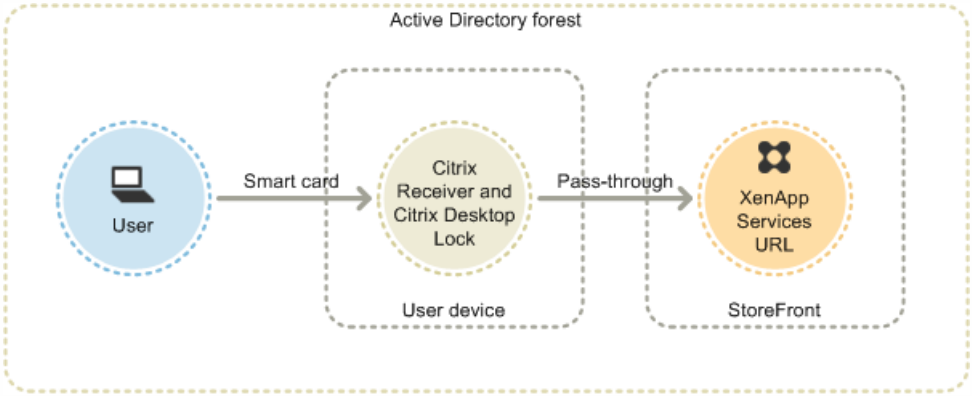
eine Anwendung starten.

Sie können Benutzern Fallback auf die explizite Authentifizierung ermöglichen, wenn diese Probleme mit ihren Smartcards haben. Hierfür konfigurieren Sie die Desktopgerätesite für die Smartcard- und die explizite Authentifizierung. In dieser Konfiguration gilt die Smartcardauthentifizierung als primäre Zugriffsmethode, Benutzer werden daher zunächst zur Eingabe ihrer PIN aufgefordert. Die Site enthält aber auch einen Link zur Anmeldung mit expliziten Anmeldeinformationen.

Verwenden von Smartcards mit XenApp Services-URLs

Benutzer domänengebundener Desktopgeräte und umfunktionierter PCs, die Citrix Desktop Lock ausführen, können sich mit Smartcards authentifizieren. Im Gegensatz zu anderen Zugriffsmethoden wird Passthrough von Smartcardanmeldeinformationen automatisch aktiviert, wenn die Smartcardauthentifizierung für eine XenApp Services-URL konfiguriert wird.

Die Abbildung zeigt die Smartcardauthentifizierung von einem domänengebundenen Gerät aus auf dem Citrix Desktop Lock ausgeführt wird.



Die Benutzer melden sich bei ihren Geräten mit Smartcard und PIN an. Citrix Desktop Lock authentifiziert dann die Benutzer automatisch bei StoreFront über die XenApp Services-URL. Benutzer werden automatisch authentifiziert, wenn sie auf ihre Desktops und Anwendungen zugreifen, und müssen ihre PIN nicht neu eingeben.

Verwenden von Smartcards mit Citrix Receiver für Web

Sie können die Smartcardauthentifizierung für Citrix Receiver für Web in der StoreFront-Verwaltungskonsole aktivieren.

1. Wählen Sie den Knoten Citrix Receiver für Web im linken Bereich aus.
2. Wählen Sie die Site aus, für die Sie die Smartcardauthentifizierung verwenden möchten.
3. Wählen Sie die Aufgabe Authentifizierungsmethoden auswählen im rechten Bereich.
4. Aktivieren Sie das Smartcardkontrollkästchen im Popupdialogfeld und klicken Sie auf OK.

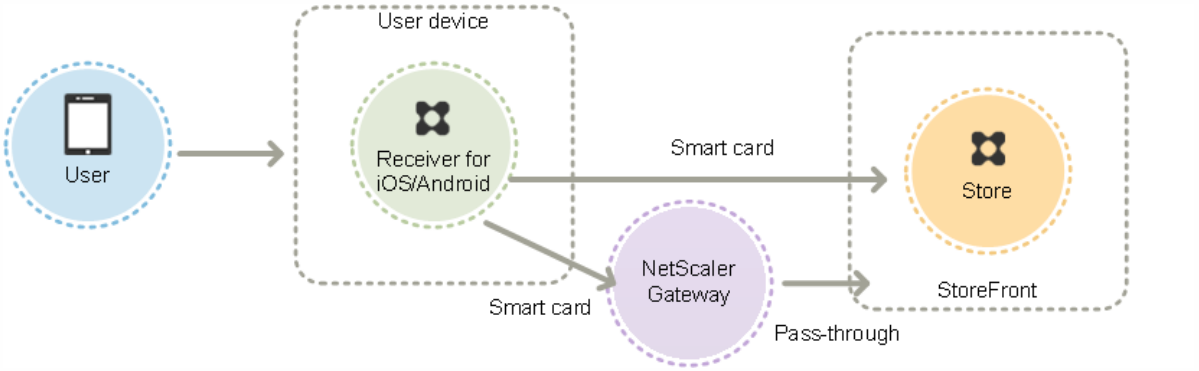
Wenn Sie die Passthrough-Authentifizierung mit Smartcards bei XenDesktop und XenApp für Citrix Receiver für Windows-Benutzer aktivieren, die domänengebundene Geräte verwenden und nicht über NetScaler Gateway auf Stores zugreifen, gilt diese Einstellung für alle Benutzer des Stores. Um die Passthrough-Authentifizierung für Domänen und mit Smartcards für Desktops und Anwendungen zu aktivieren, müssen Sie für jede Authentifizierungsmethode separate Stores erstellen. Die Benutzer müssen dann eine Verbindung mit dem für ihre Authentifizierungsmethode geeigneten Store herstellen.

Wenn Sie die Passthrough-Authentifizierung mit Smartcards bei XenDesktop und XenApp für Citrix Receiver für Windows-Benutzer aktivieren, die domänengebundene Geräte verwenden und über NetScaler Gateway auf Stores zugreifen, gilt

diese Einstellung für alle Benutzer des Stores. Wenn Sie die Passthrough-Authentifizierung für bestimmte Benutzer aktivieren und für andere die Anmeldung an Desktops und Anwendungen erzwingen möchten, müssen Sie separate Stores für jede Benutzergruppe erstellen. Dann verweisen Sie die Benutzer auf den entsprechenden Store für die Authentifizierungsmethode.

Verwenden von Smartcards mit Citrix Receiver für iOS und Android

Benutzer mit Geräten, die Citrix Receiver für iOS oder Citrix Receiver für Android ausführen, können sich mit Smartcards direkt oder über NetScaler Gateway authentifizieren. Es können nicht in Domänen eingebundene Geräte verwendet werden.



Bei Geräten im lokalen Netzwerk werden Benutzer mindestens zwei Mal zum Eingeben ihrer Anmeldeinformationen aufgefordert. Wenn sich Benutzer bei StoreFront authentifizieren oder den Store erstellen, werden sie aufgefordert, die PIN der Smartcard einzugeben. Bei entsprechender Konfiguration werden Benutzer nur dann noch einmal zur Eingabe ihrer PIN aufgefordert, wenn sie auf ihre Desktops und Anwendungen zugreifen. Hierfür aktivieren Sie die Smartcardauthentifizierung für StoreFront und installieren Smartcardtreiber auf dem VDA.

Bei diesen Citrix Receiver-Versionen können Sie Smartcards ODER Domänenanmeldeinformationen angeben. Wenn Sie einen Store für die Verwendung von Smartcards erstellt haben und mit demselben Store eine Verbindung unter Verwendung von Domänenanmeldeinformationen herstellen möchten, müssen Sie einen separaten Store ohne Aktivierung von Smartcards erstellen.

Benutzer, die eine Verbindung über NetScaler Gateway herstellen, müssen sich mindestens zwei Mal mit Smartcard und PIN anmelden, um auf ihre Desktops und Anwendungen zugreifen zu können. Benutzer authentifizieren sich mit ihrer Smartcard und PIN und werden bei entsprechender Konfiguration nur dann noch einmal zur Eingabe ihrer PIN aufgefordert, wenn sie auf ihre Desktops und Anwendungen zugreifen. Dazu aktivieren Sie die Passthrough-Authentifizierung mit NetScaler Gateway bei StoreFront und delegieren die Anmeldeinformationenvalidierung an NetScaler Gateway. Erstellen Sie dann einen weiteren virtuellen NetScaler Gateway-Server und leiten Sie über ihn die Benutzerverbindungen zu Ressourcen.

Benutzer können sich bei NetScaler Gateway mit Smartcard und PIN oder mit expliziten Anmeldeinformationen anmelden, je nachdem wie Sie die Authentifizierung für die Verbindung konfiguriert haben. 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. Wenn Sie die Authentifizierungsmethode wechseln möchten, müssen Sie die Verbindung löschen und neu erstellen.

Verwenden von Smartcards mit Citrix Receiver für Linux

Benutzer mit Geräten, auf denen Citrix Receiver für Linux ausgeführt wird, können sich mit Smartcards ähnlich wie Benutzer nicht domänengebundener Windows-Geräte authentifizieren. Selbst wenn sich ein Benutzer auf dem Linux- Gerät mit einer

Smartcard authentifiziert, gibt es in Citrix Receiver für Linux keinen Mechanismus zum Abrufen oder Wiederverwenden der eingegebenen PIN.

Konfigurieren Sie die serverseitigen Komponenten für Smartcards so, wie Sie sie für die Verwendung mit Citrix Receiver für Windows konfigurieren. Weitere Informationen finden Sie unter Konfigurieren der Smartcardauthentifizierung. Anweisungen zum Verwenden von Smartcards finden Sie unter Citrix Receiver für Linux.

Die Mindestzahl der Anmeldeaufforderungen an Benutzer ist 1. Benutzer melden sich beim Gerät an und authentifizieren sich dann bei Citrix Receiver für Linux mit ihrer Smartcard und PIN. Die Benutzer werden nicht noch einmal zur Eingabe ihrer PIN aufgefordert, wenn sie auf ihre Desktops und Anwendungen zugreifen. Aktivieren Sie hierzu die Smartcardauthentifizierung bei StoreFront.

Da die Benutzer sich direkt bei Citrix Receiver für Linux anmelden, können Sie ein Fallback auf die explizite Authentifizierung aktivieren. Wenn Sie Smartcard- und explizite Authentifizierung konfigurieren, werden Benutzer zunächst aufgefordert, sich mit der Smartcard und PIN anzumelden, können aber bei Problemen mit der Smartcard die explizite Authentifizierung auswählen.

Benutzer, die eine Verbindung über NetScaler Gateway herstellen, müssen sich mindestens einmal mit Smartcard und PIN anmelden, um auf ihre Desktops und Anwendungen zugreifen zu können. Benutzer authentifizieren sich mit ihrer Smartcard und PIN und werden bei entsprechender Konfiguration nicht noch einmal zur Eingabe ihrer PIN aufgefordert, wenn sie auf ihre Desktops und Anwendungen zugreifen. Dazu aktivieren Sie die Passthrough-Authentifizierung mit NetScaler Gateway bei StoreFront und delegieren die Anmeldeinformationenvalidierung an NetScaler Gateway. Erstellen Sie dann einen weiteren virtuellen NetScaler Gateway-Server und leiten Sie über ihn die Benutzerverbindungen zu Ressourcen.

Benutzer können sich bei NetScaler Gateway mit Smartcard und PIN oder mit expliziten Anmeldeinformationen anmelden. Sie erhalten so die Möglichkeit, für die Anmeldung bei NetScaler Gateway auf die explizite Authentifizierung zurückzugreifen. 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.

Smartcards für Citrix Receiver für Linux werden auf den XenApp Services-Supportsites nicht unterstützt.

Wenn die Smartcard-Unterstützung sowohl auf dem Server als auch in Citrix Receiver aktiviert ist und die Anwendungsrichtlinie der Smartcardzertifikate dies zulässt, können Smartcards zu folgenden Zwecken eingesetzt werden:

- Smartcard-Anmeldeauthentifizierung: Verwendung von Smartcards zur Authentifizierung von Benutzern bei Citrix XenApp- und XenDesktop-Servern.
- Smartcard-Anwendungsunterstützung: Zugriff auf lokale Smartcardgeräte über smartcardfähige veröffentlichte Anwendungen.

Verwenden von Smartcards für XenApp Services-Support

Benutzer, die sich bei XenApp Services-Supportsites zum Starten von Anwendungen und Desktops anmelden, können sich ohne spezielle Hardware, Betriebssysteme und Citrix Receiver mit Smartcards authentifizieren. Wenn ein Benutzer auf eine XenApp Services-Supportsite zugreift und erfolgreich eine Smartcard und PIN eingibt, ermittelt PNA die Identität des Benutzers, authentifiziert diesen bei StoreFront und gibt die verfügbaren Ressourcen zurück.

Damit Passthrough- und Smartcardauthentifizierung funktionieren, müssen Sie die Option "An XML-Dienst gesendeten Anfragen vertrauen" aktivieren.

Starten Sie mit einem Konto mit lokalen Administratorrechten auf dem Delivery Controller Windows PowerShell und geben Sie an der Eingabeaufforderung die folgenden Befehle ein, damit der Delivery Controller von StoreFront gesendeten XML-Anfragen vertraut. Die folgenden Schritte gelten für XenApp 7.5 bis 7.8 sowie für XenDesktop 7.0 bis 7.8.

1. Laden Sie die Citrix Cmdlets durch Eingeben von asnp Citrix*. (einschließlich dem Punkt).
2. Geben Sie **Add-PSSnapin citrix.broker.admin.v2** ein.
3. Geben Sie **Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $True** ein.
4. Schließen Sie PowerShell.

Weitere Informationen zur Konfiguration der Smartcardauthentifizierung für XenApp Services-Support finden Sie unter Konfigurieren der Authentifizierung für XenApp Services-URLs.

Wichtige Hinweise

Die Verwendung von Smartcards für die Benutzerauthentifizierung bei StoreFront unterliegt den folgenden Anforderungen und Einschränkungen.

- Zur Verwendung eines VPN-Tunnels (virtuelles privates Netzwerk) mit Smartcardauthentifizierung müssen Benutzer das NetScaler Gateway Plug-In installieren und sich über eine Webseite anmelden, wobei sie sich für jeden Schritt mit Smartcard und PIN authentifizieren. Die Passthrough-Authentifizierung bei StoreFront mit dem NetScaler Gateway Plug-In ist für Smartcardbenutzer nicht verfügbar.
- Auf einem Benutzergerät können mehrere Smartcards und mehrere Smartcardleser verwendet werden. Wenn Sie jedoch die Passthrough-Authentifizierung mit Smartcard aktivieren, müssen Benutzer darauf achten, dass beim Zugriff auf einen Desktop oder eine Anwendung nur eine Smartcard eingeführt ist.
- Wird eine Smartcard innerhalb einer Anwendung verwendet (z. B. zur digitalen Signierung oder zur Verschlüsselung), werden möglicherweise zusätzliche Aufforderungen zum Einführen einer Smartcard oder zur Eingabe einer PIN angezeigt. Dieser Fall kann eintreten, wenn eine oder mehrere Smartcards gleichzeitig eingelegt wurden. Er kann auch aufgrund von Konfigurationseinstellungen eintreten, z. B. bei Middleware-Einstellungen wie PIN-Zwischenspeicherung, die in der Regel mit der Gruppenrichtlinie konfiguriert werden. Benutzer, die zum Einführen einer Smartcard aufgefordert werden, obwohl bereits eine Smartcard einliegt, müssen auf Abbrechen klicken. Wenn Benutzer aufgefordert werden, ein PIN einzugeben, müssen sie die PIN neu eingeben.
- Wenn Sie die Passthrough-Authentifizierung mit Smartcards bei XenDesktop und XenApp für Citrix Receiver für Windows-Benutzer aktivieren, die domänengebundene Geräte verwenden und nicht über NetScaler Gateway auf Stores zugreifen, gilt diese Einstellung für alle Benutzer des Stores. Um die Passthrough-Authentifizierung für Domänen und mit Smartcards für Desktops und Anwendungen zu aktivieren, müssen Sie für jede Authentifizierungsmethode separate Stores erstellen. Die Benutzer müssen dann eine Verbindung mit dem für ihre Authentifizierungsmethode geeigneten Store herstellen.
- Wenn Sie die Passthrough-Authentifizierung mit Smartcards bei XenDesktop und XenApp für Citrix Receiver für Windows-Benutzer aktivieren, die domänengebundene Geräte verwenden und über NetScaler Gateway auf Stores zugreifen, gilt diese Einstellung für alle Benutzer des Stores. Wenn Sie die Passthrough-Authentifizierung für bestimmte Benutzer aktivieren und für andere die Anmeldung an Desktops und Anwendungen erzwingen möchten, müssen Sie separate Stores für jede Benutzergruppe erstellen. Dann verweisen Sie die Benutzer auf den entsprechenden Store für die Authentifizierungsmethode.
- Nur eine Authentifizierungsmethode kann für jede XenApp Services-URL konfiguriert werden und pro Store ist nur eine URL verfügbar. Wenn Sie zusätzlich zur Smartcardauthentifizierung weitere Authentifizierungsmethoden aktivieren möchten, müssen Sie für jede Authentifizierungsmethode einen eigenen Store mit einer XenApp Services-URL erstellen. Dann verweisen Sie die Benutzer auf den entsprechenden Store für die Authentifizierungsmethode.
- Wenn StoreFront installiert ist, erfordert die Standardkonfiguration in Microsoft Internetinformationsdienste (IIS) nur,

dass Clientzertifikate für HTTPS-Verbindungen mit der URL für die Zertifikatauthentifizierung des StoreFront-Authentifizierungsdiensts präsentiert werden. IIS fordert keine Clientzertifikate für andere StoreFront-URLs an. Dank dieser Konfiguration können Sie Smartcardbenutzern die Option des Fallbacks auf die explizite Authentifizierung gewähren, wenn diese Probleme mit ihren Smartcards haben. Abhängig von den entsprechenden Windows-Richtlinieneinstellungen können Benutzer auch ihre Smartcard entfernen, ohne sich neu authentifizieren zu müssen.

Wenn Sie IIS für die Anforderung von Clientzertifikaten für alle HTTPS-Verbindungen mit allen StoreFront-URLs konfigurieren, müssen Authentifizierungsdienst und Stores auf demselben Server sein. Sie müssen ein Clientzertifikat verwenden, das für alle Stores gültig ist. Innerhalb dieser IIS-Sitekonfiguration können Smartcardbenutzer keine Verbindung über NetScaler Gateway herstellen und nicht auf die explizite Authentifizierung zurückgreifen. Sie müssen sich dann neu anmelden, wenn sie ihre Smartcards aus Geräten entfernen.

Optimieren der Benutzererfahrung

Feb 26, 2018

StoreFront hat Features zur Verbesserung der Benutzererfahrung. Diese sind standardmäßig konfiguriert, wenn Sie neue Stores und die zugehörigen Citrix Receiver für Web-Sites, Desktopgerätesites und XenApp Services-URLs erstellen.

Workspace Control

Wenn Benutzer zwischen Geräten wechseln, wird von Workspace Control sichergestellt, dass die benutzten Anwendungen ihnen folgen. Benutzer können mit den gleichen Anwendungsinstanzen über mehrere Geräte hinweg arbeiten anstatt alle Anwendungen neu starten zu müssen, wenn sie sich an einem neuen Gerät anmelden. So können etwa Krankenhausärzte Zeit sparen, wenn sie sich von Arbeitsstation zu Arbeitsstation bewegen und auf Patientendaten zugreifen.

Workspace Control ist standardmäßig für Citrix Receiver für Web-Sites und Verbindungen mit Stores über XenApp Services-URLs aktiviert. Wenn Benutzer sich anmelden, werden sie automatisch mit allen Anwendungen wiederverbunden, die sie nicht beendet haben. Beispiel: Ein Benutzer meldet sich über die Citrix Receiver für Web-Site oder die XenApp Services-URL bei einem Store an und startet einige Anwendungen. Wenn der Benutzer sich anschließend bei dem gleichen Store mit der gleichen Zugriffsmethode aber auf einem anderen Gerät anmeldet, werden die ausgeführten Anwendungen automatisch auf das neue Gerät übertragen. Alle Anwendungen, die ein Benutzer über einen bestimmten Store startet, werden bei Abmeldung des Benutzers von dem Store automatisch getrennt, jedoch nicht heruntergefahren. Bei Citrix Receiver für Web-Sites muss für Anmeldung, Anwendungsstart und Abmeldung der gleiche Browser verwendet werden.

Workspace Control für XenApp Services-URLs kann nicht konfiguriert oder deaktiviert werden. Weitere Informationen zum Konfigurieren von Workspace Control für Citrix Receiver für Web-Sites finden Sie unter Konfigurieren von Workspace Control.

Die Verwendung von Workspace Control auf Citrix Receiver für Web-Sites unterliegt den folgenden Anforderungen und Einschränkungen.

- Workspace Control ist nicht verfügbar, wenn Citrix Receiver für Web-Sites über gehostete Desktops und Anwendungen aufgerufen werden.
- Bei Benutzern, die über Windows-Geräte auf Citrix Receiver für Web-Sites zugreifen, ist Workspace Control nur dann aktiviert, wenn die Site feststellen kann, dass Citrix Receiver auf den Geräten der Benutzer installiert ist oder wenn Receiver für HTML5 für den Zugriff auf Ressourcen verwendet wird.
- Um eine Verbindung zu getrennten Anwendungen wiederherzustellen, müssen Benutzer, die über Internet Explorer auf Citrix Receiver für Web-Sites zugreifen, die Site den Zonen "Lokales Intranet" oder "Vertrauenswürdige Sites" hinzufügen.
- Wenn nur ein Desktop für einen Benutzer auf einer Citrix Receiver für Web-Site verfügbar ist, die so konfiguriert ist, dass einzelne Desktops bei Anmeldung automatisch gestartet werden, erfolgt unabhängig von der Workspace Control-Konfiguration keine Wiederverbindung der Anwendungen des Benutzers.
- Benutzer müssen die Verbindung zu ihren Anwendungen mit demselben Browser trennen, den sie ursprünglich zum Starten der Anwendungen verwendet haben. Verbindungen mit Ressourcen, die mit einem anderen Browser oder lokal vom Desktop bzw. über das Menü Start mit Citrix Receiver gestartet wurden, können nicht mit Citrix Receiver für Web-Sites getrennt oder heruntergefahren werden.

Inhaltsumleitung

Wenn Benutzer die entsprechende Anwendung abonniert haben, ermöglicht die Inhaltsumleitung, dass Benutzer Dateien auf ihren lokalen Geräten mit den abonnierten Anwendungen öffnen können. Um die Umleitung lokaler Dateien zu

aktivieren, verknüpfen Sie die Anwendung in XenDesktop oder XenApp mit den erforderlichen Dateitypen. Die Dateitypzuordnung ist für neue Stores standardmäßig aktiviert. Weitere Informationen finden Sie unter Deaktivieren der Dateitypzuordnung.

Benutzerseitige Kennwortänderung

Sie können Benutzern von Citrix Receiver für Web-Sites, die sich mit Microsoft Active Directory-Domänenanmeldeinformationen anmelden, gestatten, ihre Kennwörter jederzeit zu ändern. Alternativ können Sie die Kennwortänderung auf Benutzer beschränken, deren Kennwort abgelaufen ist. So können Sie sicherstellen, dass Benutzern nie der Zugriff auf ihre Desktops und Anwendungen verweigert wird, weil ein Kennwort abgelaufen ist.

Wenn Sie zulassen, dass Benutzer von Citrix Receiver für Web-Sites ihre Kennwörter jederzeit ändern können, wird lokalen Benutzern, deren Kennwörter bald ablaufen, beim Anmelden eine Warnung angezeigt. Standardmäßig hängt der Benachrichtigungszeitraum von der entsprechenden Windows-Richtlinieneinstellung ab. Warnungen über den Ablauf von Kennwörtern werden nur für Benutzer angezeigt, die eine Verbindung über das interne Netzwerk herstellen. Weitere Informationen zum Aktivieren der Kennwortänderung durch Benutzer finden Sie unter Konfigurieren des Authentifizierungsdiensts.

Benutzer, die sich an Desktopgerätesites anmelden, können nur abgelaufene Kennwörter ändern, selbst wenn Sie zulassen, dass Benutzer ihr Kennwort jederzeit ändern können. Desktopgerätesites bieten keine Steuerelemente zur Kennwortänderung, nachdem sich Benutzer angemeldet haben.

Beim Erstellen des Authentifizierungsdiensts verhindert die Standardkonfiguration, dass Benutzer von Citrix Receiver für Web-Sites ihre Kennwörter ändern, selbst wenn die Kennwörter abgelaufen sind. Wenn Sie diese Funktion aktivieren, vergewissern Sie sich, dass die Richtlinien für die Domänen mit Ihren Servern nicht die Benutzer davon abhalten, ihre Kennwörter zu ändern. StoreFront muss eine Verbindung mit dem Domänencontroller herstellen können, um die Kennwörter der Benutzer zu ändern.

Wenn Benutzer Kennwörter ändern können, werden vertrauliche Sicherheitsfunktionen für alle Personen offengelegt, die auf einen der Stores, die diesen Authentifizierungsdienst verwenden, zugreifen können. Wenn Ihr Unternehmen eine Sicherheitsrichtlinie hat, die Funktionen zur Änderung des Kennworts nur zur internen Verwendung reserviert, stellen Sie sicher, dass auf keinen der Stores von außerhalb des Unternehmensnetzwerks zugegriffen werden kann.

Ansichten für Desktops und Anwendungen bei Citrix Receiver für Web-Sites

Wenn sowohl Desktops als auch Anwendungen über eine Citrix Receiver für Web-Site verfügbar sind, werden standardmäßig separate Ansichten für Desktops und Anwendungen angezeigt. Benutzern wird nach der Anmeldung an der Site zuerst die Desktopansicht angezeigt. Wenn nur ein einziger Desktop für einen Benutzer auf einer Citrix Receiver für Web-Site verfügbar ist, startet die Site diesen Desktop automatisch, wenn sich der Benutzer anmeldet, unabhängig davon, ob auch Anwendungen verfügbar sind. Sie können angeben, welche Ansichten für die Sites angezeigt werden, und verhindern, dass Citrix Receiver für Web-Sites Desktops für Benutzer automatisch starten. Weitere Informationen finden Sie unter Konfigurieren der Anzeige von Ressourcen für Benutzer.

Das Verhalten der Ansichten bei Citrix Receiver für Web-Sites hängt davon ab, welche Ressourcentypen bereitgestellt werden. Beispielsweise müssen Benutzer Anwendungen abonnieren, bevor sie in der Anwendungsansicht angezeigt werden. Dagegen werden alle für einen Benutzer verfügbaren Desktops automatisch in der Desktopansicht angezeigt. Aus diesem Grund können Benutzer keine Desktops aus der Desktopansicht entfernen oder die Desktops durch Ziehen und Ablegen der Symbole neu anordnen. Wenn der XenDesktop-Administrator Desktopneustarts aktiviert hat, werden in der Desktopansicht Steuerelemente angezeigt, mit denen Benutzer ihre Desktops neu starten können. Wenn Benutzer über eine einzelne Desktopgruppe auf mehrere Instanzen eines Desktops zugreifen können, kennzeichnen Citrix Receiver für

Web-Sites die Desktops für die Benutzer, indem eine Ziffer an den Desktopnamen angehängt wird.

Für Benutzer, die eine Verbindung mit Stores in Citrix Receiver oder über XenApp Services-URLs herstellen, wird die Art und Weise, in der Desktops und Anwendungen angezeigt werden, sowie deren Verhalten von dem verwendeten Citrix Client bestimmt.

Zusätzliche Empfehlungen

Bei der Bereitstellung von Anwendungen mit XenDesktop und XenApp sollten Sie die folgenden Optionen in Betracht ziehen, um die Benutzererfahrung beim Zugriff auf Anwendungen über Stores zu verbessern. Weitere Informationen zur Bereitstellung von Anwendungen finden Sie unter Erstellen einer Bereitstellungsgruppenanwendung.

- Gruppieren Sie Anwendungen in Ordnern, damit Benutzer die benötigten Anwendungen leichter finden, wenn sie durch die verfügbaren Ressourcen navigieren. Ordner, die Sie in XenDesktop und XenApp erstellen, werden als Kategorien in Citrix Receiver angezeigt. Sie können beispielsweise Anwendungen nach Typ gruppieren oder alternativ Ordner für verschiedene Benutzerrollen in der Organisation erstellen.
- Verwenden Sie aussagekräftige Beschreibungen für veröffentlichte Anwendungen, da diese Beschreibungen in Citrix Receiver angezeigt werden.
- Sie können für alle Benutzer einen Kern von Anwendungen festlegen, die sich nicht vom Citrix Receiver-Homebildschirm entfernen lassen. Hängen Sie dazu die Zeichenfolge KEYWORDS:Mandatory an die Anwendungsbeschreibung an. Benutzer können weiter die Self-Service-Benutzeroberfläche verwenden, um nicht vorgegebene Anwendungen hinzuzufügen oder zu entfernen.
- Sie können eine Anwendung automatisch für alle Benutzer eines Stores abonnieren, indem Sie die Zeichenfolge KEYWORDS:Auto an die Beschreibung anhängen, die Sie beim Veröffentlichen der Anwendung angeben. Wenn Benutzer sich am Store anmelden, wird die Anwendung automatisch bereitgestellt, ohne dass die Benutzer sie manuell abonnieren müssen.
- Aktivieren Sie bei der Konfiguration der Anwendungseinstellungen das Kontrollkästchen App is available in Citrix Receiver to all users automatically, wenn eine Web- oder SaaS (Software-as-a-Service)-Anwendung, die von App Controller verwaltet wird, für alle Benutzer im Abonnement bereitgestellt werden soll.
- Kündigen Sie die XenDesktop-Anwendungen den Benutzern an oder sorgen Sie dafür, dass häufig verwendete Anwendungen leichter gefunden werden, indem Sie sie in der Liste Highlights in Citrix Receiver aufführen. Hängen Sie dazu die Zeichenfolge KEYWORDS:Featured an die Anwendungsbeschreibung an.
  Hinweis: Mehrere Schlüsselwörter müssen ausschließlich durch Leerzeichen voneinander getrennt werden, z. B. KEYWORDS:Auto Featured.
- Standardmäßig werden freigegebene, von XenDesktop und XenApp gehostete Desktops von Citrix Receiver für Web-Sites wie andere Desktops behandelt. Hängen Sie die Zeichenfolge KEYWORDS:TreatAsApp an die Desktopbeschreibung an, um dieses Verhalten zu ändern. Der Desktop wird dann in den Anwendungsansichten von Citrix Receiver für Web-Sites statt den Desktopansichten angezeigt und Benutzer müssen ihn abonnieren, um darauf zugreifen zu können. Außerdem wird der Desktop nicht automatisch gestartet, wenn sich der Benutzer bei der Citrix Receiver für Web-Site anmeldet, und er wird nicht mit Desktop Viewer aufgerufen, selbst wenn die Site so konfiguriert wurde, dass dies bei anderen Desktops der Fall ist.
- Für Windows-Benutzer können Sie festlegen, dass die lokal installierte Version einer Anwendung bevorzugt vor einer übermittelten Instanz verwendet wird, wenn beide verfügbar sind. Fügen Sie hierfür die Zeichenfolge **KEYWORDS:prefer="application"** an die Anwendungsbeschreibung an. application ist hierbei mindestens ein vollständiges Wort aus dem Namen der lokalen Anwendung, und zwar gemäß dem Dateinamen der Verknüpfungsdatei oder dem absoluten Pfad (einschließlich dem Namen der ausführbaren Datei) der lokalen Anwendung aus dem Ordner "\Startmenü". Wenn ein Benutzer eine Anwendung mit diesem Schlüsselwort abonniert, sucht Citrix Receiver nach dem angegebenen Namen oder Pfad auf dem Gerät des Benutzers, um zu ermitteln, ob die Anwendung bereits lokal installiert

ist. Wird die Anwendung gefunden, abonniert Citrix Receiver die übermittelte Anwendung für den Benutzer, erstellt jedoch keine Verknüpfung. Wenn der Benutzer die übermittelte Anwendung mit Citrix Receiver startet, wird stattdessen die lokal installierte Instanz ausgeführt. Weitere Informationen finden Sie unter Konfigurieren der Anwendungsbereitstellung.

- In XenApp und XenDesktop 7.17, wenn Benutzer eine veröffentlichte Anwendung auf einem veröffentlichten Desktop starten, können Administratoren steuern, ob die Anwendung in der Desktopsitzung oder als veröffentlichte Anwendung in derselben Bereitstellungsgruppe gestartet wird. Verwenden Sie ein PowerShell-Cmdlet für den Brokerdienst und eine Richtlinieneinstellung in Citrix Receiver für Windows (vPrefer), um dieses Verhalten zu steuern. Diese Funktion funktioniert nur, wenn Citrix Receiver für Windows für das Starten von veröffentlichten Apps verwendet wird. Sie kann nicht verwendet werden, um eine App lokal zu starten, wenn die veröffentlichte App über die StoreFront-Site in einem Webbrowser gestartet wird. In früheren Releases erforderte der Double-Hop-Anwendungstart die Verwendung des Tags KEYWORDS:Prefer in Studio. Das Tag KEYWORDS:Prefer kann weiterhin verwendet werden. Wenn sowohl die KEYWORDS-Methode als auch die vPrefer-Methode konfiguriert wurden, hat vPrefer Vorrang.

  Weitere Informationen finden Sie in CTX232210, im Artikel Anwendungen unter XenApp und XenDesktop sowie in der Dokumentation von Citrix Receiver für Windows.

Hohe Verfügbarkeit und Multisitekonfiguration für StoreFront

Nov 27, 2017

StoreFront enthält eine Reihe von Features, die zusammen Lastausgleich und Failover zwischen den Bereitstellungen von Ressourcen für Stores bieten. Sie können auch zur Erhöhung der Systemstabilität dedizierte Bereitstellungen für die Notfallwiederherstellung spezifizieren. Mit diesen Features können Sie StoreFront-Bereitstellungen, die über mehrere Sites verteilt sind, für hohe Verfügbarkeit für die Stores konfigurieren. Weitere Informationen finden Sie unter Einrichten hoch verfügbarer Stores mit mehreren Sites.

Ressourcenaggregation

Standardmäßig werden in StoreFront alle Bereitstellungen, die Desktops und Anwendungen für einen Store bieten, aufgelistet und alle entsprechenden Ressourcen als separat behandelt. Wenn die gleiche Ressource aus mehreren Bereitstellungen verfügbar ist, sehen Benutzer daher ein Symbol für jede Ressource, was verwirrend sein kann, wenn die Ressourcen den gleichen Namen haben. Wenn Sie hoch verfügbare Multisitekonfigurationen einrichten, können Sie XenDesktop- und XenApp-Bereitstellungen, die den gleichen Desktop oder die gleiche Anwendung anbieten, so gruppieren, dass identische Ressourcen für Benutzer aggregiert werden können. Gruppierte Bereitstellungen müssen nicht identisch sein, aber Ressourcen müssen für die Aggregation den gleichen Namen und Pfad auf jedem Server haben.

Wenn ein Desktop oder eine Anwendung aus mehreren, für einen bestimmten Store konfigurierten XenDesktop- oder XenApp-Bereitstellungen verfügbar ist, werden alle Instanzen der Ressource in StoreFront aggregiert und den Benutzern wird ein einzelnes Symbol angezeigt. App Controller-Anwendungen können nicht aggregiert werden. Wenn ein Benutzer eine aggregierte Ressource startet, bestimmt StoreFront die für den Benutzer am besten geeignete Instanz der Ressource auf der Grundlage der Serververfügbarkeit, der Tatsache, ob der Benutzer bereits eine aktive Sitzung hat, und der Reihenfolge, die Sie in der Konfiguration angegeben haben.

StoreFront überwacht dynamisch Server, die nicht auf Anforderungen reagieren, auf der Basis, dass solche Server entweder überlastet oder vorübergehend nicht verfügbar sind. Benutzer werden zu Ressourceninstanzen auf anderen Servern umgeleitet, bis die Kommunikation wiederhergestellt ist. Wenn die Server, auf denen die Ressourcen bereitgestellt werden, dies unterstützen, versucht StoreFront eine Wiederverwendung vorhandener Sitzungen, um zusätzliche Ressourcen zu liefern. Wenn ein Benutzer bereits eine aktive Sitzung auf einer Bereitstellung hat, die auch die angeforderte Ressource umfasst, verwendet StoreFront diese Sitzung, wenn sie mit der Ressource kompatibel ist. Durch Minimieren der Anzahl Sitzungen für jeden Benutzer wird die Zeit zum Starten zusätzlicher Desktops oder Anwendungen reduziert und ggf. eine effizientere Verwendung von Produktlizenzen ermöglicht.

Nach der Überprüfung auf Verfügbarkeit und vorhandene Benutzersitzungen verwendet StoreFront die in der Konfiguration angegebene Reihenfolge zur Bestimmung der Bereitstellung, mit der der Benutzer verbunden wird. Wenn dem Benutzer mehrere äquivalente Bereitstellungen zur Verfügung stehen, können Sie festlegen, dass eine Verbindung mit der ersten verfügbaren Bereitstellung oder per Zufallsprinzip mit einer beliebigen Bereitstellung in der Liste erfolgt. Die Verbindung von Benutzern mit der ersten verfügbaren Bereitstellung ermöglicht eine Minimierung der Anzahl der von den aktuellen Benutzern verwendeten Bereitstellungen. Die Verbindung per Zufallsprinzip erzielt eine gleichmäßigere Verteilung der Benutzer über alle verfügbaren Bereitstellungen.

Sie können die angegebene Reihenfolge der Bereitstellungen für einzelne XenDesktop- und XenApp-Ressourcen außer Kraft setzen und bevorzugte Bereitstellungen definieren, mit denen Benutzer bei Zugriff auf einen bestimmten Desktop

oder eine bestimmte Anwendung verbunden werden. Damit können Sie z. B. festlegen, dass Benutzer bevorzugt mit einer speziell für einen bestimmten Desktop oder eine bestimmte Anwendung angepassten Bereitstellung verbunden werden, für andere Ressourcen jedoch andere Bereitstellungen verwenden. Fügen Sie zu diesem Zweck die Zeichenfolge KEYWORDS:Primary an die Beschreibung des Desktops oder der Anwendung in der bevorzugten Bereitstellung an und KEYWORDS:Secondary an die Ressource in anderen Bereitstellungen. Soweit möglich, werden Benutzer unabhängig von der Reihenfolge der Bereitstellungen in der Konfiguration mit der Bereitstellung mit der primären Ressource verbunden.Benutzer werden mit Bereitstellungen mit sekundären Ressourcen verbunden, wenn die bevorzugte Bereitstellung nicht verfügbar ist.

Zuordnen von Benutzern zu Ressourcen

Standardmäßig wird Benutzern beim Zugriff auf einen Store ein Aggregat aller verfügbaren Ressourcen aus allen für den Store konfigurierten Bereitstellungen angezeigt. Um unterschiedlichen Benutzern eigene Ressourcen bereitzustellen, können Sie separate Stores oder sogar separate StoreFront-Bereitstellungen konfigurieren. Wenn Sie jedoch eine Multisitekonfiguration mit hoher Verfügbarkeit einrichten, können Sie den Zugriff auf bestimmte Bereitstellungen auf der Basis der Mitgliedschaft der Benutzer bei Microsoft Active Directory-Gruppen konfigurieren. So können Sie für verschiedene Benutzergruppen verschiedene Benutzererfahrungen über einen einzelnen Store konfigurieren.

Sie können z. B. allgemeine Ressourcen für alle Benutzer in einer Bereitstellung gruppieren und Finanzanwendungen für die Buchhaltungsabteilung in einer anderen. In einer solchen Konfiguration sieht ein Benutzer, der kein Mitglied der Benutzergruppe "Buchhaltung" ist, nur die allgemeinen Ressourcen, wenn er auf den Store zugreift. Ein Mitglied der Gruppe "Buchhaltung" sieht neben den allgemeinen Ressourcen auch die Finanzanwendungen.

Für Poweruser können Sie auch eine Bereitstellung erstellen, die dieselben Ressourcen wie die anderen Bereitstellungen enthält, jedoch auf schnellerer und leistungsfähigerer Hardware beruht. So können Sie eine verbesserte Benutzererfahrung für wichtige Benutzer, wie etwa Führungskräfte, bereitstellen. Alle Benutzer sehen bei der Anmeldung bei einem Store die gleichen Desktops und Anwendungen, die Mitglieder der Gruppe "Führungskräfte" werden jedoch bevorzugt mit den Ressourcen der Bereitstellung für Poweruser verbunden.

Abonnementsynchronisierung

Wenn Sie Benutzern den Zugriff auf dieselben Anwendungen aus ähnlichen Stores in unterschiedlichen StoreFront-Bereitstellungen ermöglichen, müssen die Anwendungsabonnements der Benutzer zwischen den Servergruppen synchronisiert werden. Andernfalls müssen Benutzer, die eine Anwendung in einem Store in einer StoreFront-Bereitstellung abonniert haben, beim Anmelden bei einer anderen Servergruppe diese möglicherweise neu abonnieren. Zur Gewährleistung einer nahtlosen Benutzererfahrung beim Wechsel zwischen StoreFront Bereitstellungen können Sie eine regelmäßige Synchronisierung der Anwendungsabonnements zwischen den Stores in verschiedenen Servergruppen konfigurieren. Wählen Sie zwischen einer regelmäßigen Synchronisierung nach bestimmten Intervallen oder einer für bestimmte Tageszeiten geplanten Synchronisierung. Weitere Informationen finden Sie unter Konfigurieren der Abonnementsynchronisierung.

Dedizierte Ressourcen für die Notfallwiederherstellung

Sie können spezifische Bereitstellungen für die Notfallwiederherstellung konfigurieren, die nur verwendet werden, wenn alle anderen Bereitstellungen nicht verfügbar sind. In der Regel befinden sich Bereitstellungen für die Notfallwiederherstellung nicht am gleichen Standort wie Hauptbereitstellungen, sie enthalten nur eine Teilmenge der normalerweise verfügbaren Ressourcen und sie bieten ggf. eine beeinträchtigte Benutzererfahrung. Wenn Sie festlegen, dass eine Bereitstellung für die Notfallwiederherstellung verwendet werden soll, wird sie für Lastausgleich oder Failover nicht verwendet. Benutzer können nur dann auf die Desktops und Anwendungen der Bereitstellung für die Notfallwiederherstellung zugreifen, wenn alle anderen Bereitstellungen, für die letztere eingerichtet wurde, nicht mehr verfügbar sind.

Ist der Zugriff auf eine andere Bereitstellung wieder möglich, können Benutzer keine weitere Ressourcen der

Notfallwiederherstellung starten, selbst wenn sie bereits eine dieser Ressourcen verwenden. Benutzer, die Ressourcen der Notfallwiederherstellung verwenden, werden nicht von diesen Ressourcen getrennt, wenn der Zugriff auf andere Bereitstellungen wieder möglich wird. Sobald sie eine der Ressourcen für die Notfallwiederherstellung beendet haben, können sie diese jedoch nicht wieder starten. Genauso gilt, dass StoreFront keine Wiederverwendung vorhandener Sitzungen mit Bereitstellungen für die Notfallwiederherstellung versucht, wenn zwischenzeitlich andere Bereitstellungen wieder verfügbar geworden sind.

Optimales NetScaler Gateway-Routing

Wenn Sie konfigurierte separate NetScaler Gateway-Geräte für die Bereitstellungen haben, können Sie mit StoreFront das optimale Gerät für den Zugriff auf die Bereitstellungen mit den Ressourcen für einen Store definieren. Beispiel: Wenn Sie einen Store mit aggregierten Ressourcen aus zwei geografischen Standorten erstellen, von denen jeder ein NetScaler Gateway-Gerät hat, können Benutzer, die eine Verbindung über das Gerät an einem Standort herstellen, einen Desktop oder eine Anwendung am anderen Standort starten. Standardmäßig wird die Verbindung jedoch über das Gerät geleitet, mit dem der Benutzer ursprünglich eine Verbindung hergestellt hat, sodass das Unternehmens-WAN durchquert werden muss.

Zur Verbesserung der Benutzererfahrung und zur Reduzierung des Netzwerkdatenverkehrs im WAN können Sie das optimale NetScaler Gateway-Gerät für jede Bereitstellung festlegen. Mit dieser Konfiguration werden Benutzerverbindungen automatisch über das lokal zur Bereitstellung mit den Ressourcen vorliegende Gerät geleitet, unabhängig von dem Standort des Geräts, über das der Benutzer auf den Store zugreift.

Das optimale NetScaler Gateway-Routing können Sie auch in dem Spezialfall verwenden, wo lokale Benutzer im internen Netzwerk sich für die Endpunktanalyse an NetScaler Gateway anmelden müssen. Mit dieser Konfiguration stellen Benutzer eine Verbindung mit dem Store über das NetScaler Gateway-Gerät her, allerdings muss die Verbindung nicht über das Gerät zu der Ressource geleitet werden, weil die Benutzer im internen Netzwerk sind. In diesem Fall aktivieren Sie das optimale Routing, geben aber kein Gerät für die Bereitstellung an, sodass Benutzerverbindungen mit Desktops und Anwendungen direkt und nicht über NetScaler Gateway geleitet werden. Sie müssen auch eine spezifische interne virtuelle Server-IP-Adresse für das NetScaler Gateway-Gerät konfigurieren. Außerdem müssen Sie einen nicht zugänglichen internen Beacon festlegen, damit Citrix Receiver unabhängig vom Netzwerkstandort des Benutzers immer angefordert wird, eine Verbindung zu NetScaler Gateway herzustellen.

Globaler Serverlastausgleich mit NetScaler Gateway

StoreFront unterstützt für den globalen Serverlastausgleich konfigurierte NetScaler Gateway-Bereitstellungen mit mehreren Geräten, die mit einem einzelnen vollqualifizierten Domänennamen (FQDN) konfiguriert sind. Für die Benutzerauthentifizierung und das Routing der Verbindungen über das richtige Gerät muss StoreFront zwischen den Geräten unterscheiden können. Da der Geräte-FQDN in einer Konfiguration mit globalem Serverlastausgleich nicht als eindeutige ID verwendet werden kann, müssen Sie StoreFront mit eindeutigen IP-Adressen für alle Geräte konfigurieren. Normalerweise ist dies die IP-Adresse des virtuellen Servers für NetScaler Gateway.

Weitere Informationen über den Lastausgleich finden Sie unter Lastausgleich mit NetScaler.

Wichtige Hinweise

Bei der Entscheidung, ob Sie hoch verfügbare Multisitekonfigurationen für Ihre Stores einrichten, sollten Sie die folgenden Anforderungen und Einschränkungen in Betracht ziehen.

- Desktops und Anwendungen müssen für eine Aggregation auf jedem Server denselben Namen und Pfad haben. Außerdem müssen die Eigenschaften der aggregierten Ressourcen, wie Namen und Symbole, identisch sein. Ist dies nicht der Fall, sehen Benutzer evtl. eine Änderung der Eigenschaften ihrer Ressourcen, wenn Citrix Receiver die verfügbaren

Ressourcen auflistet.

- Zugewiesene Desktops, sowohl vorab zugewiesene und solche, die bei der ersten Verwendung zugewiesen werden, sollten nicht aggregiert werden. Stellen Sie sicher, das Bereitstellungsgruppen, die solche Desktops enthalten, nicht den gleichen Namen und Pfad in Sites haben, die Sie für die Aggregation konfigurieren.
- App Controller-Anwendungen können nicht aggregiert werden.
- Wenn Sie die Synchronisierung der Anwendungsabonnements von Benutzern zwischen Stores in separaten StoreFront-Bereitstellungen konfigurieren, müssen die Stores in jeder Servergruppe denselben Namen haben. Außerdem müssen beide Servergruppen in der Active Directory-Domäne mit den Benutzerkonten residieren oder aber in einer Domäne die mit dieser eine Vertrauensstellung hat.
- StoreFront bietet nur Zugriff auf Backupbereitstellungen für die Notfallwiederherstellung, wenn alle primären Sites im äquivalenten Bereitstellungssatz nicht verfügbar sind. Wird eine Backupbereitstellung von mehreren äquivalenten Bereitstellungssätzen verwendet, können Benutzer erst dann auf die Ressourcen für die Notfallwiederherstellung zugreifen, wenn alle primären Sites in jedem Bereitstellungssatz nicht verfügbar sind.

Installieren, Einrichten, Upgrade durchführen und Deinstallieren

Jun 04, 2018

Vorbereiten der Installation

Führen Sie die nachfolgend beschriebenen Schritte aus, um StoreFront zu installieren und zu konfigurieren:

1. Wenn Sie mit StoreFront XenDesktop- und XenApp-Ressourcen für Benutzer bereitstellen möchten, muss der StoreFront-Server Mitglied der Microsoft Active Directory-Domäne sein, in der Konten der Benutzer sind, oder in einer Domäne, die eine Vertrauensstellung mit der Domäne mit den Benutzerkonten hat.

   Wichtig:
   - Für Einzelserverbereitstellungen können Sie StoreFront auf einem Server installieren, der nicht in einer Domäne ist.
   - StoreFront kann nicht auf einem Domänencontroller installiert werden.

2. StoreFront erfordert Microsoft .NET Framework, das Sie ggf. von Microsoft herunterladen können. Microsoft .NET muss installiert sein, bevor StoreFront installiert werden kann.
3. Wenn Sie eine Multiserverbereitstellung konfigurieren möchten, können Sie optional auch eine Lastausgleichsumgebung für Ihre StoreFront-Server einrichten.

   Um NetScaler zum Lastausgleich zu verwenden, müssen Sie einen virtuellen Server als Proxyserver für die StoreFront-Server definieren. Weitere Informationen zum Konfigurieren von NetScaler für den Lastausgleich finden Sie unter Lastausgleich mit NetScaler.

   1. Stellen Sie sicher, dass der Lastausgleich auf dem NetScaler-Gerät aktiviert ist.
   2. Erstellen Sie für jeden StoreFront-Server nach Bedarf individuelle HTTP- oder TLS-Lastausgleichsdienste. Verwenden Sie dazu den Monitortyp "StoreFront".
   3. Konfigurieren Sie den Dienst so, dass die Client-IP-Adresse in den X-Forwarded-For HTTP-Header von an StoreFront weitergeleitete Anfragen eingefügt wird und alle globalen Richtlinien außer Kraft gesetzt werden.

      Für StoreFront müssen die IP-Adressen von Benutzern mit ihren Ressourcen verbunden sein.
   4. Erstellen Sie einen virtuellen Server und binden Sie die Dienste an den virtuellen Server.
   5. Konfigurieren Sie auf dem virtuellen Server Persistenz unter Verwendung der Cookie-Insert-Methode, sofern auf allen Plattformen die aktuellen Citrix Receiver-Versionen installiert sind und keine Unterstützung für Android erforderlich ist. Andernfalls konfigurieren Sie Persistenz auf der Basis der Quell-IP-Adresse.Stellen Sie sicher, dass die Gültigkeitsdauer (TTL) ausreicht, damit Benutzer so lange wie nötig beim Server angemeldet bleiben.

      Durch Persistenz wird sichergestellt, dass nur für die anfängliche Benutzerverbindung ein Lastausgleich stattfindet und nachfolgende Anfragen dieses Benutzers an denselben StoreFront-Server weitergeleitet werden.

4. Die folgenden Features können nach Wunsch aktiviert werden.

   - .NET Framework-Features > .NET Framework, ASP.NET

   Nach Wunsch können Sie die folgenden Rollen und ihre Abhängigkeiten auf dem StoreFront-Server aktivieren.

   - Webserver (IIS) > Webserver > Allgemeine HTTP-Features > Standarddokument, HTTP-Fehler, Statischer Inhalt, HTTP-

Umleitung
- Webserver (IIS) > Webserver > Integrität und Diagnose > HTTP-Protokollierung
- Webserver (IIS) > Webserver > Sicherheit > Anforderungsfilterung, Windows-Authentifizierung
  Das Installationsprogramm für StoreFront prüft, ob alle oben aufgeführten Features und Serverrollen aktiviert sind.

5. Installieren Sie StoreFront.

   Soll der Server Teil einer Servergruppe werden, müssen StoreFront-Installationsort und IIS-Websiteeinstellungen, physischer Pfad und Site-IDs in der Gruppe überall identisch sein.
6. Wenn Sie die Kommunikation zwischen StoreFront und Benutzergeräten mit HTTPS sichern möchten, müssen Sie Microsoft-Internetinformationsdienste (IIS) für HTTPS konfigurieren.

   HTTPS ist für die Smartcardauthentifizierung erforderlich. Standardmäßig erfordert Citrix Receiver HTTPS-Verbindungen zu Stores. Sie können jederzeit nach der Installation von StoreFront von HTTP zu HTTPS wechseln, vorausgesetzt, die entsprechende IIS-Konfiguration ist vorhanden.

   Zum Konfigurieren von IIS für HTTPS erstellen Sie mit der IIS-Verwaltungskonsole auf dem StoreFront-Server ein Serverzertifikat, das von Ihrer Domänenzertifizierungsstelle signiert wurde. Fügen Sie anschließend eine HTTPS-Bindung zur Standardwebsite hinzu. Weitere Informationen zum Erstellen eines Serverzertifikats in IIS finden Sie unter http://technet.microsoft.com/de-de/library/hh831637.aspx#CreateCertificate. Weitere Informationen über das Hinzufügen einer HTTPS-Bindung zu einer IIS-Website finden Sie unter http://technet.microsoft.com/de-de/library/hh831632.aspx#SSLBinding.

7. Stellen Sie sicher, dass Firewalls und andere Netzwerkgeräte Zugriff auf den TCP-Port 80 oder 443 von innerhalb und außerhalb des Unternehmensnetzwerks gestatten. Stellen Sie außerdem sicher, dass Firewalls oder andere Geräte im internen Netzwerk keinen Datenverkehr an nicht zugewiesene TCP-Ports blockieren.

   Wenn Sie StoreFront installieren, wird eine Windows-Firewallregel konfiguriert, die den Zugriff auf die ausführbare StoreFront-Datei über einen zufällig unter allen nicht reservierten Ports ausgewählten TCP-Port ermöglicht. Dieser Port wird für die Kommunikation zwischen den StoreFront-Servern in einer Servergruppe verwendet.

8. Wenn Sie mehrere Internetinformationsdienste- (IIS)-Websites verwenden möchten, erstellen Sie mehrere Websites in IIS und erstellen Sie danach mit dem PowerShell SDK eine StoreFront-Bereitstellung in jeder dieser IIS-Websites. Weitere Informationen finden Sie unter Mehrere Internetinformationsdienste- (IIS)-Websites.
   Hinweis: StoreFront deaktiviert die Verwaltungskonsole, wenn mehrere Sites erkannt werden, und zeigt eine entsprechende Meldung an.

9. Konfigurieren Sie den Server mit der Citrix StoreFront-Verwaltungskonsole.

Installieren von StoreFront

> **Important**
>
> Um potenzielle Fehler und Datenverlust beim Installieren von StoreFront zu vermeiden, müssen Sie sicherstellen, dass alle Anwendungen geschlossen sind und keine anderen Aufgaben oder Vorgänge auf dem Zielsystem ausgeführt werden.

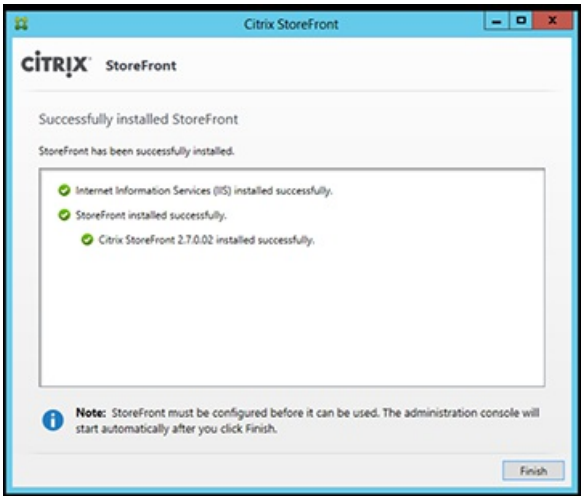
1. Laden Sie das Installationsprogramm von der Downloadseite herunter.
2. Melden Sie sich mit einem Konto mit lokalen Administratorberechtigungen bei StoreFront an.

3. Stellen Sie sicher, dass das erforderliche Microsoft .NET Framework auf dem Server installiert ist.
4. Navigieren Sie zum Downloadpaket, suchen Sie die Datei CitrixStoreFront-x64.exe und führen Sie die Datei als Administrator aus.
5. Lesen und akzeptieren Sie die Lizenzvereinbarung und klicken Sie auf Weiter.
6. Wenn die Seite Voraussetzungen prüfen angezeigt wird, klicken Sie auf Weiter.
7. Prüfen Sie auf der Seite Bereit zur Installation die Voraussetzungen und StoreFront-Komponenten für die Installation und klicken Sie auf Installieren.
   Vor der Installation der Komponenten werden die folgenden Rollen aktiviert, sofern sie nicht bereits auf dem Server konfiguriert sind.

   - Webserver (IIS) > Webserver > Allgemeine HTTP-Features > Standarddokument, HTTP-Fehler, Statischer Inhalt, HTTP-Umleitung
   - Webserver (IIS) > Webserver > Integrität und Diagnose > HTTP-Protokollierung
   - Webserver (IIS) > Webserver > Sicherheit > Anforderungsfilterung, Windows-Authentifizierung
   - Webserver (IIS) > Verwaltungstools > IIS-Verwaltungskonsole, IIS-Verwaltungsskripts und -tools

   Die folgenden Features werden ebenfalls aktiviert, sofern sie nicht bereits konfiguriert sind.

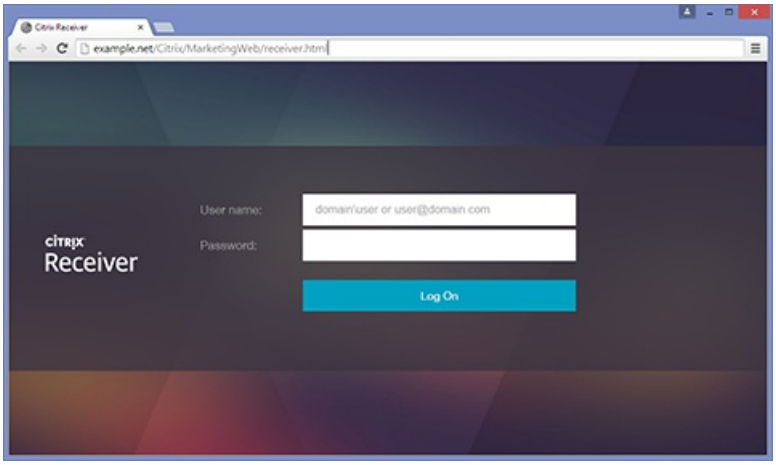
   - .NET Framework-Features > .NET Framework, ASP.NET
8. Wenn die Installation abgeschlossen ist, klicken Sie auf Fertig stellen. Die Citrix StoreFront-Verwaltungskonsole wird automatisch gestartet. Sie können StoreFront auch über die Startseite öffnen.



9. Klicken Sie in der Citrix StoreFront-Verwaltungskonsole auf Neue Bereitstellung erstellen.
   1. Geben Sie die URL des StoreFront-Servers in das Feld **Basis-URL** ein.
   2. Geben Sie auf der Seite **Storename** einen Namen für den Store an und klicken Sie auf Weiter.
10. Geben Sie auf der Seite **Delivery Controller** die Infrastruktur (XenApp- bzw. XenDesktop-Dienste) an, über die die Ressourcen bereitgestellt werden, die Sie im Store zur Verfügung stellen möchten. Sie können hier einen Dummy-Server eingeben, dann werden jedoch keine Apps im Store angezeigt.
11. Legen Sie die Parameter Transporttyp **und** Port **fest.**Sie können HTTP und 443 festlegen; klicken Sie dann auf **OK**. Kopieren Sie alternativ die Einstellungen einer vorhandenen Webinterface- oder StoreFront Bereitstellung.
12. Wählen Sie auf der Seite **Remotezugriff** die Option Keine aus. Wenn Sie NetScaler Gateway verwenden, wählen Sie Kein VPN-Tunnel aus und geben Sie die Gateway-Details ein.
13. Wählen Sie auf der Seite **Remotezugriff** die Option Erstellen aus. Nach dem Erstellen des Stores klicken Sie auf Fertig stellen.

Der Store steht Benutzern nun über Citrix Receiver fürWeb-Site zur Verfügung, d. h. sie können über eine Webseite auf ihre

Desktops und Apps zugreifen.
Die URL, über die Benutzer auf die Receiver für Web-Site für den neuen Store zugreifen, wird angezeigt. Beispiel: example.net/Citrix/MarketingWeb/. Wenn Sie sich anmelden, greifen Sie auf die neue Benutzeroberfläche in Citrix Receiver zu.



CEIP

Wenn Sie am Programm zur Verbesserung der Benutzerfreundlichkeit (Customer Experience Improvement Program, CEIP) teilnehmen, werden anonyme Statistiken und Nutzungsinformationen an Citrix gesendet, damit die Qualität und Leistung der Citrix Produkte verbessert wird.

Sie werden standardmäßig automatisch beim CEIP registriert, wenn Sie StoreFront installieren. Der erste Datenupload erfolgt ca. sieben Tage nach der Installation von StoreFront. Sie können die Standardeinstellung über eine Registrierungseinstellung ändern. Wenn Sie die Registrierungseinstellung ändern, bevor Sie StoreFront installieren, wird der neue Wert verwendet. Wenn Sie die Registrierungseinstellung ändern, bevor Sie StoreFront aktualisieren, wird der neue Wert verwendet.

> ## Warnung
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall eine Sicherungskopie der Registrierung, bevor Sie sie bearbeiten.

Registrierungseinstellung zur Steuerung des automatischen Uploads von Analysedaten (Standard = 1):

Ort: HKLM:\Software\Citrix\Telemetry\CEIP

Name: Enabled

Typ: REG_DWORD

Wert: 0 = deaktiviert , 1 = aktiviert

Standardmäßig ist die Eigenschaft "Enabled" in der Registrierung verborgen. Wird sie nicht festgelegt, dann ist der automatische Upload aktiviert.

Mit dem folgenden PowerShell-Cmdlet wird die Registrierung beim CEIP deaktiviert:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\Telemetry\CEIP -Name Enabled -PropertyType DWORD -Value 0
```

Hinweis: Die Registrierungseinstellung steuert den automatischen Upload anonymer Statistiken und Nutzungsinformationen für alle Komponenten auf einem Server. Wenn Sie StoreFront beispielsweise auf demselben Server wie den Delivery Controller installiert haben und die Teilnahme am CEIP per Registrierungseinstellung beenden, gilt dies für beide Komponenten.

Vom CEIP gesammelte StoreFront-Daten

In der folgende Tabelle sehen Sie Beispiele für die Art der anonymen Informationen, die gesammelt werden. Die Daten enthalten keine Informationen, die Sie als Kunden identifizieren.

Daten	Beschreibung
StoreFront-Version	Die Zeichenfolge steht für die installierte Version von StoreFront. Beispiel: "3.8.0.0"
Anzahl der Stores	Anzahl der Stores in der Bereitstellung
Anzahl der Server in der Servergruppe	Die Anzahl der Server in der Servergruppe
Delivery Controller pro Store	Liste numerischer Werte mit der Anzahl der für jeden Store in der Bereitstellung verfügbaren Delivery Controller
HTTPS aktiviert	Zeichenfolge, die angibt, ob HTTPS für die Bereitstellung aktiviert ist. "True" oder "False".
Klassische Benutzeroberfläche für Citrix Receiver aktiviert	Liste boolescher Werte, die angeben, ob die klassische Benutzeroberfläche für Web Receiver aktiviert ist. TRUE oder FALSE für jeden Web Receiver.
HTML5-Einstellung für Citrix Receiver	Liste von Zeichenfolgen, die die HTML5-Einstellung für Web Receiver angeben. "Always", "Fallback", "Off" für jeden Web Receiver.
Workspace Control für Citrix Receiver aktiviert	Liste boolescher Werte, die angeben, ob Workspace Control für jeden Web Receiver aktiviert ist. TRUE oder FALSE für jeden Web Receiver.
Remotezugriff für den Store aktiviert	Liste von Zeichenfolgen, die angeben, ob Remotezugriff für die Stores in der Bereitstellung aktiviert ist. ENABLED oder DISABLED für jeden Store.
Gateways	Anzahl der in der Bereitstellung konfigurierten NetScaler Gateways.

Installieren von StoreFront über eine Eingabeaufforderung

1. Melden Sie sich mit einem Konto mit lokalen Administratorberechtigungen bei StoreFront an.
2. Stellen Sie sicher, dass alle Installationsanforderungen vor der Installation von StoreFront erfüllt sind. Weitere Informationen finden Sie unter Vorbereiten der Installation.
3. Navigieren Sie zum Installationsmedium oder Downloadpaket, suchen Sie die Datei CitrixStoreFront-x64.exe und kopieren Sie die Datei zu einem temporären Speicherort auf dem Server.
4. Navigieren Sie in der Befehlszeile zu dem Ordner mit der Installationsdatei und geben Sie den folgenden Befehl ein.
   CitrixStoreFront-x64.exe [-silent] [-INSTALLDIR installationlocation]
   [-WINDOWS_CLIENT filelocation\filename.exe]
   [-MAC_CLIENT filelocation\filename.dmg]
   Verwenden Sie das Argument -silent, um StoreFront und alle erforderlichen Komponenten ohne Benutzereingriff zu installieren. Standardmäßig wird StoreFront unter C:\Program Files\Citrix\Receiver StoreFront\ installiert. Sie können einen anderen Speicherort für die Installation mit dem Argument -INSTALLDIR und installationlocation als Verzeichnis, in dem StoreFront installiert wird, angeben. Soll der Server Teil einer Servergruppe werden, müssen StoreFront-Installationsort und IIS-Websiteeinstellungen, physischer Pfad und Site-IDs in der Gruppe überall identisch sein.

   Wenn eine Citrix Receiver für Web-Site Citrix Receiver auf einem Windows- oder Mac OS X-Gerät nicht erkennt, wird der Benutzer standardmäßig aufgefordert, die für seine Plattform geeignete Citrix Receiver-Version von der Citrix Website herunterzuladen und zu installieren. Sie können dieses Verhalten insofern ändern, dass Benutzer die Citrix Receiver-Installationsdateien von dem StoreFront-Server herunterladen. Weitere Informationen finden Sie unter Verfügbarmachen von Citrix Receiver-Installationsdateien auf dem Server.

   Wenn Sie eine solche Konfigurationsänderung beabsichtigen, geben Sie die Argumente -WINDOWS_CLIENT und -MAC_CLIENT an, um die Installationsdateien für Citrix Receiver für Windows und Citrix Receiver für Mac an den entsprechenden Speicherort in der StoreFront-Bereitstellung zu kopieren. Ersetzen Sie filelocation durch das Verzeichnis, das die zu kopierende Installationsdatei enthält, und filename durch den Namen der Citrix Receiver-Installationsdatei. Installationsdateien für Citrix Receiver für Windows und Citrix Receiver für Mac befinden sich auf dem StoreFront-Installationsmedium bzw. im Downloadpaket.

Aktualisieren von StoreFront

Für das Upgrade vorhandener 3.x-Bereitstellungen auf diese Version von StoreFront führen Sie die Installationsdatei für diese StoreFront-Version aus.

Der Upgradeprozess kann nach dem Start nicht mehr rückgängig gemacht werden. Wenn das Upgrade unterbrochen wird oder nicht abgeschlossen werden kann, wird die vorhandene Konfiguration entfernt, StoreFront jedoch nicht installiert. Bevor Sie mit dem Upgrade beginnen, müssen Sie alle Benutzerverbindungen mit der StoreFront-Bereitstellung trennen und verhindern, dass neue Benutzer sich an den Servern anmelden, während das Upgrade durchgeführt wird. So wird sichergestellt, dass das Installationsprogramm während des Upgrades auf alle StoreFront-Dateien zugreifen kann. Kann das Installationsprogramm auf eine Datei nicht zugreifen, dann kann sie nicht ersetzt werden und das Upgrade schlägt fehl, wodurch die vorhandene StoreFront-Konfiguration entfernt wird. StoreFront unterstützt keine Multiserverbereitstellung mit mehreren Produktversionen. Daher müssen alle Server einer Gruppe aktualisiert werden, bevor Zugriff auf die Bereitstellung erteilt wird. Ein Upgrade aller Server in Bereitstellungen mit mehreren Servern in einem Arbeitsgang wird nicht unterstützt. Die Server müssen nacheinander aktualisiert werden. Citrix empfiehlt, dass Sie vor dem Upgrade eine Sicherungskopie des Datenspeichers anlegen.

Bei der Deinstallation von StoreFront werden Authentifizierungsdienst, Stores, die Anwendungsabonnements der Benutzer,

Citrix Receiver für Web-Sites, Desktopgerätesites und XenApp Services-URLs entfernt. Wenn Sie also StoreFront deinstallieren, müssen Sie den Dienst, die Stores und Sites manuell neu erstellen, wenn Sie StoreFront neu installieren. Durch ein Upgrade können Sie die StoreFront-Konfiguration beibehalten. Darüber hinaus bleiben die Anwendungsabonnementdaten erhalten, sodass Benutzer nicht alle ihre Anwendungen neu abonnieren müssen.

Das Aktualisieren des Betriebssystems eines Servers, auf dem StoreFront ausgeführt wird, wird nicht unterstützt. Citrix empfiehlt die Installation von StoreFront auf einer neuen Installation des Betriebssystems.

Important

Führen Sie vor dem Upgrade folgende Schritte durch:

- Schließen Sie alle anderen Anwendungen auf dem StoreFront-Server.
- Schließen Sie alle Befehlszeilen- und PowerShell-Fenster.

Aktualisieren vorhandener 3.x-Bereitstellungen auf diese Version von StoreFront

1. Deaktivieren Sie den Zugriff auf die Bereitstellung über die Lastausgleichsumgebung. Durch Deaktivieren der Lastausgleichs-URL wird verhindert, dass Benutzer während des Upgrades eine Verbindung mit der Bereitstellung herstellen.
2. Erstellen Sie ein Backup aller Server in der Servergruppe.
3. Entfernen Sie einen der Server aus der Servergruppe.
4. Starten Sie dann diesen Server neu.
   Sie können einen parallelen Load Balancer zum Überprüfen der neuen Servergruppe während deren Erstellung verwenden. Die Variante zur Maximierung der Verfügbarkeit und Minimierung von Risiken wäre das Entfernen und Aktualisieren eines einzigen Servers aus der ursprünglichen Servergruppe. Sie können dann die neue Gruppe auf der Basis neuer Maschinen erstellen, statt Maschinen aus der ursprünglichen Servergruppe zu verwenden.
5. Verwenden Sie zum Durchführen des Serverupgrades ein Administratorkonto, das keine anderen Installationen ausführt und möglichst wenige andere Anwendungen geöffnet hat.
6. Vergewissern Sie sich, dass das Upgrade des entfernten Servers erfolgreich war.
7. Entfernen Sie einen weiteren Server aus der vorhandenen Servergruppe des Load Balancers.
8. Starten Sie diesen Server neu (aus den in Schritt 1 erwähnten Gründen).
9. Deinstallieren Sie StoreFront und installieren Sie die neue StoreFront-Version.
10. Fügen Sie den Server mit der neu installierten Version einer neuen Servergruppe hinzu, die sämtliche aktualisierten Server und Server mit neuer Installation enthält, und vergewissern Sie sich, dass diese einwandfrei funktionieren.
11. Wiederholen Sie die Schritte 3–10 bis die neue Servergruppe ausreichend Kapazität hat, um die Aufgabe der alten Servergruppe zu übernehmen, verweisen Sie den Load Balancer auf die neue Servergruppe und vergewissern Sie sich, dass sie einwandfrei funktioniert.
12. Wiederholen Sie die Schritte 3–10 mit allen verbleibenden Servern und fügen Sie diese jeweils nach dem Upgrade einzeln dem Load Balancer hinzu.

Hinweis

- Wenn Sie die Verfügbarkeit maximieren möchten, können Sie den Zugriff auf die ursprüngliche Servergruppe während des Upgrades aufrechterhalten, bis die neue Servergruppe zur Verfügung steht. Gehen Sie hierzu folgendermaßen vor:
  1. Überspringen Sie Schritt 1.

2. Deaktivieren Sie in Schritt 11 zusätzlich den Zugriff auf die ursprüngliche Servergruppe über den Load Balancer. Exportieren Sie die Abonnementdaten aus der ursprünglichen Servergruppe und importieren Sie sie in die neue. Aktivieren Sie den Zugriff auf die neue Servergruppe über den Load Balancer.

   Damit wird gewährleistet, dass alle Abonnementänderungen, die Benutzer nach Schritt 3 und vor Schritt 11 gemacht haben, in der neuen Servergruppe verfügbar sind.

- Zur weiteren Maximierung der Verfügbarkeit können Sie nur einen Server aus der ursprünglichen Servergruppe entfernen, das Upgrade für diesen durchführen und dann die neue Servergruppe unter Verwendung neuer Server anstelle von Servern aus der ursprünglichen Servergruppe erstellen. Wenn die neue Servergruppe in Betrieb ist, können Sie die alten Server außer Betrieb nehmen.
- Speichern Sie Backups der Datei "web.config" an einem **anderen** Speicherort als dem IIS-Standardverzeichnis des Stores. Speichern Sie beispielweise keine Backups in C:\inetpub\wwwroot\citrix\. Das Speichern von Backups an demselben Speicherort wie das IIS-Standardverzeichnis des Stores kann das Upgrade von StoreFront beeinträchtigen.

Konfigurieren von StoreFront

Beim ersten Start der Citrix StoreFront-Verwaltungskonsole sind drei Optionen verfügbar.

- Neue Bereitstellung erstellen:Konfigurieren Sie den ersten StoreFront-Server in einer neuen StoreFront-Bereitstellung. Bereitstellungen mit einem Server sind ideal für die Evaluierung von StoreFront oder für kleine Produktionsbereitstellungen. Nachdem Sie den ersten StoreFront-Server konfiguriert haben, können Sie jederzeit weitere Server zur Gruppe hinzufügen, um die Kapazität der Bereitstellung zu erhöhen.
- Vorhandener Servergruppe beitreten:Fügen Sie einer vorhandenen StoreFront-Bereitstellung einen Server hinzu. Wählen Sie diese Option aus, um die Kapazität der StoreFront-Bereitstellung schnell zu erhöhen. Für Bereitstellungen mit mehreren Servern ist ein externer Lastausgleich erforderlich. Sie müssen auf einen vorhandenen Server in der Bereitstellung zugreifen, um einen neuen Server hinzuzufügen.

Deinstallieren von StoreFront

Neben dem Produkt selbst werden bei der Deinstallation von StoreFront der Authentifizierungsdienst, die Stores, Citrix Receiver für Web-Sites, Desktopgerätesites sowie XenApp Services-URLs und die zugeordneten Konfigurationen entfernt. Der Abonnementstoredienst, der die Anwendungsabonnementdaten der Benutzer enthält, wird ebenfalls gelöscht. Bei Einzelserverbereitstellungen bedeutet dies, dass die Details zu den Anwendungsabonnements der Benutzer verloren gehen. Bei Multiserverbereitstellungen werden diese Daten jedoch auf den anderen Servern der Gruppe beibehalten. ErforderlicheKomponenten, die vom StoreFront-Installationsprogramm aktiviert werden, z. B. .NET Framework-Features und die Webserver (IIS)-Rollendienste, werden nicht vom Server entfernt, wenn StoreFront deinstalliert wird.

1. Melden Sie sich mit einem Konto mit lokalen Administratorberechtigungen bei StoreFront an.
2. Navigieren Sie auf derWindows-Startseite oder auf der Apps-Seite zur Kachel **Citrix StoreFront**. Klicken Sie mit der rechten Maustaste auf die Kachel und klicken Sie auf **Deinstallieren**.
3. Wählen Sie im Dialogfeld **Programme und FunktionenCitrix StoreFront** aus und klicken Sie auf **Deinstallieren**, um alle StoreFront-Komponenten vom Server zu entfernen.
4. Klicken Sie im Dialogfeld **Citrix StoreFront deinstallieren** auf **Ja**. Wenn die Deinstallation abgeschlossen ist, klicken Sie auf **OK**.

Erstellen einer neuen Bereitstellung

Jun 04, 2018

1. Wenn die Citrix StoreFront-Verwaltungskonsole nach der Installation von StoreFront nicht bereits geöffnet ist, klicken Sie auf der Windows-Startseite oder auf der Apps-Seite auf die Kachel Citrix StoreFront.
2. Klicken Sie im Ergebnisbereich der Citrix StoreFront-Verwaltungskonsole auf Neue Bereitstellung erstellen.
3. Geben Sie die URL des StoreFront-Servers oder der Lastausgleichsumgebung bei einer Multiserverbereitstellung in das Feld Basis-URL ein.
   Wenn Sie noch keine Lastausgleichsumgebung eingerichtet haben, geben Sie die Server-URL an. Sie können die URL für Ihre Bereitstellung später jederzeit ändern.

   Mit der Aufgabe Basis-URL ändern können Sie jederzeit von HTTP zu HTTPS wechseln, vorausgesetzt, dass Microsoft Internetinformationsdienste (IIS) für HTTPS konfiguriert ist.

4. Klicken Sie auf Weiter, um den Authentifizierungsdienst einzurichten, über den Benutzer bei Microsoft Active Directory authentifiziert werden.
   Wenn Sie die Kommunikation zwischen StoreFront und Benutzergeräten mit HTTPS sichern möchten, müssen Sie Microsoft Internetinformationsdienste (IIS) für HTTPS konfigurieren. Wenn die entsprechende IIS-Konfiguration nicht verfügbar ist, verwendet StoreFront HTTP für die Kommunikation.

   Standardmäßig erfordert Citrix Receiver HTTPS-Verbindungen zu Stores. Wenn StoreFront nicht für HTTPS konfiguriert ist, müssen Benutzer zusätzliche Konfigurationsschritte ausführen, um HTTP-Verbindungen zu verwenden. HTTPS ist für die Smartcardauthentifizierung erforderlich. Sie können jederzeit nach dem Konfigurieren von StoreFront von HTTP zu HTTPS wechseln, vorausgesetzt, die entsprechende IIS-Konfiguration ist vorhanden. Weitere Informationen finden Sie unter Konfigurieren von Servergruppen.

   Mit der Aufgabe **Basis-URL ändern** können Sie jederzeit von HTTP zu HTTPS wechseln, vorausgesetzt, dass Microsoft Internetinformationsdienste (IIS) für HTTPS konfiguriert ist.

5. Geben Sie auf der Seite Storename einen Namen für den Store ein, geben Sie an, ob nicht authentifizierte (anonyme) Benutzer auf den Store Zugriff erhalten sollen, und klicken Sie auf Weiter.
   In StoreFront-Stores werden Desktops und Anwendungen aggregiert und so den Benutzern zur Verfügung gestellt. Storenamen erscheinen in Citrix Receiver unter den Konten der Benutzer. Wählen Sie daher einen Namen, anhand dessen Benutzer den Inhalt des Stores erkennen können.

6. Listen Sie auf der Seite Controller die Infrastruktur und die Ressourcen auf, die Sie im Store zur Verfügung stellen möchten. Zum Hinzufügen von Desktops und Anwendungen zu dem Store befolgen Sie das entsprechende Verfahren unten. Sie können Stores konfigurieren, die Ressourcen aus einer beliebigen Zusammenstellung von XenDesktop und XenApp-Bereitstellungen bieten. Wiederholen Sie die Verfahren bei Bedarf, um alle Bereitstellungen, von Ressourcen für den Store hinzuzufügen.
   - Hinzufügen von XenDesktop- und XenApp-Ressourcen zum Store
7. Wenn Sie dem Store alle erforderlichen Ressourcen hinzugefügt haben, klicken Sie auf der Seite Controller auf Weiter.
8. Geben Sie auf der Seite Remotezugriff an, ob und wie Benutzer, die eine Verbindung aus einem öffentlichen Netzwerk herstellen, auf die internen Ressourcen zugreifen können:
   - Soll der Store Benutzern in öffentlichen Netzwerken zur Verfügung stehen, stellen Sie sicher, dass die Option **Remotezugriff aktivieren** aktiviert ist. Wenn Sie dieses Kontrollkästchen nicht aktivieren, können nur lokale Benutzer im internen Netzwerk auf den Store zugreifen.

- Wenn Sie nur Ressourcen, die über den Store angeboten werden, über NetScaler Gateway verfügbar machen möchten, wählen Sie **Benutzern nur Zugriff auf Ressourcen geben, die über StoreFront bereitgestellt werden (kein _VPN-Tunnel)** aus.
- Um den Store und alle anderen Ressourcen im internen Netzwerk über einen SSL-VPN-Tunnel verfügbar zu machen, wählen Sie **Benutzern Zugriff auf alle Ressourcen im internen Netzwerk geben (vollständiger VPN-Tunnel)**. Benutzer benötigen möglicherweise das NetScaler Gateway-Plug-In für das Erstellen des VPN-Tunnels.

Wenn Sie Remotezugriff auf den Store über NetScaler Gateway konfigurieren, wird die Passthrough-Authentifizierung von NetScaler Gateway automatisch aktiviert. Benutzer authentifizieren sich bei NetScaler Gateway und werden beim Zugriff auf ihre Stores automatisch angemeldet.

9. Listen Sie die NetScaler Gateway-Bereitstellungen auf, durch die Benutzer auf den Store zugreifen können, wenn Sie Remotezugriff aktiviert haben. Zum Hinzufügen einer NetScaler Gateway-Bereitstellung folgen Sie dem entsprechenden Verfahren unten. Wiederholen Sie die Schritte bei Bedarf, um weitere Bereitstellungen hinzuzufügen.
   - Konfigurieren des Remotezugriffs auf den Store über ein NetScaler Gateway-Gerät
10. Wenn alle NetScaler Gateway-Bereitstellungen hinzugefügt sind, wählen Sie in der Liste NetScaler Gateway-Geräte die Bereitstellungen aus, über die Benutzer auf den Store zugreifen können. Wenn Sie Zugriff über mehrere Bereitstellungen aktivieren, geben Sie die Standardbereitstellung für den Zugriff auf den Store an.Klicken Sie auf **Weiter**.
11. Wählen Sie auf der Seite **Authentifizierungsmethoden** die Methoden zur Authentifizierung der Benutzer bei dem Store aus und klicken Sie auf **Weiter**. Wählen Sie eine der folgenden Methoden:

- **Benutzername und Kennwort:** Die Benutzer geben zur Authentifizierung bei ihren Stores ihre Anmeldeinformationen ein.
- **SAML-Authentifizierung:** Benutzer authentifizieren sich bei NetScaler Gateway und werden beim Zugriff auf ihre Stores automatisch angemeldet.
- **Domänen-Passthrough-Authentifizierung:** Benutzer authentifizieren sich bei ihrem domänengebundenen Computer und ihre Anmeldeinformationen werden für eine automatische Anmeldung beim Zugriff auf ihre Stores verwendet.
- **Smartcard:** Benutzer authentifizieren sich mit Smartcards und PINs beim Zugriff auf ihre Stores.
- **HTTB Basic:** Benutzer authentifizieren sich über den IIS-Webserver des StoreFront-Servers.
- **Passthrough-Authentifizierung von NetScaler Gateway:** Benutzer authentifizieren sich bei NetScaler Gateway und werden beim Zugriff auf ihre Stores automatisch angemeldet. Diese Option wird automatisch aktiviert, wenn Remotezugriff aktiviert wird.

12. Konfigurieren Sie auf der Seite **XenApp Services-URL** die XenApp- Services-URL für Benutzer, die PNAgent für den Zugriff auf Anwendungen und Desktops verwenden.

13. Nach dem Erstellen des Stores sind weitere Optionen in der Citrix StoreFront-Verwaltungskonsole verfügbar. Weitere Informationen finden Sie in diversen Artikeln zur Verwaltung.

Der Store steht jetzt für den Zugriff durch Benutzer über Citrix Receiver zur Verfügung. Citrix Receiver muss mit den Zugriffsinformationen für den Store konfiguriert werden. Es gibt eine Reihe von Methoden der Bekanntgabe dieser Informationen an die Benutzer, sodass Sie diesen die Konfiguration erleichtern können. Weitere Informationen finden Sie unter Benutzerzugriffsoptionen.

Alternativ können Benutzer auf den Store über Citrix Receiver für Web-Site zugreifen und somit über eine Webseite auf ihre Desktops und Anwendungen zugreifen. Die URL, über die Benutzer auf die Citrix Receiver für Web-Site für den Store zugreifen, wird angezeigt, wenn Sie den Store erstellen.

Wenn Sie einen neuen Store erstellen, wird die XenApp Services-URL standardmäßig aktiviert. Benutzer domänengebundener Desktopgeräte und umfunktionierter PCs, auf denen Citrix Desktop Lock ausgeführt wird, sowie

Benutzer mit älteren Citrix Clients, die nicht aktualisiert werden können, können über die XenApp-Services-URL direkt auf Stores zugreifen. Die XenApp Services-URL hat das Format http[s]://serveradresse/Citrix/storename/PNAgent/config.xml, wobei serveradresse der vollqualifizierte Domänenname des Servers oder der Lastausgleichsumgebung für die StoreFront-Bereitstellung ist und storename der Name, den Sie in Schritt 5 angegeben haben.

Sie können sekundäre Server hinzufügen, indem Sie die Option zum Beitreten bei einer vorhandenen Servergruppe auswählen, wenn Sie weitere Instanzen von StoreFront installieren.

Hinzufügen von XenDesktop- und XenApp-Ressourcen zum Store

Führen Sie die folgenden Schritte aus, um von XenDesktop und XenApp bereitgestellte Desktops und Anwendungen in dem Store verfügbar zu machen, den Sie als Teil der Erstkonfiguration des StoreFront-Servers erstellen. Es wird davon ausgegangen, dass Sie die unter "Neue Bereitstellung erstellen" weiter oben beschriebenen Schritte 1 bis 6 ausgeführt haben.

1. Klicken Sie auf der Seite Controller der Seite der StoreFront-Verwaltungskonsole zum Erstellen von Stores auf Hinzufügen.
2. Geben Sie im Dialogfeld Controller hinzufügen einen Namen an, über den Sie die Bereitstellung identifizieren können, und geben Sie an, ob die Ressourcen, die Sie über den Store verfügbar machen möchten, von XenDesktop, XenApp oder XenMobile bereitgestellt werden.
3. Fügen Sie der Liste Server die Namen oder IP-Adressen der Server hinzu. Geben Sie aus Gründen der Fehlertoleranz mehrere Server an und führen Sie die Server dabei in der Reihenfolge ihrer Priorität auf, um die Failover-Reihenfolge festzulegen. Geben Sie für XenDesktop-Sites die Details der Controller an. Listen Sie für XenApp-Farmen Server auf, auf denen der Citrix XML-Dienst ausgeführt wird.
4. Wählen Sie aus der Liste Transporttyp die Verbindungstypen für StoreFront aus, die für die Kommunikation mit den Servern verwendet werden sollen.
   - Wählen Sie HTTP aus, wenn Daten über unverschlüsselte Verbindungen gesendet werden sollen. Bei Auswahl dieser Option müssen Sie eigene Maßnahmen treffen, um die Verbindungen zwischen StoreFront und den Servern zu sichern.
   - Wählen Sie HTTPS aus, um Daten über sichere HTTP-Verbindungen mit SSL (Secure Sockets Layer) oder TLS (Transport Layer Security) zu senden. Wenn Sie diese Option für XenDesktop- oder XenApp-Server auswählen, vergewissern Sie sich, dass der Citrix XML-Dienst so konfiguriert ist, dass der Port gemeinsam mit Internetinformationsdienste (IIS) verwendet wird und in der IIS-Konfiguration HTTPS-Unterstützung festgelegt wurde.
   - Wählen Sie SSL-Relay aus, um Daten über sichere Verbindungen an XenApp-Server zu senden. SSL-Relay übernimmt die Hostauthentifizierung und Datenverschlüsselung.

   Hinweis: Wenn Sie die Verbindungen zwischen StoreFront und den Servern mit HTTPS oder SSL-Relay sichern, achten Sie darauf, dass die in der Liste Server eingegebenen Servernamen genau mit den Namen in den Zertifikaten für die Server übereinstimmen. Dies gilt auch für die Groß- und Kleinschreibung.
5. Geben Sie den Port an, den StoreFront für Verbindungen mit den Servern verwenden soll. Der Standardport ist 80 für Verbindungen über HTTP und SSL-Relay bzw. 443 für HTTPS-Verbindungen. Bei XenDesktop- und XenApp-Servern muss der angegebene Port dem vom Citrix XML-Dienst verwendeten Port entsprechen.
6. Wenn Sie SSL-Relay verwenden, um Verbindungen zwischen StoreFront und XenApp-Servern zu sichern, geben Sie den TCP-Port für SSL-Relay im Feld SSL-Relay-Port an. Der Standardport ist 443. Stellen Sie sicher, dass alle Server, auf denen SSL-Relay ausgeführt wird, denselben Port überwachen.

Sie können Stores konfigurieren, die Ressourcen aus einer beliebigen Zusammenstellung von XenDesktop-, XenApp- und XenMobile-Bereitstellungen bieten. Zum Hinzufügen weiterer XenDesktop-Sites oder XenApp-Farmen wiederholen Sie das o. g. Verfahren.Wenn Sie dem Store alle erforderlichen Ressourcen hinzugefügt haben, kehren Sie zu Schritt 7 unter "Neue

Bereitstellung erstellen" zurück.

Konfigurieren des Remotezugriffs auf den Store über ein NetScaler Gateway-Gerät

Führen Sie die folgenden Schritte aus, um Remotezugriff über ein NetScaler Gateway-Gerät auf den Store zu konfigurieren, den Sie als Teil der Erstkonfiguration des StoreFront-Servers erstellt haben. Es wird davon ausgegangen, dass Sie die unter "Neue Bereitstellung erstellen" weiter oben beschriebenen Schritte 1 bis 9 ausgeführt haben.

1. Klicken Sie auf der Seite Remotezugriff der Seite der StoreFront-Verwaltungskonsole zum Erstellen von Stores auf Hinzufügen.
2. Geben im Dialogfeld NetScaler Gateway-Gerät hinzufügen einen Namen für das Gerät an, über den die Benutzer dieses identifizieren können.
   Benutzern wird der Anzeigename angezeigt, den Sie in Citrix Receiver angegeben haben. Nehmen Sie deshalb relevante Informationen in den Namen auf, damit Benutzer leichter entscheiden können, ob sie das Gerät verwenden möchten. Beispielsweise können Sie den geographischen Standort in die Anzeigenamen der NetScaler Gateway-Bereitstellungen einfügen, damit Benutzer problemlos das beste Gateway für ihren Standort identifizieren können.

3. Geben Sie die URL des virtuellen Servers oder Benutzeranmeldepunkts (für Access Gateway 5.0) für das Gerät an. Geben Sie die Produktversion Ihrer Bereitstellung an.
   Weitere Informationen zum Erstellen eines einzelnen vollqualifizierten Domänennamens (FQDN) für den internen und externen Zugriff auf einen Store finden Sie unter Erstellen eines einzelnen vollqualifizierten Domänennamens (FQDN) für den internen und externen Zugriff auf einen Store.

4. Wenn Sie ein Access Gateway 5.0-Gerät hinzuzufügen, wählen Sie aus der Liste Bereitstellungsmodus die Option Gerät aus. Andernfalls und geben Sie ggf. die Subnetz-IP-Adresse des NetScaler Gateway-Geräts an.
   Die Subnetzadresse ist die IP-Adresse, durch die NetScaler Gateway für die Kommunikation mit Servern im internen Netzwerk das Benutzergerät darstellt. Dies kann es sich auch die zugeordnete IP-Adresse des NetScaler Gateway-Geräts sein. Wenn angegeben, verwendet StoreFront die Subnetz-IP-Adresse, um zu überprüfen, ob eingehende Anfragen von einem vertrauenswürdigen Gerät stammen.

5. Wenn Sie ein Gerät mit NetScaler Gateway hinzufügen, wählen Sie aus der Liste Anmeldetyp die Authentifizierungsmethode aus, die Sie auf dem Gerät für Benutzer von Citrix Receiver konfiguriert haben.
   Die von Ihnen angegebenen Informationen über die Konfiguration des NetScaler Gateway-Geräts wird der Provisioningdatei für den Store hinzugefügt. Dies ermöglicht, dass Citrix Receiver die entsprechende Verbindungsanforderung schickt, wenn das Gerät zum ersten Mal kontaktiert wird.

   - Wenn Benutzer die Domänenanmeldeinformationen für Microsoft Active Directory eingeben müssen, wählen Sie Domäne.
   - WählenSie Sicherheitstoken, wenn Benutzer einen Tokencode von einem Sicherheitstoken eingeben müssen.
   - WählenSie Domäne und Sicherheitstoken aus, wenn Benutzer ihre Domänenanmeldeinformationen und einen Tokencode von einem Sicherheitstoken eingeben müssen.
   - Wählen Sie SMS-Authentifizierung, wenn Benutzer ein in einer Textnachricht gesendetes Einmalkennwort eingeben müssen.
   - Wenn Benutzer eine Smartcard vorlegen und eine PIN eingeben müssen, wählen Sie Smartcard.

   Wenn Sie die Smartcardauthentifizierung mit einer sekundären Authentifizierungsmethode konfigurieren, auf die Benutzer zurückgreifen können, wenn es Probleme mit den Smartcards gibt, wählen Sie die sekundäre Authentifizierungsmethode aus der Liste Smartcard-Fallback.

6. Geben Sie die URL des NetScaler Gateway-Authentifizierungsdiensts in das Feld Rückruf-URL ein. StoreFront fügt

automatisch den Standardteil der URL an. Klicken Sie auf Weiter.
Geben Sie die intern zugängliche URL des Geräts ein. StoreFront kontaktiert den NetScaler Gateway-Authentifizierungsdienst, um zu überprüfen, ob von NetScaler Gateway empfangene Anforderungen auch tatsächlich von diesem Gerät ausgehen.

7. Wenn Sie Ressourcen von XenDesktop oder XenApp im Store verfügbar machen, listen Sie auf der Seite Secure Ticket Authority (STA) URLs für Server auf, auf denen die STA ausgeführt wird. Geben Sie aus Gründen der Fehlertoleranz URLs für mehrere STAs ein und führen Sie die Server dabei in der Reihenfolge ihrer Priorität auf, um die Failoversequenz festzulegen.
   Die STA wird auf XenDesktop- und XenApp-Servern gehostet und gibt Sitzungstickets als Reaktion auf Verbindungsanforderungen aus. Auf diesen Sitzungstickets basiert die Authentifizierung und Autorisierung für den Zugriff auf XenDesktop- und XenApp-Ressourcen.

8. Aktivieren Sie das Kontrollkästchen Sitzungszuverlässigkeit aktivieren, wenn XenDesktop und XenApp getrennte Sitzungen aufrechterhalten sollen, während Citrix Receiver eine automatische Wiederverbindung versucht. Aktivieren Sie das Kontrollkästchen Tickets von zwei Secure Ticket Authoritys anfordern (falls verfügbar), wenn Sie mehrere STAs konfiguriert haben und sicherstellen möchten, dass Sitzungszuverlässigkeit immer gegeben ist.
   Wenn das Kontrollkästchen Tickets von zwei Secure Ticket Authoritys anfordern (falls verfügbar) aktiviert ist, ruft StoreFront Tickets von zwei verschiedenen Secure Ticket Authoritys ab, damit Benutzersitzungen nicht unterbrochen werden, wenn eine Secure Ticket Authority während der Sitzung ausfällt. Wenn StoreFront aus irgendeinem Grund keine Verbindung zu zwei Secure Ticket Authoritys herstellen kann, wird automatisch nur eine Secure Ticket Authority verwendet.

9. Klicken Sie auf Erstellen, um die NetScaler Gateway-Bereitstellung der Liste auf der Seite Remotezugriff hinzuzufügen.

Zum Hinzufügen weiterer Bereitstellungen wiederholen Sie das o. g. Verfahren. Zum Konfigurieren von Remotezugriff auf den Store über Access Gateway 5.0-Cluster folgen Sie den Schritten unter Konfigurieren des Remotezugriffs auf den Store über einen Access Gateway 5.0-Cluster bereit. Wenn Sie alle NetScaler Gateway-Bereitstellungen hinzugefügt haben, kehren Sie zu Schritt 10 unter "Neue Bereitstellung erstellen" zurück.

Konfigurieren des Remotezugriffs auf den Store über einen Access Gateway 5.0-Cluster bereit

Führen Sie die folgenden Schritte aus, um Remotezugriff über einen Access Gateway 5.0-Cluster auf den Store zu konfigurieren, den Sie als Teil der Erstkonfiguration des StoreFront-Servers erstellt haben. Es wird davon ausgegangen, dass Sie die unter "Neue Bereitstellung erstellen" weiter oben beschriebenen Schritte 1 bis 9 ausgeführt haben.

1. Klicken Sie auf der Seite Remotezugriff der Seite der StoreFront-Verwaltungskonsole zum Erstellen von Stores auf Hinzufügen.
2. Geben im Dialogfeld NetScaler Gateway-Gerät hinzufügen einen Namen für den Cluster an, über den die Benutzer diesen identifizieren können.
   Benutzern wird der Anzeigename angezeigt, den Sie in Citrix Receiver angegeben haben. Nehmen Sie deshalb relevante Informationen in den Namen auf, damit Benutzer leichter entscheiden können, ob sie den Cluster verwenden möchten. Beispielsweise können Sie den geographischen Standort in die Anzeigenamen der NetScaler Gateway-Bereitstellungen einfügen, damit Benutzer problemlos das beste Gateway für ihren Standort identifizieren können.

3. Geben Sie die URL des Benutzeranmeldepunkts für den Cluster ein, und wählen Sie aus der Liste Version die Option 5.x aus.
4. Wählen Sie in der Liste Bereitstellungsmodus die Option Access Controller und klicken Sie auf Weiter.
5. Listen Sie auf der Seite Geräte die IP-Adressen oder vollqualifizierten Domänennamen (FQDNs) der Geräte im Cluster auf

und klicken Sie auf Weiter.

6. Listen Sie auf der Seite Authentifizierung ohne Benutzereingriff aktivieren die URLs für den Authentifizierungsdienst, der auf den Access Controller-Servern ausgeführt wird, auf. Geben zur Aktivierung der Fehlertoleranz URLs mehrerer Server ein und führen Sie die Server dabei in der Reihenfolge ihrer Priorität auf, um die Failoversequenz festzulegen. Klicken Sie auf Weiter.
   StoreFront authentifiziert Remotebenutzer über den Authentifizierungsdienst, damit sie ihre Anmeldeinformationen nicht neu eingeben müssen, wenn sie auf Stores zugreifen.

7. Wenn Sie Ressourcen von XenDesktop und XenApp im Store verfügbar machen, listen Sie auf der Seite Secure Ticket Authority (STA) URLs für Server auf, auf denen die STA ausgeführt wird. Geben Sie aus Gründen der Fehlertoleranz URLs für mehrere STAs ein und führen Sie die Server dabei in der Reihenfolge ihrer Priorität auf, um die Failoversequenz festzulegen.
   Die STA wird auf XenDesktop- und XenApp-Servern gehostet und gibt Sitzungstickets als Reaktion auf Verbindungsanforderungen aus. Auf diesen Sitzungstickets basiert die Authentifizierung und Autorisierung für den Zugriff auf XenDesktop- und XenApp-Ressourcen.

8. Aktivieren Sie das Kontrollkästchen Sitzungszuverlässigkeit aktivieren, wenn XenDesktop und XenApp getrennte Sitzungen aufrechterhalten sollen, während Citrix Receiver eine automatische Wiederverbindung versucht. Aktivieren Sie das Kontrollkästchen Tickets von zwei Secure Ticket Authoritys anfordern (falls verfügbar), wenn Sie mehrere STAs konfiguriert haben und sicherstellen möchten, dass Sitzungszuverlässigkeit immer gegeben ist.
   Wenn das Kontrollkästchen Tickets von zwei Secure Ticket Authoritys anfordern (falls verfügbar) aktiviert ist, ruft StoreFront Tickets von zwei verschiedenen Secure Ticket Authoritys ab, damit Benutzersitzungen nicht unterbrochen werden, wenn eine Secure Ticket Authority während der Sitzung ausfällt. Wenn StoreFront aus irgendeinem Grund keine Verbindung zu zwei Secure Ticket Authoritys herstellen kann, wird automatisch nur eine Secure Ticket Authority verwendet.

9. Klicken Sie auf Erstellen, um die NetScaler Gateway-Bereitstellung der Liste auf der Seite Remotezugriff hinzuzufügen.

Zum Hinzufügen weiterer Cluster wiederholen Sie das o. g. Verfahren. Zum Konfigurieren von Remotezugriff auf den Store über NetScaler Gateway oder ein einzelnes Access Gateway 5.0-Gerät folgen Sie den Schritten unter Konfigurieren des Remotezugriffs auf den Store über ein NetScaler Gateway-Gerät. Wenn Sie alle NetScaler Gateway-Bereitstellungen hinzugefügt haben, kehren Sie zu Schritt 10 unter "Neue Bereitstellung erstellen" zurück.

Vorhandener Servergruppe beitreten

Nov 27, 2017

Vor der Installation von StoreFront stellen Sie sicher, dass auf dem Server, den Sie der Gruppe hinzufügen, die gleiche Betriebssystemversion mit dem gleichen Gebietsschema ausgeführt wird, wie auf den anderen Servern in der Gruppe. StoreFront-Servergruppen mit unterschiedlichen Betriebssystemversionen und Gebietsschemas werden nicht unterstützt. Zwar kann eine Servergruppe maximal fünf Server enthalten, basierend auf Simulationen bieten Servergruppen mit mehr als drei Servern jedoch für die Kapazität keinen Vorteil. Außerdem müssen Sie sicherstellen, dass der relative Pfad zu StoreFront in IIS auf dem Server, den Sie hinzufügen, mit dem auf den anderen Servern in der Gruppe identisch ist.

> ## Important
>
> Wenn Sie einer Servergruppe einen neuen Server hinzufügen, werden StoreFront-Dienstkonten als Mitglieder der lokalen Administratorgruppe auf dem neuen Server hinzugefügt. Für diese Dienste sind lokalen Administratorberechtigungen erforderlich, um der Servergruppe beizutreten und für die Synchronisierung. Wenn Sie eine Gruppenrichtlinie verwenden, die verhindert, dass der lokalen Administratorgruppe neue Mitglieder hinzugefügt werden können, bzw. wenn Sie die Berechtigungen der lokalen Administratorgruppe auf den Servern einschränken, kann StoreFront nicht der Servergruppe beitreten.

1. Wenn die Citrix StoreFront-Verwaltungskonsole nach der Installation von StoreFront nicht bereits geöffnet ist, klicken Sie auf der Windows- Startseite oder auf der Apps-Seite auf die Kachel Citrix StoreFront.
2. Klicken Sie im Ergebnisbereich der Citrix StoreFront-Verwaltungskonsole auf Vorhandener Servergruppe beitreten.
3. Melden Sie sich bei einem Server in der StoreFront-Bereitstellung an, der Sie den Server hinzufügen möchten, und öffnen Sie die Citrix StoreFront-Verwaltungskonsole. Wählen Sie im linken Bereich der Konsole den Knoten Servergruppe aus und klicken Sie im Bereich Aktionen auf Server hinzufügen. Notieren Sie sich den angezeigten Autorisierungscode.
4. Kehren Sie zum neuen Server zurück und geben Sie im Dialogfeld Servergruppe beitreten den Namen des vorhandenen Servers im Feld Autorisierungsserver an. Geben Sie den vom primären Server erhaltenen Autorisierungscode ein und klicken Sie auf Beitreten.
   Nach dem Beitritt zu der Gruppe wird die Konfiguration des neuen Servers aktualisiert, damit sie mit der des vorhandenen Servers identisch ist. Alle anderen Server in der Gruppe werden mit den Informationen des neuen Servers aktualisiert.

Verwenden Sie zur Verwaltung einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Alle vorgenommenen Konfigurationsänderungen müssen an die anderen Server der Gruppe weitergegeben werden, damit eine konsistente Konfiguration der gesamten Bereitstellung gewährleistet ist.

Entfernen eines Servers aus einer Servergruppe

Wenn ein StoreFront-Server Mitglied einer Servergruppe war und entfernt wurde, müssen Sie das PowerShell-Cmdlet Clear-DSConfiguration ausführen, um den StoreFront-Server auf die Werkseinstellungen zurücksetzen. Nachdem Sie das Cmdlet Clear-DSConfiguration auf dem getrennten Server ausgeführt haben, fügen Sie den Server wieder einer vorhandenen Servergruppe oder einer anderen, neu erstellten Servergruppe hinzu.

1. Öffnen Sie die StoreFront-Verwaltungskonsole auf dem primären StoreFront-Server, mit dem Sie die gesamte Servergruppe verwalten.
2. Wählen Sie den Knoten für die Servergruppe im linken Bereich aus und wählen Sie dann einen anderen Server zum Entfernen aus.

3. Entfernen Sie den ausgewählten Server aus der Servergruppe.
4. Im Bereich "Aktionen" übertragen Sie die Änderungen vom getrennten Server auf eines der Mitglieder der Servergruppe. Alle anderen Mitglieder der Servergruppe wissen jetzt, dass ein Server aus der Gruppe entfernt wurde. Wenn Sie den getrennten Server nicht auf die Werkseinstellungen zurücksetzen, erkennt er nicht, dass er nicht mehr Mitglied der Gruppe ist.
5. Schließen Sie die Verwaltungskonsole für den getrennten Server.
6. Öffnen Sie eine PowerShell-Sitzung auf dem getrennten Server, der aus der Gruppe entfernt wurde, und importieren Sie die PowerShell-Module von StoreFront mit folgendem Befehl: & "$Env:PROGRAMFILES\Citrix\ReceiverStoreFront\Scripts\ImportModules.ps1"
7. Führen Sie den Befehl Clear-DSConfiguration aus, der den Server auf die Standardeinstellungen zurücksetzt.
8. Öffnen Sie die StoreFront-Verwaltungskonsole. Der getrennte Server wurde zurückgesetzt und kann nun einer anderen Servergruppe hinzugefügt werden.

Migrieren von Webinterface-Features nach StoreFront

Nov 27, 2017

Für viele Webinterface-Anpassungen gibt es Entsprechungen in StoreFront über JavaScript-Optimierungen, veröffentlichten Citrix APIs oder der StoreFront-Verwaltungskonsole.

Die folgende Tabelle enthält eine Übersicht über die Anpassungen und grundlegende Informationen darüber, wie sie programmiert werden.

Ordnerpfade

- Für Skript-Anpassungen fügen Sie die Beispiele in die Datei script.js in folgendem Ordner ein:

  C:\inetpub\wwwroot\Citrix\StoreNameWeb\custom

- Für Stil-Anpassungen fügen Sie die Beispiele in die Datei style.css in folgendem Ordner ein:

  C:\inetpub\wwwroot\Citrix\StoreNameWeb\custom

- Für dynamischen Inhalt fügen Sie den dynamischen Kontext in einer Textdatei in folgendem Ordner ein:

  C:\inetpub\wwwroot\Citrix\StoreNameWeb\customweb

- In Bereitstellungen mit mehreren Servern können Sie alle Änderungen über die StoreFront-Verwaltungskonsole oder PowerShell auf die anderen Server replizieren.

Hinweis: In Webinterface können einzelne Benutzer verschiedene Einstellungen anpassen. Das ist derzeit in StoreFront nicht möglich. Eine solche Möglichkeit kann zwar durch umfassendere Anpassungen geschaffen werden, dies ist jedoch nicht Gegenstand des vorliegenden Artikels.

Webinterface-Funktion	**StoreFront-Äquivalent**
Anpassung per Verwaltungskonsole	
• Layout mit reduziertem Grafikinhalt • Layout mit komplettem Grafikinhalt • Auswahl durch Benutzer	Nicht verfügbar StoreFront erkennt automatisch den Gerätebildschirm und passt die Benutzeroberfläche entsprechend an.
• Aktivieren der Suche • Deaktivieren der Suche	• Die Suche ist standardmäßig aktiviert. • Deaktivieren: Zum Ausblenden der Suchfelder auf der Desktop-/Web-Benutzeroberfläche fügen Sie der Datei style.css folgenden Stil hinzu: **.search-container {** **display: none;** **}**

	Zum Ausblenden der Suchfelder auf der Telefon-Benutzeroberfläche fügen Sie folgenden Stil hinzu: **#searchBtnPhone {** **display: none;** **}**
Aktualisierung	Standardmäßig aktiviert (Browseraktualisierung).
Rückkehr zum letzten Ordner	Nicht standardmäßig aktiviert. Zum Aktivieren der Funktion zum Speichern des aktuellen Ordners und Zurückkehren zu diesem beim Laden fügen Sie der Datei script.js Folgendes hinzu: **CTXS.Extensions.afterDisplayHomeScreen = function ()** **{** **// check if view was saved last time** **CTXS.ExtensionAPI.localStorageGetItem("view",** **function (view) {** **if (view) {** **// if view was saved, change to it** **CTXS.ExtensionAPI.changeView(view);** **}** **if (view == "store") {** **// if view is store, see if folder was saved** **CTXS.ExtensionAPI.localStorageGetItem("folder",** **function(folder) {** **if (folder != "") {** **// if folder was saved, change to it** **CTXS.ExtensionAPI.navigateToFolder(folder);** **}** **}** **);**

	}
	// set up monitoring of folder
	CTXS.Extensions.onFolderChange = function(folder) {
	CTXS.ExtensionAPI.localStorageSetItem("folder",
	folder);
	};
	// set up monitoring of view
	CTXS.Extensions.onViewChange = function(newview) {
	// don't retain search or appinfo views
	// instead, remember parent view.
	if ((newview != "appinfo") &&
	(newview != "search")) {
	CTXS.ExtensionAPI.localStorageSetItem(
	"view", newview);
	}
	};
	});
	};

QuickInfos	In Citrix Receiver gibt es nur sehr wenige QuickInfos, da es für Geräte mit und ohne Touchscreen vorgesehen ist. Siekönnen QuickInfos über ein benutzerdefiniertes Skript hinzufügen.
• Symbolansicht • Baumstrukturansicht • Detailansicht • Listenansicht • Gruppenansicht • Standardansicht festlegen • Symbolansicht (reduzierter Grafikinhalt) • Listenansicht (reduzierter Grafikinhalt) Standardansicht (reduzierter Grafikinhalt)	Citrix Receiver hat eine andere Benutzeroberfläche, daher gelten diese Optionen nicht. Sie können mit der StoreFront-Verwaltungskonsole Ansichten konfigurieren. Weitere Informationen finden Sie unter Angeben verschiedener Ansichten für Anwendungen und Desktops.

• Benutzeroberfläche mit einer Registerkarte
• Benutzeroberfläche mit mehreren Registerkarten
  • App-Registerkarte
  • Desktop-Registerkarte
  • Inhalt-Registerkarte
  • (Registerkartenreihenfolge)
	Die Benutzeroberfläche von Citrix Receiver ist standardmäßig in Registerkarten unterteilt, wobei sich Apps und Inhalt auf einer Registerkarte und Desktops auf der anderen befinden. Es gibt außerdem eine optionale Registerkarte **Favoriten**.

• Kopfzeilenlogo • Textfarbe • Kopfzeilen-Hintergrundfarbe • Kopfzeilen-Hintergrundbild	Äquivalente für Farben und Logos bei Verwendung der StoreFront-Verwaltungskonsole. Klicken Sie in der StoreFront-Verwaltungskonsole im Bereich "Aktionen" auf "Websitedarstellung anpassen" und führen Sie Ihre Anpassungen auf dem angezeigten Bildschirm durch. Mit einer Stil-Anpassung können Sie als Kopfzeile ein Hintergrundbild festlegen. Beispiel: **.theme-header-bgcolor {** **background-image: url('spirals.png');** **}**

• Begrüßungsmeldung vor Anmeldung (vor Gebietsschema)
  • Titel
  • SMS
  • Hyperlink
  • Schaltflächenbezeichnung
	Standardmäßig gibt es keinen eigenen Voranmeldungsbildschirm.
	
	Mit diesem Beispielskript wird ein Meldungsfenster zum Durchklicken hinzugefügt:
	
	var doneClickThrough = false;
	
	// Before web login
	
	CTXS.Extensions.beforeLogon = function (callback) {
	
	doneClickThrough = true;
	
	CTXS.ExtensionAPI.showMessage({
	
	messageTitle: "Willkommen!",
	
	messageText: "Only for WWCo Employees",
	
	okButtonText: "Akzeptieren",
	
	okAction: callback
	
	});
	
	};
	
	// Before main screen (for native clients)

	CTXS.Extensions.beforeDisplayHomeScreen **= function (callback) {** **if (!doneClickThrough) {** **CTXS.ExtensionAPI.showMessage({** **messageTitle: "Willkommen!",** **messageText: "Only for WWCo Employees",** **okButtonText: "Akzeptieren",** **okAction: callback** **});** **} else {** **callback();** **}** **};**
• Titel des Anmeldebildschirms • Meldung des Anmeldebildschirms • Systemmeldung des Anmeldebildschirms	Es gibt vier Bereiche für Anpassungen auf dem Anmeldebildschirm bzw. den Anmeldebildschirmen. Bereichoben und unten im Bildschirm (Kopf- und Fußzeile) und Bereich oben und unten im Anmeldefeld selbst. **.customAuthHeader,** **.customAuthFooter** **.customAuthTop,** **.customAuthBottom {** **text-align: center;** **color: white;** **font-size: 16px;** **}** Beispielskript (statische Inhalte) **$('.customAuthHeader').html("Welcome to ACME");** Beispielskript (dynamische Inhalte) **function setDynamicContent(txtFile, element) {** **CTXS.ExtensionAPI.proxyRequest({**

	url: "customweb/"+txtFile, **success: function(txt) {$(element).html(txt);}});** **}** **setDynamicContent("Message.txt", ".customAuthTop");** Hinweis: Fügen Sie weder explizit im Skript noch im Verzeichnis **custom** dynamische Inhalte ein, da Änderungen hier ein erneutes Laden der Benutzeroberfläche auf allen Clients erzwingen. Fügen Sie dynamische Inhalte im Verzeichnis **customweb** ein.
• Begrüßungsmeldung des Anwendungsbildschirms • Systemmeldung des Anwendungsbildschirms	Siehe Beispiele für **CustomAuth**-Begrüßungsbildschirm oben. Siehe Beispiele für dynamische Inhalte oben. Verwenden Sie **#customTop** anstelle von **#customAuthTop**, um Inhalt auf dem Homebildschirm zu platzieren.
Fußzeilentext (alle Bildschirme)	Beispielskript: **#customBottom {** **text-align: center;** **color: white;** **font-size: 16px;** **}** Beispiel für statische Inhalte unter Verwendung eines Skripts: **$('#customBottom).html("Welcome to ACME");**
Features ohne direkte Entsprechung	
• Anmeldeseite ohne Kopfzeile • Anmeldeseite mit Kopfzeile (einschl. Meldungen)	Es gibt keine direkte Entsprechung in StoreFront. Sie können jedoch benutzerdefinierte Kopfzeilen erstellen.Siehe "Titel des Anmeldebildschirms" oben.
Benutzereinstellungen	Standardmäßig gibt es keine Benutzereinstellungen. Sie können Menüs und Schaltflächen über JavaScript hinzufügen.
Workspace Control	Äquivalente Funktionalität für Administratoreinstellungen. Die Erweiterungs-APIs bieten viel zusätzliche Flexibilität.

	Weitere Informationen finden Sie unter http://www.citrix.com/go/citrix-developer/storefront-receiver-developer-community/receiver-customization-api.html.
Tiefgreifende Anpassung (Code)	
Hooks für die ICA-Dateigenerierung und andere Anpassungen für das Aufrufrouting	Äquivalente oder bessere APIs. http://www.citrix.com/go/citrix-developer/storefront-receiver-developer-community/store-customization-sdk.html
Authentifizierungsanpassungen	Äquivalente oder bessere APIs. http://www.citrix.com/go/citrix-developer/storefront-receiver-developer-community/store-authentication-sdks.html
JSP-/ASP-Quellzugriff	Es gibt keine äquivalenten APIs in StoreFront, da die Benutzeroberfläche nicht auf die gleiche Weise gerendert wird.Es gibt zahlreiche JavaScript-APIs für die Anpassung der Benutzeroberfläche.

Konfigurieren von Servergruppen

Nov 27, 2017

Mit den folgenden Anleitungen können Sie die Einstellungen von StoreFront-Multiserverbereitstellungen ändern. Verwenden Sie zur Verwaltung einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Alle vorgenommenen Konfigurationsänderungen müssen an die anderen Server der Gruppe weitergegeben werden, damit eine konsistente Konfiguration der gesamten Bereitstellung gewährleistet ist.

Sie müssen den StoreFront-Installationsort und die IIS-Website-Einstellungen (z. B. physischer Pfad und Site-IDs) auf den Servern einer StoreFront-Servergruppe identisch konfigurieren.

Hinzufügen eines Servers zu einer Servergruppe

Mit der Aufgabe Server hinzufügen können Sie einen Autorisierungscode abrufen, der es Ihnen ermöglicht, der vorhandenen Bereitstellung einen neu installierten StoreFront-Server hinzuzufügen. Weitere Informationen zum Hinzufügen neuer Server zu vorhandenen StoreFront-Bereitstellungen finden Sie unter Vorhandener Servergruppe beitreten.Informationen zur Einschätzung der Zahl der in der Gruppe benötigten Server finden Sie unter *Planen der StoreFront- Bereitstellung* im Abschnitt Skalierbarkeit.

Entfernen von Servern aus einer Servergruppe

Mit der Aufgabe Server entfernen können Sie Server aus einer StoreFront-Multiserverbereitstellung löschen. Sie können jeden Server in der Gruppe mit Ausnahme des Servers, auf dem Sie die Aufgabe ausführen, entfernen. Entfernen Sie den Server zuerst aus der Lastausgleichsumgebung und dann aus der Multiserverbereitstellung.

Weitergeben lokaler Änderungen an eine Servergruppe

Mit der Aufgabe Änderungen verteilen können Sie die Konfiguration aller anderen Server in einer StoreFront-Multiserverbereitstellung aktualisieren, damit sie mit der Konfiguration des aktuellen Servers übereinstimmt. Alle Änderungen, die auf anderen Servern in der Gruppe vorgenommen wurden, werden verworfen. Beachten Sie bei dieser Aufgabe, dass Sie erst dann weitere Änderungen machen können, wenn alle Server in der Gruppe aktualisiert wurden.

Wichtig: Wenn Sie die Konfiguration eines Servers aktualisieren, ohne die Änderungen auf den anderen Servern in der Gruppe zu übernehmen, können die Aktualisierungen verloren gehen, falls Sie nach dem Vorgang Änderungen von einem anderen Server in der Bereitstellung übernehmen.

Ändern der Basis-URL für eine Bereitstellung

Verwenden Sie die Aufgabe Basis-URL ändern , um die Basis-URL zu ändern, die als Stamm für die URLs der Stores und andere StoreFront-Dienste dient, die in der Bereitstellung gehostet werden. Geben Sie bei Bereitstellungen mit mehreren Servern die Lastausgleichs-URL an. Sie können mit dieser Option jederzeit von HTTP zu HTTPS wechseln, vorausgesetzt, dass die Microsoft-Internetinformationsdienste (IIS) für HTTPS konfiguriert sind.

Zum Konfigurieren von IIS für HTTPS erstellen Sie mit der IIS-Verwaltungskonsole auf dem StoreFront-Server ein Serverzertifikat, das von der Microsoft Active Directory-Domänenzertifizierungsstelle signiert wurde. Fügen Sie anschließend eine HTTPS-Bindung zur Standardwebsite hinzu. Weitere Informationen zum Erstellen eines Serverzertifikats in IIS finden Sie unter http://technet.microsoft.com/de-de/library/hh831637.aspx#CreateCertificate. Weitere Informationen über das Hinzufügen einer HTTPS-Bindung zu einer IIS-Website finden Sie unter http://technet.microsoft.com/de-de/library/hh831632.aspx#SSLBinding.

Konfigurieren der Serverumgehung

Zur Verbesserung der Leistung bei Ausfall von Servern, auf denen Ressourcen bereitgestellt werden, umgeht StoreFront vorübergehend die Server, die nicht antworten. Bei einer Serverumgehung ignoriert StoreFront den Server und verwendet diesen nicht für den Zugriff auf Ressourcen. Verwenden Sie folgende Parameter, um die Dauer der Umgehung festzulegen:

- **Umgehungsdauer bei Ausfall aller Server** ist eine reduzierte Dauer in Minuten, die StoreFront anstelle von **Umgehungsdauer** verwendet, wenn alle Server eines bestimmten Delivery Controllers umgangen werden. Der Standardwert ist 0 Minuten.
- **Umgehungsdauer** ist die Zeit in Minuten, die StoreFront einen einzelnen Server nach einem fehlgeschlagenen Kommunikationsversuch umgeht. Die Standarddauer für die Umgehung ist 60 Minuten.

Überlegungen beim Angeben von "Umgehungsdauer bei Ausfall aller Server"

Die Wahl eines höheren Werts für **Umgehungsdauer bei Ausfall aller Server** vermindert die Auswirkungen eines Ausfalls eines bestimmten Delivery Controllers, jedoch stehen die Ressourcen auf diesem Delivery Controller nach einem temporären Netzwerk- oder Serverausfall Benutzern für die angegebene Dauer nicht zur Verfügung. Verwenden Sie ggf. einen höheren Wert für **Umgehungsdauer bei Ausfall aller Server**, wenn viele Delivery Controller für einen Store konfiguriert sind, insbesondere für nicht geschäftskritische Delivery Controller.

Die Wahl eines niedrigeren Werts für **Umgehungsdauer bei Ausfall aller Server** erhöht die Verfügbarkeit von Ressourcen auf dem Delivery Controller, gleichzeitig jedoch auch das Risiko clientseitiger Timeouts, wenn viele Delivery Controller für einen Store konfiguriert sind und mehrere ausfallen. Es empfiehlt sich, den Standardwert von 0 Minuten für geschäftskritische Delivery Controller, bzw. wenn nur wenige Farmen konfiguriert sind, beizubehalten.

Ändern der Umgehungsparameter für einen Store

Wichtig: Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird.Wenn Sie die Änderungen vorgenommen haben, übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden.

1. Klicken Sie auf der **Windows-Startseite** oder auf der **Apps**-Seite auf die Kachel **Citrix StoreFront**.
2. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores** und klicken Sie im Bereich **Aktionen** auf **Delivery Controller verwalten**.
3. Wählen Sie einen Controller, klicken Sie auf **Bearbeiten** und dann im Bildschirm **Delivery Controller bearbeiten** auf **Einstellungen**.
4. Klicken Sie in der Zeile **Umgehungsdauer bei Ausfall aller Server** auf die zweite Spalte und geben Sie die Dauer in Minuten ein, für die der Delivery Controller als offline gilt, nachdem alle zugehörigen Server nicht antworten.
5. Klicken Sie in der Zeile **Umgehungsdauer** auf die zweite Spalte und geben Sie die Dauer in Minuten ein, für die ein einzelner Server als offline gilt, wenn er nicht antwortet.

Konfigurieren von Authentifizierung und Delegierung

Nov 27, 2017

Es gibt mehrere Methoden für die Authentifizierung und Delegierung, die je nach den Anforderungen gewählt werden können.

Konfigurieren des Authentifizierungsdiensts	Der Authentifizierungsdienst authentifiziert Benutzer mit Microsoft Active Directory und stellt auf diese Weise sicher, dass Benutzer sich nicht erneut anmelden müssen, um auf ihre Desktops und Anwendungen zuzugreifen.
Authentifizierung auf Basis des XML-Diensts	Wenn StoreFront nicht in der gleichen Domäne wie XenApp oder XenDesktop ist und keine Active Directory-Vertrauensstellungen eingerichtet werden können, können Sie StoreFront zur Verwendung des XML-Diensts von XenApp bzw. XenDesktop für die Authentifizierung der Anmeldeinformationen konfigurieren.
Eingeschränkte Kerberos-Delegierung für XenApp 6.5	Verwenden Sie die Aufgabe Kerberos-Delegierung konfigurieren um anzugeben, ob in StoreFront die eingeschränkte Kerberos-Delegierung mit Einzeldomäne für die Authentifizierung bei Delivery Controllern verwendet werden soll.
Smartcardauthentifizierung	Richten Sie die Smartcardauthentifizierung für alle Komponenten in einer typischen StoreFront-Bereitstellung ein.
Benachrichtigungszeitraum für den Kennwortablauf	Wenn Sie zulassen, dass Benutzer von Citrix Receiver für Web-Sites ihre Kennwörter jederzeit ändern können, wird lokalen Benutzern, deren Kennwörter bald ablaufen, beim Anmelden eine Warnung angezeigt.

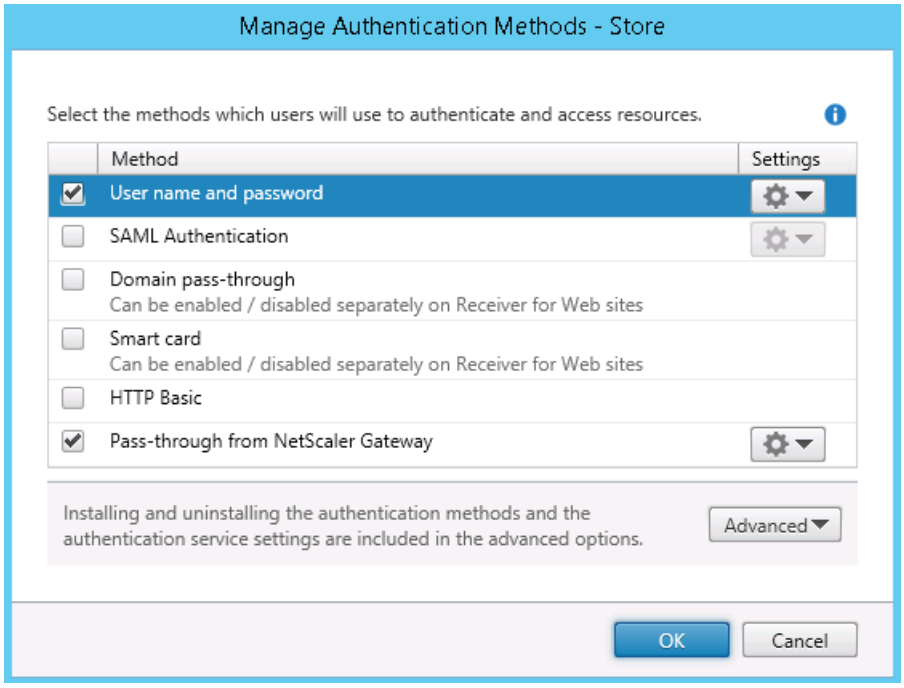
Konfigurieren des Authentifizierungsdiensts

Nov 27, 2017

Verwalten von Authentifizierungsmethoden

Sie können Benutzerauthentifizierungsmethoden, die beim Erstellen des Authentifizierungsdiensts eingestellt wurden, aktivieren oder deaktivieren, indem Sie im Ergebnisbereich der Citrix StoreFront-Verwaltungskonsole eine Authentifizierungsmethode auswählen und im Bereich Aktionen auf Authentifizierungsmethoden verwalten klicken.

1. Klicken Sie auf derWindows-Startseite oder auf der Seite Apps auf die Kachel **Citrix StoreFront**.
2. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores** und klicken Sie im Aktionsbereich auf **Authentifizierungsmethoden verwalten**.
3. Geben Sie an, welche Zugriffsmethoden für die Benutzer aktiviert werden sollen.



- AktivierenSie das Kontrollkästchen **Benutzername und Kennwort**, um die explizite Authentifizierung zu aktivieren. Benutzer geben beim Zugriff auf ihre Stores ihre Anmeldeinformationen ein.
- Wählen Sie das Kontrollkästchen **SAML-Authentifizierung**, um die Integration eines SAML-Identitätsanbieters zu ermöglichen. Benutzer authentifizieren sich bei einem Idenditätsanbieter und werden beim Zugriff auf ihre Stores automatisch angemeldet.Dropdownmenü "Einstellungen":
  - Wählen Sie **Identitätsanbieter**, um die Vertrauensstellung mit dem Identitätsanbieter zu konfigurieren.
  - Wählen Sie **Dienstanbieter**, um die Vertrauensstellung mit dem Dienstanbieter zu konfigurieren. Diese Informationen sind für den Identitätsanbieter erforderlich.

- Aktivieren Sie das Kontrollkästchen Domänen-Passthrough, um Passthrough für Active Directory-Domänenanmeldeinformationen von Benutzergeräten zu aktivieren. Benutzer authentifizieren sich bei den Windows-Computern, die der Domäne angehören, und werden beim Zugriff auf ihre Stores automatisch angemeldet. Um diese Option verwenden zu können, muss Passthrough-Authentifizierung aktiviert sein, wenn Citrix Receiver für Windows auf den Benutzergeräten installiert ist.
- Aktivieren Sie das Kontrollkästchen Smartcard, um die Smartcardauthentifizierung zu aktivieren. Benutzer authentifizieren sich mit Smartcards und PINs beim Zugriff auf ihre Stores.
- Aktivieren Sie das Kontrollkästchen HTTP Basic, um die HTTP Basic-Authentifizierung zu aktivieren. Benutzer authentifizieren sich über den IIS-Webserver des StoreFront-Servers.
- Aktivieren Sie das Kontrollkästchen Passthrough-Authentifizierung von NetScaler Gateway zum Aktivieren der Passthrough-Authentifizierung von NetScaler Gateway. Benutzer authentifizieren sich bei NetScaler Gateway und werden beim Zugriff auf ihre Stores automatisch angemeldet.

Zum Aktivieren der Passthrough-Authentifizierung für Smartcardbenutzer, die auf Stores über NetScaler Gateway zugreifen, verwenden Sie die Aufgabe Delegierte Authentifizierung konfigurieren.

Konfigurieren vertrauenswürdiger Benutzerdomänen

Mit der Aufgabe Vertrauenswürdige Domänen schränken Sie den Zugriff auf Stores für Benutzer ein, die sich mit expliziten Domänenanmeldeinformationen entweder direkt oder über die Passthrough-Authentifizierung von NetScaler Gateway anmelden.

1. Klicken Sie auf der Windows-Startseite oder auf der Apps-Seite auf die Kachel Citrix StoreFront.
2. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten Stores und im Ergebnisbereich die gewünschte Authentifizierungsmethode aus. Klicken Sie im Bereich Aktionen auf **Authentifizierungsmethoden verwalten**.
3. Wählen Sie im Dropdownmenü **Benutzername und Kennwort (explizit) > Einstellungen** die Option **Vertrauenswürdige Domänen konfigurieren** aus.
4. Wählen Sie **Nur vertrauenswürdige Domänen** und klicken Sie auf Hinzufügen, um den Namen einer vertrauenswürdigen Domäne einzugeben. Benutzer mit Konten in der Domäne können sich an allen Stores anmelden, die diesen Authentifizierungsdienst verwenden. Zum Ändern eines Domänennamens wählen Sie den Eintrag in der Liste Vertrauenswürdige Domänen aus und klicken Sie auf Bearbeiten. Wählen Sie eine Domäne in der Liste aus und klicken Sie auf Entfernen, um den Zugriff auf Stores für Benutzerkonten in der Domäne zu entfernen.
   Die Art, in der Sie den Domänennamen angeben, bestimmt das Format, in dem Benutzer ihre Anmeldeinformationen eingeben müssen. Wenn Benutzer ihre Anmeldeinformationen im Format des Domänenbenutzernamens eingeben sollen, fügen Sie der Liste den NetBIOS-Namen hinzu. Sollen Benutzer ihre Anmeldeinformationen im Format des Benutzerprinzipalnamens eingeben, fügen Sie der Liste den vollqualifizierten Domänennamen hinzu. Wenn Benutzern ermöglicht werden soll, ihre Anmeldeinformationen sowohl im Format des Domänenbenutzernamens als auch im Format des Benutzerprinzipalnamens einzugeben, müssen Sie der Liste den NetBIOS-Namen und den vollqualifizierten Domänennamen hinzufügen.
5. Wenn Sie mehrere vertrauenswürdige Domänen konfigurieren, wählen Sie in der Liste Standarddomäne die Domäne aus, die standardmäßig ausgewählt wird, wenn Benutzer sich anmelden.
6. Sollen die vertrauenswürdigen Domänen auf der Anmeldeseite aufgelistet werden, klicken Sie auf das Kontrollkästchen Domänenliste auf Anmeldeseite anzeigen.

Zulassen der Kennwortänderung durch Benutzer

Mit der Aufgabe **Kennwortoptionen verwalten** können Sie zulassen, dass Benutzer von Desktop Receiver und Receiver für Web-Sites, die sich mit Domänenanmeldeinformationen anmelden, ihre Kennwörter ändern. Beim Erstellen des Authentifizierungsdiensts verhindert die Standardkonfiguration, dass Benutzer von Citrix Receiver und Citrix Receiver für Web-Site ihre Kennwörter ändern, selbst wenn die Kennwörter abgelaufen sind. Wenn Sie diese Funktion aktivieren,

vergewissern Sie sich, dass die Richtlinien für die Domänen mit Ihren Servern nicht die Benutzer davon abhalten, ihre Kennwörter zu ändern. Wenn Benutzer Kennwörter ändern können, werden vertrauliche Sicherheitsfunktionen für alle Personen offengelegt, die auf einen der Stores, die diesen Authentifizierungsdienst verwenden, zugreifen können. Wenn Ihr Unternehmen eine Sicherheitsrichtlinie hat, die Funktionen zur Änderung des Kennworts nur zur internen Verwendung reserviert, stellen Sie sicher, dass auf keinen der Stores von außerhalb des Unternehmensnetzwerks zugegriffen werden kann.

1. Citrix Receiver für Web unterstützt die Kennwortänderung bei Ablauf sowie die wahlweise Kennwortänderung. Alle Desktop-Versionen von Citrix Receiver unterstützen die Kennwortänderung über NetScaler Gateway nur bei Kennwortablauf. Klicken Sie auf der Windows-Startseite oder auf der Apps-Seite auf die Kachel Citrix StoreFront.
2. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores** und klicken Sie im Aktionsbereich auf Authentifizierungsmethoden verwalten.
3. Wählen Sie im Dropdownmenü **Benutzername und Kennwörter > Einstellungen** die Option **Kennwortoptionen verwalten** und legen Sie die Bedingungen fest, unter denen Benutzer von Citrix Receiver für Web-Sites, die sich mit Domänenanmeldeinformationen anmelden, ihr Kennwort ändern können.
   - Damit Benutzer ihre Kennwörter jederzeit auf Wunsch ändern können, wählen Sie Jederzeit. Lokalen Benutzern, deren Kennwort bald abläuft, wird bei der Anmeldung eine Warnung angezeigt. Warnungen über den Ablauf von Kennwörtern werden nur für Benutzer angezeigt, die eine Verbindung über das interne Netzwerk herstellen. Standardmäßig hängt der Benachrichtigungszeitraum von der entsprechenden Windows-Richtlinieneinstellung ab. Weitere Informationen zum Einrichten benutzerdefinierter Benachrichtigungszeiträume finden Sie unter Konfigurieren des Zeitraums für den Kennwortablauf. Wird nur für Citrix Receiver für Web unterstützt.
   - Sollen Benutzer ihr Kennwort nur ändern können, wenn es abgelaufen ist, wählen Sie Wenn abgelaufen. Benutzer, die sich nicht anmelden können, weil das Kennwort abgelaufen ist, werden an das Dialogfeld Kennwort ändern weitergeleitet. Wird nur für Citrix Desktop Receiver und Receiver für Web unterstützt.
   - Wenn Sie verhindern möchten, dass Benutzer ihr Kennwort ändern, deaktivieren Sie **Benutzer dürfen Kennwort ändern**. Wenn Sie diese Option nicht auswählen, müssen Sie Benutzern unterstützen, die keinen Zugriff auf ihre Desktops und Anwendungen haben, weil das Kennwort abgelaufen ist.

   Wenn Sie zulassen, dass Benutzer von Citrix Receiver für Web-Sites jederzeit ihre Kennwörter ändern können, muss auf den StoreFront-Servern ausreichend Speicherplatz zum Speichern aller Benutzerprofile vorhanden sein. Um zu prüfen, ob das Kennwort eines Benutzers bald abläuft, erstellt StoreFront ein lokales Profil für den Benutzer auf dem Server. StoreFront muss eine Verbindung mit dem Domänencontroller herstellen können, um die Kennwörter der Benutzer zu ändern.

Citrix Receiver	Benutzer kann ein abgelaufenes Kennwort ändern, sofern in StoreFront aktiviert	Benutzer wird benachrichtigt, dass das Kennwort abläuft	Benutzer kann das Kennwort vor Ablaufen ändern, sofern in StoreFront aktiviert
Windows	Ja		
Mac	Ja		
Android			
iOS			
Linux	Ja		
Web-	Ja	Ja	Ja

Site			
Citrix Receiver	**Benutzer kann ein abgelaufenes Kennwort ändern, sofern in StoreFront aktiviert**	**Benutzer wird benachrichtigt, dass das Kennwort abläuft**	**Benutzer kann das Kennwort vor Ablaufen ändern, sofern in StoreFront aktiviert**

Sicherheitsfragen bei Self-Service-Kennwortzurücksetzung

Mit Self-Service-Kennwortzurücksetzung haben die Benutzer mehr Kontrolle über ihre Benutzerkonten. Wenn Self-Service-Kennwortzurücksetzung konfiguriert ist, können Benutzer, die Probleme mit der Anmeldung haben, ihr Konto entsperren oder ihr Kennwort ändern, nachdem sie einige Sicherheitsfragen korrekt beantwortet haben.

Wenn Sie Self-Service-Kennwortzurücksetzung einrichten, geben Sie an, welche Benutzer Kennwortzurücksetzungen durchführen und ihre Konten über die Verwaltungskonsole entsperren dürfen. Wenn Sie diese Funktionen für StoreFront aktivieren, wird Benutzern unter Umständen aufgrund der in der Konfigurationskonsole für die Self-Service-Kennwortzurücksetzung konfigurierten Einstellungen dennoch die Ausführung dieser Aufgaben verweigert.

Self-Service-Kennwortzurücksetzung steht nur den Benutzern zur Verfügung, die über HTTPS-Verbindungen auf StoreFront zugreifen. Bei verfügbarer Self-Service-Kennwortzurücksetzung können diese Benutzer nicht über eine HTTP-Verbindung auf StoreFront zugreifen und Self-Service-Kennwortzurücksetzung steht nur bei direkter Authentifizierung bei StoreFront mit Benutzernamen und Kennwort zur Verfügung.

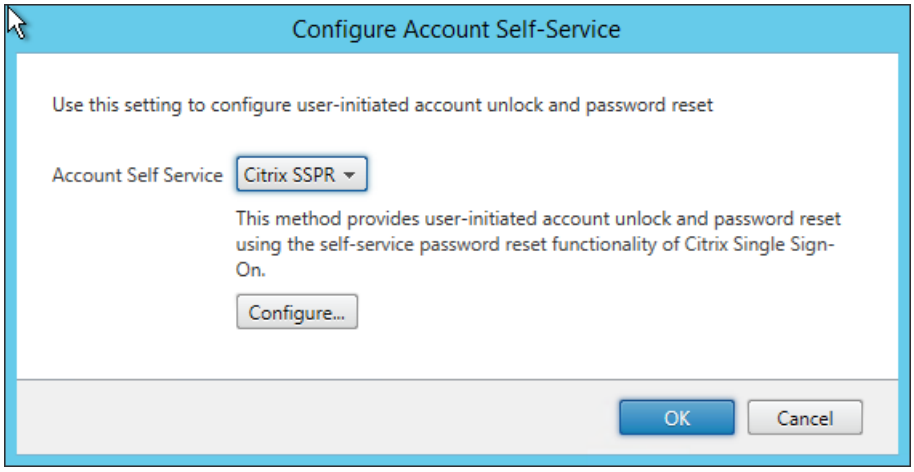
Self-Service-Kennwortzurücksetzung unterstützt keine UPN-Anmeldungen, wie benutzername@domäne.com.

Bevor Sie Self-Service-Kennwortzurücksetzung für einen Store konfigurieren, müssen Sie Folgendes sicherstellen:

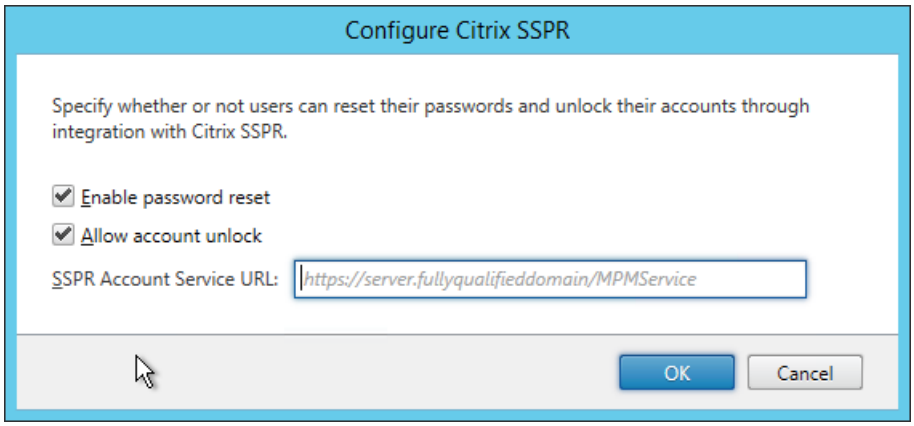
- Der Store ist für die Authentifizierung mit Benutzernamen und Kennwort konfiguriert.
- Der Store ist für die Verwendung von nur einer Self-Service-Kennwortzurücksetzung konfiguriert. Wenn StoreFront zur Verwendung mehrerer Farmen in derselben Domäne oder in vertrauenswürdigen Domänen konfiguriert ist, muss Self-Service-Kennwortzurücksetzung so konfiguriert sein, dass Anmeldeinformationen aus all diesen Domänen akzeptiert werden.
- Der Store ist so konfiguriert, dass Benutzer jederzeit Kennwörter ändern können. Dies ist Voraussetzung dafür, dass Sie die Kennwortzurücksetzung aktivieren können.
- Sie müssen einen StoreFront-Store einer Receiver für Web-Site zuweisen und diese Site zur Verwendung der einheitlichen Benutzeroberfläche konfigurieren.

Zur Verwendung der Self-Service-Kennwortzurücksetzung müssen Sie diese installieren und konfigurieren. Sie ist auf dem XenApp-Medium und dem XenDesktop-Medium verfügbar.Weitere Informationen finden Sie in der Dokumentation Self-Service-Kennwortzurücksetzung.

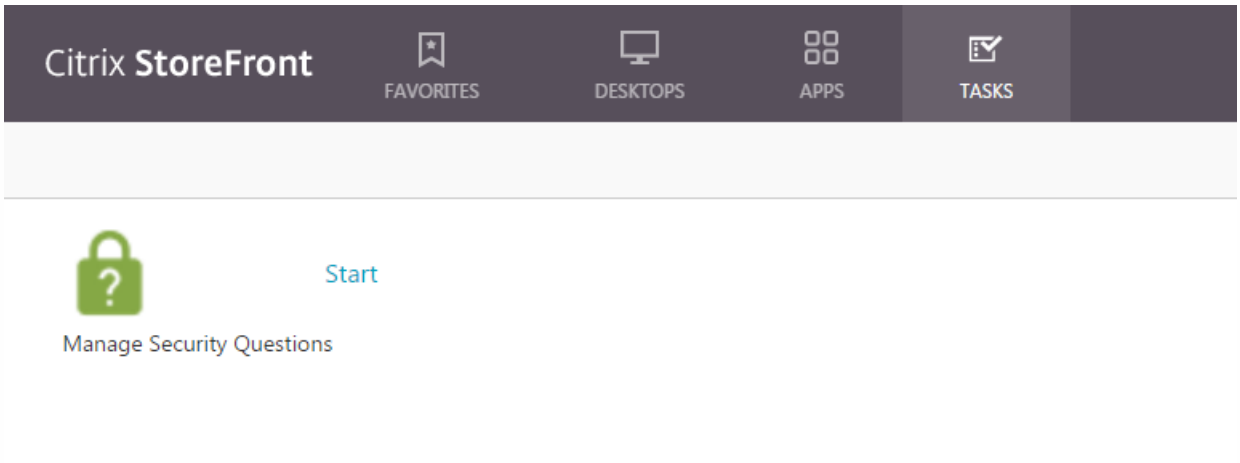
1. Wählen Sie zum Aktivieren der Unterstützung der Self-Service-Kennwortzurücksetzung im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores** aus, klicken Sie im Bereich **Aktionen** auf **Authentifizierungsmethoden verwalten > Benutzername und Kennwort** und wählen Sie im Dropdownmenü **Kennwortoptionen verwalten**.
2. Wählen Sie, wann Benutzer ihre Kennwörter ändern können, und klicken Sie auf **OK**.
3. Wählen Sie im Dropdownmenü **Benutzername und Kennwörter** die Option **Konto-Self-Service konfigurieren**, wählen Sie dann **Citrix SSPR** aus dem Dropdownmenü und klicken Sie auf **OK.**
4. Geben Sie an, ob Benutzer mit Self-Service-Kennwortzurücksetzung ihre Kennwörter zurücksetzen und ihre Konten entsperren können, fügen Sie die Konto-URL für den Self-Service-Kennwortzurücksetzungsdienst hinzu, klicken Sie auf **OK** und dann erneut auf **OK.**



Diese Option ist nur verfügbar, wenn die StoreFront-Basis-URL HTTPS ist (nicht HTTP) und die Option **Zurücksetzen des Kennworts aktivieren** ist nur verfügbar, wenn Sie mit **Kennwortoptionen verwalten** festgelegt haben, dass die Benutzer ihr Kennwort jederzeit ändern können.



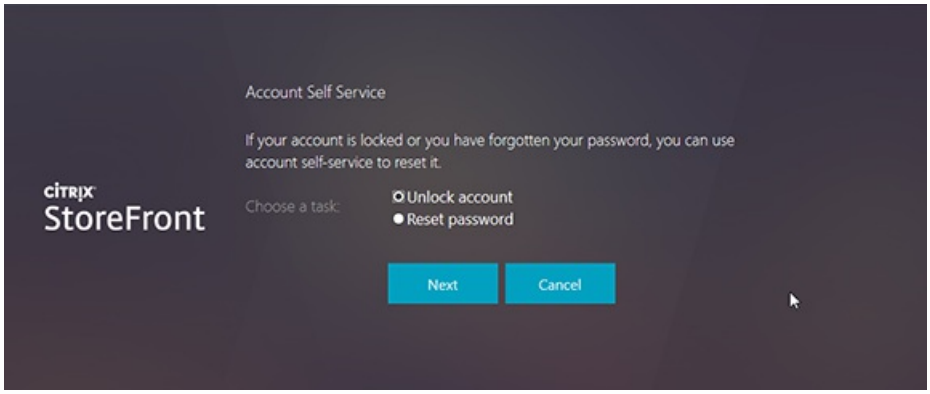
Das nächste Mal, wenn ein Benutzer sich an Citrix Receiver oder Citrix Receiver für Web anmeldet, ist die Registrierung für Sicherheitszwecke verfügbar. Nachdem der Benutzer auf **Start** geklickt hat, werden Fragen angezeigt, für die der Benutzer Antworten angeben muss.



Nach der Aktivierung in StoreFront wird im Anmeldebildschirm von Citrix Receiver für Web der Link **Konto-Self-Service** angezeigt. In anderen Citrix Receiver-Varianten wird die Option als Schaltfläche angezeigt.

Klickt der Benutzer auf den Link, wird er durch mehrere Formulare zur Auswahl zwischen **Konto entsperren** und **Kennwort zurücksetzen** (sofern beides verfügbar) geführt.

Nachdem der Benutzer seine Wahl getroffen und auf **Weiter** geklickt hat, wird er zur Eingabe von Domäne und Benutzername (*domäne\benutzer*) aufgefordert, sofern diese Daten nicht im Anmeldeformular eingegeben wurden. Der Konto-Self-Service unterstützt keine UPN-Anmeldungen, wie benutzername@domäne.com.



Sie sind für die Beantwortung der Sicherheitsfrage erforderlich. Stimmen alle Antworten mit den angegebenen Antworten überein, erfolgt der angeforderte Vorgang (Entsperren oder Zurücksetzen) und der Benutzer wird über dessen Erfolg informiert.

Einstellungen für gemeinsam genutzte Authentifizierung

Verwenden Sie die Aufgabe zur Einstellung des gemeinsam genutzten Authentifizierungsdiensts zum Angeben von Stores, die den Authentifizierungsdienst gemeinsam verwenden, sodass Single Sign-On möglich ist.

1. Klicken Sieauf der Windows-Startseite oder auf der Apps-Seiteauf die Kachel **Citrix StoreFront**.
2. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores** aus und wählen Sie im Ergebnisbereich einen Store aus. Klicken Sie im Bereich **Aktionen** auf **Authentifizierungsmethoden verwalten**.
3. Wählen Sie im Dropdownmenü **Erweitert** die Option **Freigegebener Authentifizierungsdienst - Einstellungen** aus.
4. Klicken Sie auf das Kontrollkästchen **Freigegebenen Authentifizierungsdienst verwenden** und wählen Sie einen Store aus dem Dropdownmenü **Store** aus.

Hinweis: Es gibt keinen Unterschied bei der Funktionsweise eines gemeinsam genutzten und eines dedizierten Authentifizierungsdiensts. Ein von mehreren Stores genutzter Authentifizierungsdienst wird als gemeinsam verwendeter Authentifizierungsdienst behandelt und alle Konfigurationsänderungen gelten für alle Stores, die den Authentifizierungsdienst gemeinsam nutzen.

Delegieren der Anmeldeinformationenvalidierung an NetScaler Gateway

Verwenden Sie die Aufgabe Delegierte Authentifizierung konfigurieren , um die Passthrough-Authentifizierung für Smartcardbenutzer zu aktivieren, die auf Stores über NetScaler Gateway zugreifen. Diese Aufgabe ist nur verfügbar, wenn Passthrough-Authentifizierung von NetScaler Gateway aktiviert und im Ergebnisbereich ausgewählt ist.

Wenn die Validierung der Anmeldeinformationen an NetScaler Gateway delegiert wird, authentifizieren sich Benutzer bei NetScaler Gateway mit Smartcards und werden beim Zugriff auf ihre Stores automatisch angemeldet. Diese Einstellung ist standardmäßig deaktiviert, wenn Sie die Passthrough-Authentifizierung von NetScaler Gateway aktivieren, sodass die Passthrough-Authentifizierung nur erfolgt, wenn Benutzer sich bei NetScaler Gateway mit einem Kennwort anmelden.

Authentifizierung auf Basis des XML-Diensts

Nov 27, 2017

Wenn StoreFront nicht in der gleichen Domäne wie XenApp oder XenDesktop ist und keine Active Directory-Vertrauensstellungen eingerichtet werden können, können Sie StoreFront zur Verwendung des XML-Diensts von XenApp bzw. XenDesktop für die Authentifizierung der Anmeldeinformationen konfigurieren.

Aktivieren der Authentifizierung auf Basis des XML-Diensts

1. Klicken Sie auf derWindows-Startseite oder auf der Apps-Seite auf die Kachel **Citrix StoreFront**.
2. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores** aus und klicken Sie im Aktionsbereich auf **Authentifizierungsmethoden verwalten**.
3. Wählen Sie auf der Seite **Authentifizierungsmethoden verwalten** im Dropdownmenü **Benutzername und Kennwort > Einstellungen** die Option **Kennwortvalidierung konfigurieren** aus.
4. Wählen Sie im Dropdownmenü **Kennwörter validieren mit** die Option **Delivery Controller** und klicken Sie auf **Konfigurieren**.
5. Fügen Sie unter Befolgen der Anweisungen auf den Seiten **Delivery Controller konfigurieren** mindestenseinen Delivery Controller zur Validierung von Anmeldeinformationen hinzu und klicken Sie auf **OK**.

Deaktivieren der Authentifizierung auf Basis des XML-Diensts

1. Klicken Sie auf derWindows-Startseite oder auf der Apps-Seite auf die Kachel **Citrix StoreFront**.
2. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores** aus und klicken Sie im Aktionsbereich auf **Authentifizierungsmethoden verwalten**.
3. Wählen Sie auf der Seite **Authentifizierungsmethoden** im Dropdownmenü **Benutzername und Kennwort > Einstellungen** die Option **Kennwortvalidierung konfigurieren**.
4. Wählen Sie im Dropdownmenü **Kennwörter validieren mit** die Option **Active Directory** und klicken Sie auf **OK**.

Konfigurieren der eingeschränkten Kerberos-Delegierung für XenApp 6.5

Nov 27, 2017

Verwenden Sie die Aufgabe **Storeeinstellungen konfigurieren > Kerberos-Delegierung konfigurieren** um anzugeben, ob in StoreFront die eingeschränkte Kerberos-Delegierung mit Einzeldomäne für die Authentifizierung bei Delivery Controllern verwendet werden soll.

Wichtig: Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Wenn Sie die Änderungen vorgenommen haben, übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden.

1. Klicken Sie auf der Windows-Startseite oder auf der Apps-Seite auf die Kachel Citrix StoreFront.
2. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten Stores und im Ergebnisbereich einen Store aus. Klicken Sie im Bereich Aktionen auf **Storeeinstellungen konfigurieren** und dann auf Kerberos-Delegierung.
3. Aktivieren oder deaktivieren Sie nach Bedarf das Kontrollkästchen Kerberos-Delegierung zum Authentifizieren bei Delivery Controllern verwenden, um die eingeschränkte Kerberos-Delegierung zu aktivieren bzw. zu deaktivieren.

Konfigurieren des StoreFront-Servers für die Delegierung

Verwenden Sie dieses Verfahren, wenn StoreFront nicht auf der gleichen Maschine wie XenApp installiert ist.

1. Öffnen Sie auf dem Domänencontroller das MMC-Snap-In Active Directory-Benutzer und -Computer.
2. Klicken Sie im Menü Ansicht auf Erweiterte Funktionen.
3. Klicken Sie im linken Bereich unter dem Domänennamen auf den Knoten Computer und wählen Sie den StoreFront-Server aus.
4. Klicken Sie im Bereich Aktion auf Eigenschaften.
5. Klicken Sie auf der Registerkarte Delegierung auf Computer bei Delegierungen angegebener Dienste vertrauen und Beliebiges Authentifizierungsprotokoll verwenden und klicken Sie dann auf Hinzufügen .
6. Klicken Sie im Dialogfeld Dienste hinzufügen auf Benutzer oder Computer.
7. Geben Sie im Dialogfeld Benutzer oder Computer auswählen im Feld Geben Sie die zu verwendenden Objektnamen ein den Namen des Servers ein, auf dem der Citrix XML-Dienst (XenApp) ausgeführt wird, und klicken Sie auf OK.
8. Wählen Sie in der Liste den Diensttyp "HTTP" aus und klicken Sie auf OK .
9. Übernehmen Sie die Änderungen und schließen Sie das Dialogfeld.

Konfigurieren des XenApp-Servers für die Delegierung

Konfigurieren Sie die vertrauenswürdige Active Directory-Delegierung für jeden XenApp-Server.

1. Öffnen Sie auf dem Domänencontroller das MMC-Snap-In **Active Directory-Benutzer und -Computer**.
2. Klicken Sie im linken Bereich unter dem Domänennamen auf den Knoten **Computer** und wählen Sie den Server mit dem Citrix XML-Dienst (XenApp) aus, mit dem StoreFront eine Verbindung herstellen soll.
3. Klicken Sie im Bereich **Aktion** auf **Eigenschaften**.
4. Klicken Sie auf der Registerkarte **Delegierung** auf **Computer bei Delegierungen angegebener Dienste vertrauen** und **Beliebiges Authentifizierungsprotokoll verwenden** und klicken Sie dann auf **Hinzufügen**.
5. Klicken Sie im Dialogfeld **Dienste hinzufügen** auf **Benutzer oder Computer**.
6. Geben Sie im Dialogfeld **Benutzer oder Computer auswählen** im Feld **Geben Sie die zu verwendenden**

Objektnamen ein den Namen des Servers ein, auf dem der Citrix XML-Dienst (XenApp) ausgeführt wird, und klicken Sie auf **OK**.

7. Wählen Sie in der Liste den Diensttyp "HOST" aus, klicken Sie auf **OK** und klicken Sie auf **Hinzufügen**.
8. Geben Sie im Dialogfeld **Benutzer oder Computer auswählen** im Feld **Geben Sie die zu verwendenden Objektnamen ein** den Namen des Domänencontrollers ein und klicken Sie dann auf **OK**.
9. Wählen Sie die Diensttypen **cifs** und **ldap** aus der Liste aus und klicken Sie auf **OK**. Hinweis: Wenn für den LDAP-Dienst zwei Optionen angezeigt werden, wählen Sie die Option aus, die mit dem vollqualifizierten Domänennamen des Domänencontrollers übereinstimmt.
10. Übernehmen Sie die Änderungen und schließen Sie das Dialogfeld.

Wichtige Hinweise

Bei der Entscheidung, ob Sie die eingeschränkte Kerberos-Delegierung verwenden sollten, berücksichtigen Sie die nachfolgenden Informationen.

- Wichtige Hinweise:
  - Sie brauchen ssonsvr.exe nicht, es sei denn, Sie verwenden die Passthrough-Authentifizierung (oder die Passthrough-Authentifizierung mit Smartcard-PIN) ohne die eingeschränkte Kerberos-Delegierung.
- Domänenpassthrough bei StoreFront und Citrix Receiver für Web:
  - Sie brauchen ssonsvr.exe auf dem Client nicht.
  - Sie können den Parameter Local username and password in der Citrix Vorlage icaclient.adm auf einen beliebigen Wert setzen (steuert ssonsvr.exe-Funktion).
  - Die Einstellung Kerberos der Vorlage icaclient.adm ist erforderlich.
  - Fügen Sie den vollqualifizierten Domänennamen (FQDN) von StoreFront der Liste der vertrauenswürdigen Websites von Internet Explorer hinzu. Aktivieren Sie die Option Lokalen Benutzernamen verwenden für die vertrauenswürdige Zone in den Sicherheitseinstellungen von Internet Explorer.
  - Der Client muss in einer Domäne sein.
  - Aktivieren Sie die Authentifizierungsmethode Domänen-Passthrough auf dem StoreFront-Server und aktivieren Sie diese auch für Citrix Receiver für Web.
- StoreFront, Citrix Receiver für Web und Smartcardauthentifizierung mit PIN-Eingabeaufforderung:
  - Sie brauchen ssonsvr.exe auf dem Client nicht.
  - Die Smartcardauthentifizierung wurde konfiguriert.
  - Sie können den Parameter Local username and password in der Citrix Vorlage icaclient.adm auf einen beliebigen Wert setzen (steuert ssonsvr.exe-Funktion).
  - Die Einstellung Kerberos der Vorlage icaclient.adm ist erforderlich.
  - Aktivieren Sie die Authentifizierungsmethode Smartcard auf dem StoreFront-Server und aktivieren Sie diese auch für Citrix Receiver für Web.
  - Um sicherzustellen, dass die Smartcardauthentifizierung ausgewählt ist, aktivieren Sie die Option Lokalen Benutzernamen verwenden in den Sicherheitseinstellungen von Internet Explorer für die Zone der StoreFront-Website nicht.
  - Der Client muss in einer Domäne sein.
- NetScaler Gateway, StoreFront, Citrix Receiver für Web und Smartcardauthentifizierung mit PIN-Eingabeaufforderung:
  - Sie brauchen ssonsvr.exe auf dem Client nicht.
  - Die Smartcardauthentifizierung wurde konfiguriert.
  - Sie können den Parameter Local username and password in der Citrix Vorlage icaclient.adm auf einen beliebigen Wert setzen (steuert ssonsvr.exe-Funktion).
  - Die Einstellung Kerberos der Vorlage icaclient.adm ist erforderlich.
  - Aktivieren Sie die Authentifizierungsmethode Passthrough-Authentifizierung von NetScaler Gateway auf dem StoreFront-Server und aktivieren Sie diese auch für Citrix Receiver für Web.
  - Um sicherzustellen, dass die Smartcardauthentifizierung ausgewählt ist, aktivieren Sie die Option Lokalen Benutzernamen verwenden in den Sicherheitseinstellungen von Internet Explorer für die Zone der StoreFront-Website nicht.
  - Der Client muss in einer Domäne sein.
  - Konfigurieren Sie NetScaler Gateway für die Smartcardauthentifizierung und konfigurieren Sie einen zusätzlichen virtuellen Server für den Start mit StoreFront HDX-Routing, um den ICA-Datenverkehr über den virtuellen NetScaler Gateway-Server ohne Authentifizierung zu leiten.
- Citrix Receiver für Windows (AuthManager), Smartcardauthentifizierung mit PIN-Eingabeaufforderung und StoreFront:
  - Sie brauchen ssonsvr.exe auf dem Client nicht.
  - Sie können den Parameter Local username and password in der Citrix Vorlage icaclient.adm auf einen beliebigen Wert setzen (steuert ssonsvr.exe-Funktion).
  - Die Einstellung Kerberos der Vorlage icaclient.adm ist erforderlich.
  - Der Client muss in einer Domäne sein.
  - Aktivieren Sie die Authentifizierungsmethode Smartcard auf dem StoreFront-Server.
- Citrix Receiver für Windows (AuthManager), Kerberos und StoreFront:

- Sie brauchen ssonsvr.exe auf dem Client nicht.
- Sie können den Parameter Local username and password in der Citrix Vorlage icaclient.adm auf einen beliebigen Wert setzen (steuert ssonsvr.exe-Funktion).
- Die Einstellung Kerberos der Vorlage icaclient.adm ist erforderlich.
- Aktivieren Sie die Option Lokalen Benutzernamen verwenden für die vertrauenswürdige Zone in den Sicherheitseinstellungen von Internet Explorer.
- Der Client muss in einer Domäne sein.
- Aktivieren Sie die Authentifizierungsmethode Domänen-Passthrough auf dem StoreFront-Server.
- Stellen Sie sicher, dass der Registrierungsschlüssel auf folgende Einstellung festgelegt ist:

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

32-Bit-Maschinen: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\AuthManagerProtocols\integratedwindows
Name: SSONCheckEnabled
Type: REG_SZ
Wert: true oder false

64-Bit-Maschinen:
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\AuthManagerProtocols\integratedwindows

Name: SSONCheckEnabled
Type: REG_SZ
Wert: true oder false

Konfigurieren der Smartcardauthentifizierung

Jun 04, 2018

Dieser Artikel bietet einen Überblick über die Aufgaben zum Einrichten der Smartcardauthentifizierung für alle Komponenten in einer typischen StoreFront-Bereitstellung. Weitere Informationen und schrittweise Anweisungen zur Konfiguration finden Sie in der Dokumentation für die einzelnen Produkte.

Smartcardkonfiguration für Citrix Umgebungen

This overview for configuring a Citrix deployment for smart cards uses a specific smart card type. Note that similar steps apply to smart cards from other vendors.

- Stellen Sie sicher, dass die Konten für alle Benutzer entweder in der Microsoft Active Directory-Domäne konfiguriert werden, in der Sie die StoreFront-Server bereitstellen, oder in einer Domäne, die eine direkte bidirektionale Vertrauensstellung mit der StoreFront-Serverdomäne hat.
- Wenn Sie die Passthrough-Authentifizierung mit Smartcards aktivieren möchten, müssen Sie sicherstellen, dass die Smartcardleser, die Art und Konfiguration der Middleware und die Richtlinie für das Zwischenspeichern von Middleware-PINs dies gestatten.
- Installieren Sie die Smartcard-Middleware des Herstellers auf den virtuellen oder physischen Maschinen, auf denen Virtual Delivery Agent zur Bereitstellung von Desktops und Anwendungen ausgeführt wird. Weitere Informationen zur Verwendung von Smartcards mit XenDesktop finden Sie unter Smartcards.
- Bevor Sie fortfahren, vergewissern Sie sich, dass die Public Key-Infrastruktur richtig konfiguriert ist. Prüfen Sie die ordnungsgemäße Konfiguration der Zertifikat-/Kontenzuordnung für die Active Directory-Umgebung und ob die Zertifikatüberprüfung erfolgreich ausgeführt werden kann.

- Installieren Sie auf dem NetScaler Gateway-Gerät ein signiertes Serverzertifikat von einer Zertifizierungsstelle. Weitere Informationen finden Sie unter Installieren und Verwalten von Zertifikaten.
- Installieren Sie auf dem Gerät das Stammzertifikat der Zertifizierungsstelle, die die Smartcardbenutzerzertifikate ausstellt. Weitere Informationen finden Sie unter To install a root certificate on NetScaler Gateway.
- Erstellen und konfigurieren Sie einen virtuellen Server für die Clientzertifikatauthentifizierung. Erstellen Sie eine Richtlinie für die Zertifikatauthentifizierung mit SubjectAltName:PrincipalName als Benutzernamenextrahierung aus dem Zertifikat. Binden Sie dann die Richtlinie an den virtuellen Server und konfigurieren Sie den virtuellen Server zum Anfordern von Clientzertifikaten. Weitere Informationen finden Sie unter Configuring and Binding a Client Certificate Authentication Policy.
- Binden Sie das Zertifizierungsstellen-Stammzertifikat an den virtuellen Server. Weitere Informationen finden Sie unter To add a root certificate to a virtual server.
- Sie können sicherstellen, dass Benutzer beim Herstellen einer Verbindung zu ihren Ressourcen nicht ein weiteres Mal vom virtuellen Server aufgefordert werden, ihre Anmeldeinformationen einzugeben, indem Sie einen zweiten virtuellen Server erstellen. Wenn Sie den virtuellen Server erstellen, deaktivieren Sie die Clientauthentifizierung in den SSL-Parametern (Secure Sockets Layer). Weitere Informationen finden Sie unter Konfigurieren der Smartcardauthentifizierung.
  Sie müssen auch StoreFront so konfigurieren, dass Benutzerverbindungen zu Ressourcen über diesen zusätzlichen virtuellen Server geleitet werden. Benutzer melden sich beim ersten virtuellen Server an und der zweite virtuelle Server wird für Verbindungen zu ihren Ressourcen verwendet. Wenn die Verbindung hergestellt ist, brauchen Benutzer sich nicht bei NetScaler Gateway zu authentifizieren. Sie müssen bei der Anmeldung an ihren Desktops und Anwendungen jedoch ihre

PIN eingeben. Das Konfigurieren eines zweiten virtuellen Servers für Verbindungen zu Ressourcen ist optional, sofern Sie nicht planen, allen Benutzern bei Problemen mit der Smartcard den Rückgriff auf die explizite Authentifizierung zu gestatten.

- Erstellen Sie Sitzungsrichtlinien und Profile für Verbindungen von NetScaler Gateway zu StoreFront und binden Sie diese an den geeigneten virtuellen Server. Weitere Informationen finden Sie unter Access to StoreFront Through NetScaler Gateway.
- Wenn Sie den virtuellen Server für Verbindungen mit StoreFront so konfiguriert haben, dass eine Clientzertifikat-Authentifizierung für die gesamte Kommunikation erforderlich ist, müssen Sie einen weiteren virtuellen Server zum Bereitstellen der Callback-URL für StoreFront erstellen. Dieser virtuelle Server wird nur von StoreFront verwendet, um Anforderungen vom NetScaler Gateway-Gerät zu überprüfen. Daher muss er nicht öffentlich zugänglich sein. Ein eigener virtueller Server ist erforderlich, wenn die Clientzertifikat-Authentifizierung obligatorisch ist, da StoreFront kein Zertifikat für die Authentifizierung vorlegen kann. Weitere Informationen finden Sie unter Creating Virtual Servers.

- Sie müssen HTTPS für die Kommunikation zwischen StoreFront und Benutzergeräten verwenden, um die Smartcardauthentifizierung zu aktivieren. Konfigurieren Sie Microsoft-Internetinformationsdienste (IIS) für HTTPS, indem Sie ein SSL-Zertifikat in IIS beziehen und dann die HTTPS-Bindung zu der Standardwebsite hinzufügen. Weitere Informationen zum Erstellen eines Serverzertifikats in IIS finden Sie unter http://technet.microsoft.com/de-de/library/hh831637.aspx#CreateCertificate. Weitere Informationen über das Hinzufügen einer HTTPS-Bindung zu einer IIS-Website finden Sie unter http://technet.microsoft.com/de-de/library/hh831632.aspx#SSLBinding.
- Wenn Sie möchten, dass Clientzertifikate für HTTPS-Verbindungen zu allen StoreFront-URLs präsentiert werden, konfigurieren Sie IIS auf dem StoreFront-Server.
  Wenn StoreFront installiert ist, erfordert die Standardkonfiguration in IIS nur, dass Clientzertifikate für HTTPS-Verbindungen mit der URL für die Zertifikatauthentifizierung des StoreFront-Authentifizierungsdiensts präsentiert werden. Diese Konfiguration ist erforderlich, damit Smartcardbenutzer auf die explizite Authentifizierung zurückgreifen können und damit Benutzer bei entsprechenden Windows-Richtlinieneinstellungen ihre Smartcard entfernen können, ohne sich neu authentifizieren zu müssen.

  Wenn IIS so konfiguriert ist, dass Clientzertifikate für HTTPS-Verbindungen zu allen StoreFront-URLs erforderlich sind, können Benutzer von Smartcards keine Verbindung über NetScaler Gateway herstellen und nicht auf die explizite Authentifizierung zurückgreifen. Sie müssen sich dann neu anmelden, wenn sie ihre Smartcards aus Geräten entfernen. Zum Aktivieren dieser IIS-Sitekonfiguration müssen Authentifizierungsdienst und Stores auf demselben Server sein und es muss ein Clientzertifikat verwendet werden, das für alle Stores gilt. Die Konfiguration, bei der IIS Clientzertifikate für HTTPS-Verbindungen zu allen StoreFront-URLs benötigt, verursacht einen Konflikt mit der Authentifizierung für Citrix Receiver für Web-Clients. Aus diesem Grund sollte diese Konfiguration nur verwendet werden, wenn Citrix Receiver für Web-Clientzugriff nicht erforderlich ist.

- Installieren und konfigurieren Sie StoreFront. Erstellen Sie den Authentifizierungsdienst und fügen Sie Ihre Stores wie erforderlich hinzu. Wenn Sie Remotezugriff über NetScaler Gateway konfigurieren, aktivieren Sie nicht die VPN-Integration (virtuelles privates Netzwerk). Weitere Informationen finden Sie unter Installieren und Einrichten von StoreFront.
- Aktivieren Sie die Smartcardauthentifizierung bei StoreFront für lokale Benutzer im internen Netzwerk. Für Smartcardbenutzer, die auf Stores über NetScaler Gateway zugreifen, aktivieren Sie die Passthrough-Authentifizierung mit NetScaler Gateway und stellen Sie sicher, dass StoreFront so konfiguriert ist, dass die Überprüfung der Anmeldeinformationen an NetScaler Gateway delegiert wird. Wenn Sie beabsichtigen, die Passthrough-Authentifizierung zu aktivieren, wenn Sie Citrix Receiver für Windows auf in Domänen eingebundenen Benutzergeräten installieren,

aktivieren Sie die Domänen-Passthrough-Authentifizierung. Weitere Informationen finden Sie unter Konfigurieren des Authentifizierungsdiensts.
Für die Citrix Receiver für Web-Clientauthentifizierung mit Smartcards müssen Sie die Authentifizierungsmethode über Citrix Receiver für Web-Site aktivieren. Weitere Informationen finden Sie unter Konfigurieren von Citrix Receiver für Web-Sites.

Wenn Sie Smartcardbenutzern gestatten möchten, bei Problemen mit der Smartcard auf die explizite Authentifizierung zurückzugreifen, deaktivieren Sie die Authentifizierung über Benutzernamen und Kennwort nicht.

- Wenn Sie beabsichtigen, die Passthrough-Authentifizierung zu aktivieren, wenn Sie Citrix Receiver für Windows auf domänengebundenen Benutzergeräten installieren, bearbeiten Sie die Datei "default.ica" für den Store, um den Passthrough der Smartcardanmeldeinformationen bei Zugriff auf Desktops und Anwendungen zu ermöglichen. Weitere Informationen finden Sie unter Aktivieren von Passthrough mit Smartcardauthentifizierung für Citrix Receiver für Windows.
- Wenn Sie einen zusätzlichen virtuellen Server für NetScaler Gateway erstellt haben, der ausschließlich für Verbindungen zu Ressourcen verwendet werden soll, konfigurieren Sie das optimale NetScaler Gateway-Routing über diesen virtuellen Server für Verbindungen mit den Bereitstellungen von Desktops und Anwendungen für den Store. Weitere Informationen finden Sie unter Konfigurieren des optimalen HDX-Routings für einen Store.
- Damit Benutzer nicht domänengebundener Windows-Desktopgeräte sich bei ihren Desktops mit Smartcards anmelden können, aktivieren Sie die Smartcardauthentifizierung bei den Desktopgerätesites. Weitere Informationen finden Sie unter Konfigurieren von Desktopgerätesites.

  Konfigurieren Sie die Desktopgerätesite für Smartcard- und explizite Authentifizierung, damit sich Benutzer bei einem Problem mit der Smartcard mit expliziten Anmeldeinformationen anmelden können.

- Damit Benutzer domänengebundener Desktopgeräte und umfunktionierter PCs, auf denen Citrix Desktop Lock ausgeführt wird, sich mit Smartcards authentifizieren können, aktivieren Sie die Passthrough-Authentifizierung mit Smartcards für die XenApp Services-URLs. Weitere Informationen finden Sie unter Konfigurieren der Authentifizierung für XenApp Services-URLs.

- Stellen Sie sicher, dass die Smartcard-Middleware des Herstellers auf allen Benutzergeräten installiert ist.
- Installieren Sie für Benutzer nicht domänengebundener Windows-Desktopgeräte Citrix Receiver für Windows Enterprise mit einem Konto mit Administratorrechten. Konfigurieren Sie Internet Explorer so, dass die Anwendung im Vollbildmodus gestartet und die Desktopgerätesite angezeigt wird, wenn das Gerät eingeschaltet ist. Beachten Sie, dass bei Desktopgerätesite-URLszwischen Groß- und Kleinschreibung unterschieden wird. Fügen Sie die Desktopgerätesite der Zone "Lokales Intranet" oder "Vertrauenswürdige Sites" in Internet Explorer hinzu. Nachdem Sie geprüft haben, dass Sie sich bei der Desktopgerätesite mit einer Smartcard anmelden und auf Ressourcen aus dem Store zugreifen können, installieren Sie Citrix Desktop Lock. Weitere Informationen finden Sie unter Installieren von Desktop Lock.
- Installieren Sie für Benutzer domänengebundener Desktopgeräte und für Benutzer umfunktionierter PCs Citrix Receiver für Windows Enterprise mit einem Konto mit Administratorrechten. Konfigurieren Sie Receiver für Windows mit der XenApp Services-URL für den entsprechenden Store. Nachdem Sie geprüft haben,dass Sie sich bei dem Gerät mit einer Smartcard anmelden und auf Ressourcen aus dem Store zugreifen können, installieren Sie Citrix Desktop Lock. Weitere Informationen finden Sie unter Installieren von Desktop Lock.
- Für alle anderen Benutzer installieren Sie die entsprechende Version von Citrix Receiver auf dem Benutzergerät. Zum Aktivieren des Passthrough von Smartcardanmeldeinformationen zu XenDesktop und XenApp für Benutzer domänengebundener Geräte verwenden Sie ein Konto mit Administratorrechten für die Installation von Receiver für Windows an einer Eingabeaufforderung mit der Option /includeSSON. Weitere Informationen finden Sie unter

Konfigurieren und Installieren von Receiver für Windows mit Befehlszeilenparametern.
Stellen Sie sicher, dass Receiver für Windows für die Smartcardauthentifizierung über eine Domänenrichtlinie oder eine lokale Computerrichtlinie konfiguriert wurde. Für eine Domänenrichtlinie importieren Sie mit der Gruppenrichtlinien-Verwaltungskonsole die Gruppenrichtlinienobjektvorlage icaclient.adm für Receiver für Windows auf den Controller der Domäne, in der die Benutzerkonten sind. Zum Konfigurieren eines einzelnen Geräts konfigurieren Sie mit dem Gruppenrichtlinienobjekt-Editor auf dem Gerät die Vorlage. Weitere Informationen finden Sie unter Konfigurieren von Receiver mit der Gruppenrichtlinienobjektvorlage.

Aktivieren Sie die Richtlinie Smartcardauthentifizierung. Zum Gestatten von Passthrough der Smartcardanmeldeinformationen wählen Sie Use pass-through authentication for PIN. Damit die Smartcardanmeldeinformationen an XenDesktop und XenApp weitergeleitet werden, aktivieren Sie dann die Richtlinie Local user name and password und wählen Sie die Option Allow pass-through authentication for all ICA connections. Weitere Informationen finden Sie in der Referenz zu ICA-Einstellungen.

Wenn Sie Passthrough von Smartcardanmeldeinformationen an XenDesktop und XenApp für Benutzer domänengebundener Geräte aktiviert haben, fügen Sie die Store-URL der Zone "Lokales Intranet" oder "Vertrauenswürdige Sites" in Internet Explorer hinzu. Stellen Sie sicher, dass Automatische Anmeldung mit aktuellem Benutzernamen und Kennwort in den Sicherheitseinstellungen der Zone ausgewählt ist.

- Wo nötig, stellen Sie Benutzern die Verbindungsinformationen für den Store (Benutzer im internen Netzwerk) oder das NetScaler Gateway-Gerät (für Remotebenutzer) mit einer entsprechenden Methode zur Verfügung. Weitere Informationen über die Bereitstellung von Konfigurationsinformationen für die Benutzer finden Sie unter Citrix Receiver.

Sie können die Passthrough-Authentifizierung aktivieren, wenn Sie Receiver für Windows auf Benutzergeräten installieren, die in der Domäne sind. Bearbeiten Sie die Datei default.ica für den Store, um Passthrough der Smartcardanmeldeinformationen des Benutzers beim Zugriff auf Desktops und Anwendungen zu aktivieren,die von XenDesktop und XenApp gehostet werden.

Wichtig: Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Wenn Sie die Änderungen vorgenommen haben, übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden.

1. Öffnen Sie die Datei default.ica für den Store mit einem Text-Editor.Die Datei ist normalerweise im Verzeichnis C:\inetpub\wwwroot\Citrix\storename\App_Data\ wobei storename für den Namen steht, der beim Erstellen des Stores angegeben wurde.
2. Um Passthrough der Smartcardanmeldeinformationen für Benutzer zu aktivieren, die ohne NetScaler Gateway auf Stores zugreifen, fügen Sie dem Abschnitt [Application] die folgenden Einstellung hinzu.
   DisableCtrlAltDel=Off
   Diese Einstellung gilt für alle Benutzer des Stores. Um die Passthrough-Authentifizierung für Domänen und mit Smartcards für Desktops und Anwendungen zu aktivieren, müssen Sie für jede Authentifizierungsmethode separate Stores erstellen. Dann verweisen Sie die Benutzer auf den entsprechenden Store für die Authentifizierungsmethode.

3. Um Passthrough der Smartcardanmeldeinformationen für Benutzer zu aktivieren, die über NetScaler Gateway auf Stores zugreifen, fügen Sie dem Abschnitt [Application] die folgenden Einstellung hinzu.
   UseLocalUserAndPassword=On
   Diese Einstellung gilt für alle Benutzer des Stores. Um die Passthrough-Authentifizierung für bestimmte Benutzer zu aktivieren, während andere sich anmelden müssen, um auf ihre Desktops und Anwendungen zuzugreifen, müssen Sie für

jede Gruppe von Benutzern verschiedenen Stores erstellen. Dann verweisen Sie die Benutzer auf den entsprechenden Store für die Authentifizierungsmethode.

Konfigurieren des Zeitraums für den Kennwortablauf

Nov 27, 2017

Wenn Sie zulassen, dass Benutzer von Citrix Receiver für Web-Sites ihre Kennwörter jederzeit ändern können, wird lokalen Benutzern, deren Kennwörter bald ablaufen, beim Anmelden eine Warnung angezeigt. Standardmäßig hängt der Benachrichtigungszeitraum von der entsprechenden Windows-Richtlinieneinstellung ab. Um einen benutzerdefinierten Benachrichtigungszeitraum für alle Benutzer einzustellen, bearbeiten Sie die Konfigurationsdatei für den Authentifizierungsdienst.

Wichtig: Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Wenn Sie die Änderungen vorgenommen haben, übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden.

1. Klicken Sie auf derWindows-Startseite oder auf der Apps-Seite auf die Kachel **Citrix StoreFront**.
2. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores** aus und klicken Sie im Aktionsbereich auf **Authentifizierungsmethoden verwalten**.
3. Wählen Sie auf der Seite **Authentifizierungsmethoden verwalten** im Dropdownmenü **Benutzername und Kennwort** > **Einstellungen** die Option **Kennwortoptionen verwalten** und aktivieren Sie das Kontrollkästchen **Benutzer dürfen Kennwort ändern**.
4. Wählen Sie **Jederzeit** und treffen Sie eine Auswahl für **Benutzer vor dem Ablauf des Kennworts erinnern**.

Hinweis: StoreFront unterstützt keine differenzierte Kennwortrichtlinie in Active Directory.

Konfigurieren und Verwalten von Stores

Nov 27, 2017

Citrix StoreFront ermöglicht das Erstellen und Verwalten von Stores für Anwendungen und Desktops aus XenDesktop und XenApp, in denen sich Benutzer nach Bedarf selbst bedienen können.

Erstellen und Entfernen von Stores	Sie können beliebig viele zusätzliche Stores konfigurieren.
Erstellen eines Stores ohne Authentifizierung	Konfigurieren Sie zusätzliche Stores ohne Authentifizierung für nicht authentifizierte (anonyme) Benutzer.
Exportieren von Store-Provisioningdateien für Benutzer	Generieren Sie Dateien mit Verbindungsinformationen für Stores, einschließlich NetScaler Gateway-Bereitstellungen und Beacons, die für Stores konfiguriert wurden.
Ausblenden und Ankündigen von Stores für Benutzer	Verhindern Sie, dass Stores den Benutzern zum Hinzufügen zu ihrem Konto angezeigt werden, wenn diese Citrix Receiver über die e-mail-basierte Kontenermittlung oder den vollqualifizierten Domänennamen (FQDN) konfigurieren.
Verwalten der durch Stores zur Verfügung gestellten Ressourcen	Fügen Sie Ressourcen in Stores hinzu oder entfernen Sie Ressourcen daraus.
Verwalten des Remotezugriffs auf Stores über NetScaler Gateway	Konfigurieren Sie den Zugriff auf Stores über NetScaler Gateway für Benutzer in öffentlichen Netzwerken.
Integrieren von Citrix Online-Anwendungen in Stores	Wählen Sie Citrix Online-Anwendungen zum Hinzufügen zu einem Store aus und legen Sie die Aktion fest, die Citrix Receiver ausführt, wenn Benutzer eine Citrix Online-Anwendung abonnieren.
Konfigurieren zweier StoreFront-Stores zur gemeinsamen Nutzung eines Abonnementdatenspeichers	Konfigurieren Sie zwei Stores zur gemeinsamen Nutzung eines Abonnementdatenspeichers.
Erweiterte Storeeinstellungen	Konfigurieren erweiterter Storeeinstellungen

Erstellen und Entfernen von Stores

Jun 04, 2018

Verwenden Sie die Aufgabe Store erstellen zum Konfigurieren zusätzlicher Stores. Sie können beliebig viele Stores erstellen. Beispielsweise kann es empfehlenswert sein, einen Store für eine bestimmte Benutzergruppe zu erstellen oder bestimmte Ressourcen zusammenzufassen. Sie können auch einen Store ohne Authentifizierung erstellen, der anonymen bzw. nicht authentifizierten Zugriff ermöglicht. Anweisungen zum Erstellen dieser Art von Store finden Sie unter Erstellen eines Stores ohne Authentifizierung.

Zum Erstellen eines Stores identifizieren und konfigurieren Sie die Kommunikation mit den Servern, auf denen die Ressourcen, die Sie im Store zur Verfügung stellen möchten, bereitgestellt werden. Anschließend konfigurieren Sie optional Remotezugriff auf den Store über NetScaler Gateway.

Wichtig: Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Wenn Sie die Änderungen vorgenommen haben, übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden.

1. Klicken Sie auf der Windows-Startseite oder auf der Apps-Seite auf die Kachel Citrix StoreFront.
2. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten Stores und klicken Sie im Bereich Aktionen auf Store erstellen.
3. Geben Sie auf der Seite Storename einen Namen für den Store an und klicken Sie auf Weiter.
   Storenamen erscheinen in Citrix Receiver unter den Konten der Benutzer. Wählen Sie daher einen Namen, anhand dessen Benutzer den Inhalt des Stores erkennen können.
4. Listen Sie auf der Seite Delivery Controller die Infrastruktur und die Ressourcen auf, die Sie im Store zur Verfügung stellen möchten. Klicken Sie auf Hinzufügen.
5. Geben Sie im Dialogfeld Delivery Controller hinzufügen einen Namen an, über den Sie die Bereitstellung identifizieren können, und geben Sie an, ob die Ressourcen, die Sie über den Store verfügbar machen möchten, von XenDesktop, XenApp oder AppController bereitgestellt werden. Für App Controller-Bereitstellungen stellen Sie sicher, dass der Name keine Leerzeichen enthält.
6. Wenn Sie Details für XenDesktop- oder XenApp-Server hinzufügen, fahren Sie mit Schritt 7 fort. Geben Sie den Namen oder die IP-Adresse eines virtuellen App Controller-Geräts im Feld Server ein und geben Sie den Port an, der von StoreFront für Verbindungen mit App Controller verwendet werden soll, um von App Controller verwaltete Anwendungen im Store verfügbar zu machen. Der Standardport ist 443. Fahren Sie mit Schritt 11 fort.
7. Um Desktops und Anwendungen, die von XenDesktop oder XenApp bereitgestellt werden, im Store verfügbar zu machen, fügen Sie die Namen oder IP-Adressen der Server der Liste Server hinzu. Geben Sie aus Gründen der Fehlertoleranz mehrere Server an und führen Sie die Server dabei in der Reihenfolge ihrer Priorität auf, um die Failover-Reihenfolge festzulegen. Geben Sie für XenDesktop-Sites die Details der Delivery Controller an. Listen Sie für XenApp-Farmen Server auf, auf denen der Citrix XML-Dienst ausgeführt wird.
8. Wählen Sie aus der Liste Transporttyp die Verbindungstypen für StoreFront aus, die für die Kommunikation mit den Servern verwendet werden sollen.
   - Wählen Sie HTTP aus, wenn Daten über unverschlüsselte Verbindungen gesendet werden sollen. Bei Auswahl dieser Option müssen Sie eigene Maßnahmen treffen, um die Verbindungen zwischen StoreFront und den Servern zu sichern.
   - Wählen Sie HTTPS aus, um Daten über sichere HTTP-Verbindungen mit SSL (Secure Sockets Layer) oder TLS (Transport Layer Security) zu senden. Wenn Sie diese Option für XenDesktop- oder XenApp-Server auswählen,

vergewissern Sie sich, dass der Citrix XML-Dienst so konfiguriert ist, dass der Port gemeinsam mit Internetinformationsdienste (IIS) verwendet wird und in der IIS-Konfiguration HTTPS-Unterstützung festgelegt wurde.
- Wählen Sie SSL-Relay aus, um Daten über sichere Verbindungen an XenApp-Server zu senden. SSL-Relay übernimmt die Hostauthentifizierung und Datenverschlüsselung.

Hinweis: Wenn Sie die Verbindungen zwischen StoreFront und den Servern mit HTTPS oder SSL-Relay sichern, achten Sie darauf, dass die in der Liste Server eingegebenen Servernamen genau mit den Namen in den Zertifikaten für die Server übereinstimmen. Dies gilt auch für die Groß- und Kleinschreibung.

9. Geben Sie den Port an, den StoreFront für Verbindungen mit den Servern verwenden soll. Der Standardport ist 80 für Verbindungen über HTTP und SSL-Relay bzw. 443 für HTTPS-Verbindungen. Bei XenDesktop- und XenApp-Servern muss der angegebene Port dem vom Citrix XML-Dienst verwendeten Port entsprechen.
10. Wenn Sie SSL-Relay verwenden, um Verbindungen zwischen StoreFront und XenApp-Servern zu sichern, geben Sie den TCP-Port für SSL-Relay im Feld SSL-Relay-Port an. Der Standardport ist 443. Stellen Sie sicher, dass alle Server, auf denen SSL-Relay ausgeführt wird, denselben Port überwachen.
11. Klicken Sie auf OK. Sie können Stores konfigurieren, die Ressourcen aus einer beliebigen Zusammenstellung von XenDesktop-, XenApp- und App Controller-Bereitstellungen bieten. Wiederholen Sie erforderlichenfalls die Schritte 4 bis 11, um weitere Bereitstellungen von Ressourcen für den Store aufzulisten. Wenn Sie alle erforderlichen Ressourcen zum Store hinzugefügt haben, klicken Sie auf Weiter.
12. Geben Sie auf der Seite Remotezugriff an, ob und wie Benutzer, die eine Verbindung aus öffentlichen Netzwerken herstellen, über NetScaler Gateway auf den Store zugreifen können.
    - Soll der Store Benutzern in öffentlichen Netzwerken nicht zur Verfügung stehen, stellen Sie sicher, dass die Option **Remotezugriff aktivieren** deaktiviert ist. Nur lokale Benutzer im internen Netzwerk können dann auf den Store zugreifen.
    - Um den Remotezugriff zu ermöglichen, aktivieren Sie **Remotezugriff aktivieren**.
        - Wenn Sie nur Ressourcen, die über den Store angeboten werden, über NetScaler Gateway verfügbar machen möchten, wählen Sie Kein VPN-Tunnel aus. Benutzer melden sich direkt bei NetScaler Gateway an und müssen das NetScaler Gateway-Plug-In nicht verwenden.
        - Wählen Sie Vollständiger VPN-Tunnel aus, um den Store und alle andere Ressourcen im internen Netzwerk über einen SSL-VPN-Tunnel (VPN = virtuelles privates Netzwerk) verfügbar zu machen. Benutzer benötigen das NetScaler Gateway-Plug-In für das Erstellen des VPN-Tunnels.

    Falls noch nicht geschehen, wird automatisch die Passthrough-Authentifizierung von NetScaler Gateway aktiviert, wenn Sie Remotezugriff auf den Store konfigurieren. Benutzer authentifizieren sich bei NetScaler Gateway und werden beim Zugriff auf ihre Stores automatisch angemeldet.

13. Wenn Sie Remotezugriff aktiviert haben, fahren Sie mit dem nächsten Verfahren fort, um die NetScaler Gateway-Bereitstellungen, über die Benutzer auf den Store zugreifen können, anzugeben. Andernfalls klicken Sie auf der Seite Remotezugriff auf Erstellen. Nach dem Erstellen des Stores klicken Sie auf Fertig stellen.

Führen Sie die folgenden Schritte zum Konfigurieren von Remotezugriff über NetScaler Gateway auf den Store, den Sie im vorherigen Verfahren erstellt haben, durch. Es wird davon ausgegangen, dass Sie alle oben beschriebenen Schritte durchgeführt haben.

1. Wählen Sie auf der Seite **Remotezugriff** des Assistenten zum Erstellen von Stores in der Liste **NetScaler Gateway-Geräte** die Bereitstellungen aus, über die Benutzerauf den Store zugreifen können. Die Liste enthält alle Bereitstellungen, die zuvor für andere Stores konfiguriert wurden. Wenn Sie eine weitere Bereitstellung hinzufügen möchten, klicken Sie auf "Hinzufügen". Fahren Sie andernfalls mit Schritt 12 fort.

2. Geben im Dialogfeld **NetScaler Gateway-Gerät hinzufügen > Allgemeine Einstellungen** einen Namen für die NetScaler Gateway-Bereitstellung an, über den die Benutzer diese identifizieren können.
   Benutzern wird der Anzeigename angezeigt, den Sie in Citrix Receiver angegeben haben. Nehmen Sie deshalb relevante Informationen in den Namen auf, damit Benutzer leichter entscheiden können, ob sie die Bereitstellung verwenden möchten. Beispielsweise können Sie den geographischen Standort in die Anzeigenamen der NetScaler Gateway-Bereitstellungen einfügen, damit Benutzer problemlos das beste Gateway für ihren Standort identifizieren können.

3. Geben Sie die URL des virtuellen Servers oder Benutzeranmeldepunkts für die Bereitstellung an. Geben Sie die Produktversion Ihrer Bereitstellung an.
   Der vollqualifizierte Domänenname (FQDN) für die StoreFront-Bereitstellung muss eindeutig sein und darf nicht dem vollqualifizierten Domänennamen des virtuellen NetScaler Gateway-Servers entsprechen. Das Verwenden des selben vollqualifizierten Domänennamens für StoreFront und den virtuellen NetScaler Gateway-Server wird nicht unterstützt.

4. Wählen Sie aus den verfügbaren Optionen die Verwendung des NetScaler Gateways aus.
   + **Authentifizierung und HDX-Routing:** Das NetScaler Gateway wird für die Authentifizierung und das Routing von HDX-Sitzungen verwendet.
   + **Nur Authentifizierung:** Das NetScaler Gateway wird nur für die Authentifizierung, jedoch nicht für das HDX-Sitzungsrouting verwendet.
   + **Nur HDX-Routing**: Das NetScaler Gateway wird für das HDX-Routing, nicht aber für die Authentifizierung verwendet.
5. Wenn Sie Ressourcen von XenDesktop oder XenApp im Store verfügbar machen, listen Sie alle URLs der Seite "Secure Ticket Authority (STA)" für Server auf, auf denen die STA ausgeführt wird. Geben Sie aus Gründen der Fehlertoleranz URLs für mehrere STAs ein und führen Sie die Server dabei in der Reihenfolge ihrer Priorität auf, um die Failoversequenz festzulegen.

   Die STA wird auf XenDesktop- und XenApp-Servern gehostet und gibt Sitzungstickets als Reaktion auf Verbindungsanforderungen aus. Auf diesen Sitzungstickets basiert die Authentifizierung und Autorisierung für den Zugriff auf XenDesktop- und XenApp-Ressourcen.
6. Wählen Sie für die STA Load Balancing aus. Sie können auch ein Zeitintervall festlegen, nach dem STAs, die nicht antworten, umgangen werden.
7. Aktivieren Sie das Kontrollkästchen **Sitzungszuverlässigkeit aktivieren**, wenn XenDesktop und XenApp getrennte Sitzungen aufrechterhalten sollen, während Citrix Receiver eine automatische Wiederverbindung versucht. Aktivieren Sie das Kontrollkästchen **Tickets von zwei Secure Ticket Authoritys anfordern (falls verfügbar)**, wenn Sie mehrere STAs konfiguriert haben und sicherstellen möchten, dass Sitzungszuverlässigkeit immer gegeben ist. StoreFront ruft Tickets von zwei verschiedenen Secure Ticket Authoritys ab, damit Benutzersitzungen nicht unterbrochen werden, wenn eine Secure Ticket Authority während der Sitzung ausfällt. Wenn StoreFront aus irgendeinem Grund keine Verbindung zu zwei Secure Ticket Authoritys herstellen kann, wird automatisch nur eine Secure Ticket Authority verwendet.
8. Wählen Sie auf der Seite "Authentifizierungseinstellungen" die NetScaler Gateway-Version, die Sie konfigurieren möchten.
9. Geben Sie, falls erforderlich, die IP-Adresse des virtuellen Servers für das NetScaler Gateway-Gerät an. Die VServer-IP-Adresse wird von NetScaler Gateway für die Kommunikation mit Servern im internen Netzwerk zur Darstellung des Benutzergeräts verwendet. Dies kann es sich auch die zugeordnete IP-Adresse des NetScaler Gateway-Geräts sein. Wenn angegeben, verwendet StoreFront die VServer-IP-Adresse, um zu überprüfen, ob eingehende Anfragen von einem vertrauenswürdigen Gerät stammen.
10. Wählen Sie aus der Liste "Anmeldetyp" die Authentifizierungsmethode aus, die Sie auf dem Gerät für Benutzer von Citrix Receiver konfiguriert haben.Die von Ihnen angegebenen Informationen über die Konfiguration des NetScaler Gateway-Geräts wird der Provisioningdatei für den Store hinzugefügt. Dies ermöglicht, dass Citrix Receiver die entsprechende Verbindungsanforderung schickt, wenn das Gerät zum ersten Mal kontaktiert wird.

- Wenn Benutzer die Domänenanmeldeinformationen für Microsoft Active Directory eingeben müssen, wählen Sie "Domäne".
- Wählen Sie "Sicherheitstoken", wenn Benutzer einen Tokencode von einem Sicherheitstoken eingeben müssen.
- Wählen Sie "Domäne und Sicherheitstoken", wenn Benutzer ihre Domänenanmeldeinformationen und einen Tokencode von einem Sicherheitstoken eingeben müssen.
- Wählen Sie "SMS-Authentifizierung", wenn Benutzer ein in einer Textnachricht gesendetes Einmalkennwort eingeben müssen.
- Wenn Benutzer eine Smartcard vorlegen und eine PIN eingeben müssen, wählen Sie "Smartcard".

Wenn Sie die Smartcardauthentifizierung mit einer sekundären Authentifizierungsmethode konfigurieren, auf die Benutzer bei Problemen mit der Smartcard zurückgreifen können, wählen Sie die sekundäre Authentifizierungsmethode aus der Liste "Smartcard-Fallback".

11. Geben Sie die URL des NetScaler Gateway-Authentifizierungsdiensts in das Feld "Callback-URL" ein. Dies ist ein optionales Feld. StoreFront fügt automatisch den Standardteil der URL an. Geben Sie die intern zugängliche URL des Geräts ein. StoreFront kontaktiert den NetScaler Gateway-Authentifizierungsdienst, um zu überprüfen, ob von NetScaler Gateway empfangene Anforderungen auch tatsächlich von diesem Gerät ausgehen.
12. Klicken Sie auf "Erstellen", um die NetScaler Gateway-Bereitstellung der Liste auf der Seite "Remotezugriff" hinzuzufügen.Wiederholen Sie erforderlichenfalls die Schritte 1 bis 11 zum Hinzufügen weiterer NetScaler Gateway-Bereitstellungen zur Liste "NetScaler Gateway-Geräte". Wenn Sie Zugriff über mehrere Bereitstellungen aktivieren, indem Sie mehr als einen Eintrag in der Liste auswählen, geben Sie die Standardbereitstellung für den Zugriff auf den Store an.
13. Klicken Sie auf der Seite "Remotezugriff" auf "Erstellen". Nach dem Erstellen des Stores klicken Sie auf "Fertig stellen".

Der Store steht jetzt für den Zugriff durch Benutzer über Citrix Receiver zur Verfügung. Citrix Receiver muss mit den Zugriffsinformationen für den Store konfiguriert werden. Es gibt eine Reihe von Methoden der Bekanntgabe dieser Informationen an die Benutzer, sodass Sie diesen die Konfiguration erleichtern können. Weitere Informationen finden Sie unter Benutzerzugriffsoptionen.

Alternativ können Benutzer auf den Store über Receiver für Web-Site zugreifen und somit über eine Webseite auf ihre Desktops und Anwendungen zugreifen. Die URL, über die Benutzer auf die Receiver für Web-Site für den Store zugreifen, wird angezeigt, wenn Sie den Store erstellen.

Wenn Sie einen neuen Store erstellen, wird die XenApp Services-URL standardmäßig aktiviert. Benutzer domänengebundener Desktopgeräte und umfunktionierter PCs, auf denen Citrix Desktop Lock ausgeführt wird, sowie Benutzer mit älteren Citrix Clients, die nicht aktualisiert werden können, können über die XenApp-Services-URL direkt auf Stores zugreifen. Die XenApp Services-URL für den Store hat das Format "http[s]://serveraddress/Citrix/storename/PNAgent/config.xml", wobei "serveraddress" der vollqualifizierte Domänenname des Servers oder der Lastausgleichsumgebung für die StoreFront-Bereitstellung ist und "storename" der für den Store in Schritt 3 angegebene Name.

Erstellen Sie einen Store für Einzelserverbereitstellungen auf einem Server, der nicht in einer Domäne ist

1. Klicken Sie auf derWindows-Startseite oder auf der Seite **Apps** auf die Kachel **Citrix StoreFront**.
2. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores** aus und klicken Sie im Bereich **Aktionen** auf **Store erstellen**.
3. Geben Sie auf der Seite **Storename** einen Namen für den Store an und klicken Sie auf **Weiter**.
   Storenamen erscheinen in Citrix Receiver unter den Konten der Benutzer. Wählen Sie daher einen Namen, anhand dessen Benutzer den Inhalt des Stores erkennen können.

4. Listen Sie auf der Seite **Delivery Controller** die Infrastruktur und die Ressourcen auf, die Sie im Store zur Verfügung stellen möchten. Klicken Sie auf **Hinzufügen**.
5. Geben Sie im Dialogfeld **Delivery Controller hinzufügen** einen Namen an, über den Sie die Bereitstellung identifizieren können, und geben Sie an, ob die Ressourcen, die Sie über den Store verfügbar machen möchten, von XenDesktop, XenApp, oder XenMobile AppController bereitgestellt werden. Für App Controller-Bereitstellungen stellen Sie sicher, dass der Name keine Leerzeichen enthält.
6. Wenn Sie Details für XenDesktop- oder XenApp-Server hinzufügen, fahren Sie mit Schritt 7 fort. Geben Sie den Namen oder die IP-Adresse eines virtuellen App Controller-Geräts im Feld Server ein und geben Sie den Port an, der von StoreFront für Verbindungen mit App Controller verwendet werden soll, um von App Controller verwaltete Anwendungen im Store verfügbar zu machen. Der Standardport ist 443. Fahren Sie mit Schritt 11 fort.
7. Um Desktops und Anwendungen, die von XenDesktop oder XenApp bereitgestellt werden, im Store verfügbar zu machen, fügen Sie die Namen oder IP-Adressen der Server der Liste **Server** hinzu. Geben Sie für XenDesktop-Sites die Details der Delivery Controller an. Listen Sie für XenApp-Farmen Server auf, auf denen der Citrix XML-Dienst ausgeführt wird.
8. Wählen Sie aus der Liste **Transporttyp** die Verbindungstypen für StoreFront aus, die für die Kommunikation mit den Servern verwendet werden sollen.
   - Wählen Sie HTTP aus, wenn Daten über unverschlüsselte Verbindungen gesendet werden sollen. Bei Auswahl dieser Option müssen Sie eigene Maßnahmen treffen, um die Verbindungen zwischen StoreFront und dem Server zu sichern.
   - Wählen Sie HTTPS aus, um Daten über sichere HTTP-Verbindungen mit SSL (Secure Sockets Layer) oder TLS (Transport Layer Security) zu senden. Wenn Sie diese Option für XenDesktop- oder XenApp-Server auswählen, vergewissern Sie sich, dass der Citrix XML-Dienst so konfiguriert ist, dass der Port gemeinsam mit Internetinformationsdienste (IIS) verwendet wird und in der IIS-Konfiguration HTTPS-Unterstützung festgelegt wurde.
   - Wählen Sie SSL-Relay aus, um Daten über sichere Verbindungen an XenApp-Server zu senden. SSL-Relay übernimmt die Hostauthentifizierung und Datenverschlüsselung.

     Hinweis: Wenn Sie die Verbindungen zwischen StoreFront und den Servern mit HTTPS oder SSL-Relay sichern, achten Sie darauf, dass der in der Liste **Server** angegebene Name genau mit den Namen in den Zertifikaten für die Server übereinstimmt. Dies gilt auch für die Groß- und Kleinschreibung.

9. Geben Sie den Port an, den StoreFront für Verbindungen mit dem Server verwenden soll. Der Standardport ist 80 für Verbindungen über HTTP und SSL-Relay bzw. 443 für HTTPS-Verbindungen. Bei XenDesktop- und XenApp-Servern muss der angegebene Port dem vom Citrix XML-Dienst verwendeten Port entsprechen.
10. Wenn Sie SSL-Relay verwenden, um Verbindungen zwischen StoreFront und dem XenApp-Server zu sichern, geben Sie den TCP-Port für SSL-Relay im Feld "SSL-Relay-Port" an. Der Standardport ist 443. Stellen Sie sicher, dass alle Server, auf denen SSL-Relay ausgeführt wird, denselben Port überwachen.
11. Klicken Sie auf **OK**. Sie können Stores konfigurieren, die Ressourcen aus einer beliebigen Zusammenstellung von XenDesktop-, XenApp- und App Controller-Bereitstellungen bieten. Wiederholen Sie erforderlichenfalls die Schritte 4 bis 11, um weitere Bereitstellungen von Ressourcen für den Store aufzulisten. Wenn Sie alle erforderlichen Ressourcen hinzugefügt haben, klicken Sie auf "Weiter".
12. Geben Sie auf der Seite **Remotezugriff** an, ob und wie Benutzer, die eine Verbindung aus öffentlichen Netzwerken herstellen, über NetScaler Gateway auf den Store zugreifen können.
   - Wählen Sie **Kein** aus, wenn der Store nicht für Benutzer in öffentlichen Netzwerken verfügbar sein soll. Nur lokale Benutzer im internen Netzwerk können dann auf den Store zugreifen.
   - Wenn Sie nur Ressourcen, die über den Store angeboten werden, über NetScaler Gateway verfügbar machen möchten, wählen Sie **Kein VPN-Tunnel** aus. Benutzer melden sich direkt bei NetScaler Gateway an und müssen das NetScaler Gateway-Plug-In nicht verwenden.

- Wählen Sie **Vollständiger VPN-Tunnel** aus, um den Store und alle andere Ressourcen im internen Netzwerk über einen SSL-VPN-Tunnel (VPN = virtuelles privates Netzwerk) verfügbar zu machen. Benutzer benötigen das NetScaler Gateway-Plug-In für das Erstellen des VPN-Tunnels.

  Falls noch nicht geschehen, wird automatisch die Passthrough-Authentifizierung von NetScaler Gateway aktiviert, wenn Sie Remotezugriff auf den Store konfigurieren. Benutzer authentifizieren sich bei NetScaler Gateway und werden beim Zugriff auf ihre Stores automatisch angemeldet.

13. Wenn Sie Remotezugriff aktiviert haben, fahren Sie mit Konfigurieren des Remotezugriffs auf den Store über NetScaler Gateway fort, um die NetScaler Gateway-Bereitstellungen anzugeben, über die Benutzer auf den Store zugreifen können. Andernfalls klicken Sie auf der Seite **Remotezugriff** auf **Weiter**.
14. Wählen Sie auf der Seite **Authentifizierungsmethoden konfigurieren** die Methoden, die Benutzer zum Authentifizieren und Zugreifen auf Ressourcen verwenden, und klicken Sie auf **Weiter**.
15. Wählen Sie auf der Seite **Kennwortvalidierung konfigurieren** die Delivery Controller, die die Kennwortvalidierung bereitstellen, und klicken Sie auf **Weiter**.
16. Konfigurieren Sie auf der Seite **XenApp Services-URL** die URL für Benutzer, die PNAgent für den Zugriff auf Anwendungen und Desktops verwenden und klicken Sie auf **Erstellen**.

Servergruppenknoten links und die Bereiche **Aktion** werden durch **Basis-URL ändern** ersetzt. Nur die Option, die Basis-URL zu ändern, ist zugänglich. Servergruppen stehen für Server, die nicht in einer Domäne sind, nicht zur Verfügung.

Store entfernen

Mit der Aufgabe "Store entfernen" können Sie einen Store löschen. Wenn Sie einen Store zu entfernen, werden alle diesem zugeordneten Receiver für Web-Sites, Desktopgerätesites und XenApp Services-URLs ebenfalls gelöscht.

Wichtig: Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird.Wenn Sie die Änderungen vorgenommen haben, übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden.

Erstellen eines Stores ohne Authentifizierung

Nov 27, 2017

Verwenden Sie Store erstellen, um weitere Stores ohne Authentifizierung zu konfigurieren und so den Zugriff für nicht authentifizierte Benutzer zu unterstützen. Sie können beliebig viele Stores ohne Authentifizierung erstellen. Beispielsweise kann es empfehlenswert sein, einen Store ohne Authentifizierung für eine bestimmte Benutzergruppe zu erstellen oder bestimmte Ressourcen zusammenzufassen.

Remotezugriff über NetScaler Gateway ist nicht für Stores ohne Authentifizierung möglich.

Zum Erstellen eines Stores ohne Authentifizierung identifizieren und konfigurieren Sie die Kommunikation mit den Servern, auf denen die Ressourcen, die Sie im Store zur Verfügung stellen möchten, bereitgestellt werden.

Wichtig: Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Wenn Sie die Änderungen vorgenommen haben, übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden.

1. Klicken Sie auf der Windows-Startseite oder auf der Apps-Seite auf die Kachel Citrix StoreFront.
2. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten Stores und klicken Sie im Bereich Aktionen auf Store erstellen.
3. Geben Sie auf der Seite Storename einen Namen für den Store ein, klicken Sie auf **Nur nicht authentifizierte (anonyme) Benutzer dürfen auf diesen Store zugreifen** und klicken Sie auf Weiter.
   Storenamen erscheinen in Citrix Receiver unter den Konten der Benutzer. Wählen Sie daher einen Namen, anhand dessen Benutzer den Inhalt des Stores erkennen können.
4. Listen Sie auf der Seite **Delivery Controller** die Infrastruktur und die Ressourcen auf, die Sie im Store zur Verfügung stellen möchten. Klicken Sie auf Hinzufügen.
5. Geben Sie im Dialogfeld Controller hinzufügen einen Namen an, über den Sie die Bereitstellung identifizieren können, und geben Sie an, ob die Ressourcen, die Sie über den Store verfügbar machen möchten, von XenApp oder XenMobile (AppController) bereitgestellt werden. Bei XenMobile(App Controller)-Bereitstellungen stellen Sie sicher, dass der Name keine Leerzeichen enthält. Stellen Sie beim Zuweisen von Controllern sicher, dass Sie nur die verwenden, die anonyme Apps unterstützen. Wenn Sie für den Store ohne Authentifizierung Controller konfigurieren, die dieses Feature nicht unterstützen, können möglicherweise keine anonymen Apps im Store verfügbar gemacht werden.
6. Wenn Sie Details für XenApp-Server hinzufügen, fahren Sie mit Schritt 7 fort. Geben Sie den Namen oder die IP-Adresse eines virtuellen XenMobile(App Controller)-Geräts im Feld Server ein und geben Sie den Port an, der von StoreFront für Verbindungen mit XenMobile (App Controller) verwendet werden soll, um von XenMobile (App Controller) verwaltete Anwendungen im Store verfügbar zu machen. Der Standardport ist 443. Fahren Sie mit Schritt 10 fort.
7. Um Desktops und Anwendungen, die von XenApp bereitgestellt werden, im Store verfügbar zu machen, fügen Sie die Namen oder IP-Adressen der Server der Liste Server hinzu. Geben Sie aus Gründen der Fehlertoleranz mehrere Server an und führen Sie die Server dabei in der Reihenfolge ihrer Priorität auf, um die Failover-Reihenfolge festzulegen. Geben Sie für XenDesktop-Sites die Details der Controller an. Listen Sie für XenApp-Farmen Server auf, auf denen der Citrix XML-Dienst ausgeführt wird.
8. Wählen Sie aus der Liste Transporttyp die Verbindungstypen für StoreFront aus, die für die Kommunikation mit den Servern verwendet werden sollen.
   - Wählen Sie HTTP aus, wenn Daten über unverschlüsselte Verbindungen gesendet werden sollen. Bei Auswahl dieser Option müssen Sie eigene Maßnahmen treffen, um die Verbindungen zwischen StoreFront und den Servern zu sichern.

- Wählen Sie HTTPS aus, um Daten über sichere HTTP-Verbindungen mit SSL (Secure Sockets Layer) oder TLS (Transport Layer Security) zu senden. Wenn Sie diese Option für XenDesktop- oder XenApp-Server auswählen, vergewissern Sie sich, dass der Citrix XML-Dienst so konfiguriert ist, dass der Port gemeinsam mit Internetinformationsdienste (IIS) verwendet wird und in der IIS-Konfiguration HTTPS-Unterstützung festgelegt wurde.

Hinweis: Wenn Sie die Verbindungen zwischen StoreFront und den Servern mit HTTPS sichern, achten Sie darauf, dass die in der Liste Server eingegebenen Servernamen genau mit den Namen in den Zertifikaten für die Server übereinstimmen. Die Groß- und Kleinschreibung wird berücksichtigt.

9. Geben Sie den Port an, den StoreFront für Verbindungen mit den Servern verwenden soll. Der Standardport ist 80 für Verbindungen mit HTTP und 443 für HTTPS-Verbindungen. Bei XenDesktop- und XenApp-Servern muss der angegebene Port dem vom Citrix XML-Dienst verwendeten Port entsprechen.
10. Klicken Sie auf OK. Sie können Stores konfigurieren, die Ressourcen aus einer beliebigen Zusammenstellung von XenDesktop-, XenApp- und App Controller-Bereitstellungen bieten. Wiederholen Sie erforderlichenfalls die Schritte 4 bis 10, um weitere Bereitstellungen von Ressourcen für den Store aufzulisten. Wenn Sie dem Store alle erforderlichen Ressourcen hinzugefügt haben, klicken Sie auf Erstellen.

Der Store ohne Authentifizierung ist nun bereit zum Verwenden. Damit Benutzer auf den neuen Store zugreifen können, muss Citrix Receiver mit den Zugriffsdetails für den Store konfiguriert sein. Es gibt eine Reihe von Methoden der Bekanntgabe dieser Informationen an die Benutzer, sodass Sie diesen die Konfiguration erleichtern können. Weitere Informationen finden Sie unter Benutzerzugriffsoptionen.
Alternativ können Benutzer auf den Store über Receiver für Web-Site zugreifen und somit über eine Webseite auf ihre Desktops und Anwendungen zugreifen. Standardmäßigwerden für Stores ohne Authentifizierung in Receiver für Web die Anwendungen in einer Ordnerhierarchie einschließlich einer Breadcrumbspur angezeigt. Die URL, über die Benutzer auf die Receiver für Web-Site für den Store zugreifen, wird angezeigt, wenn Sie den Store erstellen.

Wenn Sie einen neuen Store erstellen, wird die XenApp Services-URL standardmäßig aktiviert. Benutzer domänengebundener Desktopgeräte und umfunktionierter PCs, auf denen Citrix Desktop Lock ausgeführt wird, sowie Benutzer mit älteren Citrix Clients, die nicht aktualisiert werden können, können über die XenApp-Services-URL direkt auf Stores zugreifen. Die XenApp Services-URL hat das Format http[s]://serveraddress/Citrix/storename/PNAgent/config.xml, wobei serveraddress der vollqualifizierte Domänenname des Servers oder der Lastausgleichsumgebung für die StoreFront-Bereitstellung ist und storename der Name, den Sie in Schritt 3 angegeben haben.

Hinweis: In StoreFront-Konfigurationen, in denen die Datei web.config mit dem Parameter LogoffAction=”terminate" konfiguriert wurde, werden Citrix Receiver für Web-Sitzungen, die auf diesen Store ohne Authentifizierung zugreifen, nicht beendet. Die Datei web.config ist normalerweise im Verzeichnis C:\inetpub\wwwroot\Citrix\storename\, wobei storename der Name des Stores ist, der bei der Erstellung festgelegt wurde. Damit diese Sitzungen richtig beendet werden, muss auf dem von diesem Store verwendeten XenApp-Server die Option "XML-Anforderungen vertrauen" aktiviert sein, wie in der Dokumentation zu XenDesktop und XenApp unter *Konfigurieren von Port und Vertrauensbeziehung für den Citrix XML-Dienst* beschrieben.

Exportieren von Store-Provisioningdateien für Benutzer

Nov 27, 2017

Mit den Aufgaben Multistore-Provisioningdatei exportieren und Provisioningdatei exportieren können Sie Dateien mit Verbindungsinformationen für Stores generieren, z. B. für NetScaler Gateway-Bereitstellungen und Beacons, die für Stores konfiguriert wurden. Stellen Sie diese Dateien Benutzern zur Verfügung, damit diese Citrix Receiver automatisch mit den Details der Stores konfigurieren können. Benutzer können auch Citrix Receiver-Provisioningdateien von Receiver für Web-Sites erhalten.

Wichtig: Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Wenn Sie die Änderungen vorgenommen haben, übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden.

1. Klicken Sie auf der Windows-Startseite oder auf der Seite Apps auf die Kachel Citrix StoreFront. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten Stores aus.
2. Um eine Provisioningdatei mit Details für mehrere Stores zu generieren, klicken Sie im Bereich Aktionen auf Multistore-Provisioningdatei exportieren und wählen Sie die Stores aus, die der Datei hinzugefügt werden sollen.
3. Klicken Sie auf Exportieren und speichern Sie die Provisioningdatei mit der Erweiterung ".cr" an einem geeigneten Speicherort im Netzwerk.

Ankündigen und Ausblenden von Stores für Benutzer

Nov 27, 2017

Mit der Aufgabe Store ausblenden können Sie verhindern, dass Stores den Benutzern zum Hinzufügen zu ihrem Konto angezeigt werden, wenn diese Citrix Receiver über die e-mail-basierte Kontenermittlung oder den vollqualifizierten Domänennamen (FQDN) konfigurieren. Wenn Benutzer die StoreFront-Bereitstellung, die einen Store hostet, ermitteln, werden erstellte Stores standardmäßig als Option zum Hinzufügen in Citrix Receiver angezeigt. Wenn Sie einen Store ausblenden, wird dieser dadurch nicht unzugänglich, doch Benutzer müssen Citrix Receiver mit den Verbindungsinformationen für den Store konfigurieren, und zwar entweder manuell mit einer Setup-URL oder mit einer Provisioningdatei. Soll ein ausgeblendeter Store wieder angezeigt werden, verwenden Sie die Aufgabe Store anbieten.

Wichtig: Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Wenn Sie die Änderungen vorgenommen haben, übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden.

1. Klicken Sie auf derWindows-Startseite oder auf der Seite **Apps** auf die Kachel **Citrix StoreFront**.
2. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores** und klicken Sie im Bereich **Aktionen** auf **Storeeinstellungen konfigurieren > Store ankündigen**.
3. Wählen Sie auf der Seite **Store ankündigen** die Option **Store ankündigen** oder **Store ausblenden** aus.

Verwalten der durch Stores zur Verfügung gestellten Ressourcen

Nov 27, 2017

Mit der Aufgabe Delivery Controller verwalten können Sie Ressourcen, die durch XenDesktop, XenApp und App Controller bereitgestellt werden, zu Stores hinzufügen bzw. daraus entfernen und die Informationen zu den Servern ändern, mit denen die Ressourcen bereitgestellt werden.

Wichtig: Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Wenn Sie die Änderungen vorgenommen haben, übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden.

1. Klicken Sie auf der Windows-Startseite oder auf der Apps-Seite auf die Kachel Citrix StoreFront.
2. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten Stores und im Ergebnisbereich einen Store aus. Klicken Sie im Bereich Aktionen auf Delivery Controller verwalten.
3. Klicken Sie im Dialogfeld Delivery Controller verwalten auf Hinzufügen, um die Desktops und Anwendungen von einer anderen XenDesktop-, XenApp- oder App Controller-Bereitstellung in den Store einzuschließen. Wenn Sie die Einstellungen für eine Bereitstellung ändern möchten, wählen Sie den Eintrag in der Liste Delivery Controller und klicken Sie auf Bearbeiten. Wählen Sie einen Eintrag in der Liste aus und klicken Sie auf Entfernen, um die Verfügbarkeit der Ressourcen der Bereitstellung im Store zu beenden.
4. Geben Sie im Dialogfeld Controller hinzufügen oder Controller bearbeiten einen Namen ein, über den Sie die Bereitstellung identifizieren können, und geben Sie an, ob die Ressourcen, die Sie im Store verfügbar machen möchten, von XenDesktop, XenApp oder AppController bereitgestellt werden. Für App Controller-Bereitstellungen stellen Sie sicher, dass der Name keine Leerzeichen enthält.
5. Wenn Sie Details für XenDesktop- oder XenApp-Server hinzufügen, fahren Sie mit Schritt 6 fort. Geben Sie den Namen oder die IP-Adresse eines virtuellen App Controller-Geräts im Feld Server ein und geben Sie den Port an, der von StoreFront für Verbindungen mit App Controller verwendet werden soll, um von App Controller verwaltete Anwendungen im Store verfügbar zu machen. Der Standardport ist 443. Fahren Sie mit Schritt 10 fort.
6. Um Desktops und Anwendungen, die von XenDesktop oder XenApp bereitgestellt werden, im Store verfügbar zu machen, klicken Sie auf Hinzufügen, um den Namen oder die IP-Adresse eines Servers einzugeben. Abhängig von der Konfiguration der Datei web.config wird durch das Festlegen mehrerer Server entweder Load Balancing oder Failover aktiviert, wie im Dialogfeld angegeben. Load Balancing ist standardmäßig konfiguriert. Wenn Failover konfiguriert ist, führen Sie die Server in der Reihenfolge ihrer Priorität auf, um die Failover-Reihenfolge festzulegen. Geben Sie für XenDesktop-Sites die Details der Delivery Controller an. Listen Sie für XenApp-Farmen Server auf, auf denen der Citrix XML-Dienst ausgeführt wird. Um den Namen oder die IP-Adresse eines Servers zu ändern, wählen Sie den Eintrag in der Liste Server aus und klicken Sie auf Bearbeiten. Wählen Sie einen Eintrag in der Liste aus und klicken Sie auf Entfernen, damit StoreFront den Server nicht mehr kontaktiert, um die verfügbaren Ressourcen aufzulisten.
7. Wählen Sie aus der Liste Transporttyp die Verbindungstypen für StoreFront aus, die für die Kommunikation mit den Servern verwendet werden sollen.
   - Wählen Sie HTTP aus, wenn Daten über unverschlüsselte Verbindungen gesendet werden sollen. Bei Auswahl dieser Option müssen Sie eigene Maßnahmen treffen, um die Verbindungen zwischen StoreFront und den Servern zu sichern.
   - Wählen Sie HTTPS aus, um Daten über sichere HTTP-Verbindungen mit SSL (Secure Sockets Layer) oder TLS (Transport Layer Security) zu senden. Wenn Sie diese Option für XenDesktop- oder XenApp-Server auswählen, vergewissern Sie sich, dass der Citrix XML-Dienst so konfiguriert ist, dass der Port gemeinsam mit Internetinformationsdienste (IIS) verwendet wird und in der IIS-Konfiguration HTTPS-Unterstützung festgelegt

wurde.

- Wählen Sie SSL-Relay aus, um Daten über sichere Verbindungen an XenApp-Server zu senden. SSL-Relay übernimmt die Hostauthentifizierung und Datenverschlüsselung.

Hinweis: Wenn Sie die Verbindungen zwischen StoreFront und den Servern mit HTTPS oder SSL-Relay sichern, achten Sie darauf, dass die in der Liste Server eingegebenen Servernamen genau mit den Namen in den Zertifikaten für die Server übereinstimmen. Dies gilt auch für die Groß- und Kleinschreibung.

8. Geben Sie den Port an, den StoreFront für Verbindungen mit den Servern verwenden soll. Der Standardport ist 80 für Verbindungen über HTTP und SSL-Relay bzw. 443 für HTTPS-Verbindungen. Bei XenDesktop- und XenApp-Servern muss der angegebene Port dem vom Citrix XML-Dienst verwendeten Port entsprechen.
9. Wenn Sie SSL-Relay verwenden, um Verbindungen zwischen StoreFront und XenApp-Servern zu sichern, geben Sie den TCP-Port für SSL-Relay im Feld SSL-Relay-Port an. Der Standardport ist 443. Stellen Sie sicher, dass alle Server, auf denen SSL-Relay ausgeführt wird, denselben Port überwachen.
10. Klicken Sie auf OK. Sie können Stores konfigurieren, die Ressourcen aus einer beliebigen Zusammenstellung von XenDesktop-, XenApp- und App Controller-Bereitstellungen bieten. Wiederholen Sie erforderlichenfalls die Schritte 3 bis 10 zum Hinzufügen oder Ändern weiterer Bereitstellungen unter Delivery Controller.

Verwalten des Remotezugriffs auf Stores über NetScaler Gateway

Jun 04, 2018

Mit der Aufgabe Remotezugriffeinstellungen können Sie den Zugriff auf Stores über NetScaler Gateway für Benutzer in öffentlichen Netzwerken konfigurieren. Remotezugriff über NetScaler Gateway ist nicht für Stores ohne Authentifizierung möglich.

Wichtig: Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Wenn Sie die Änderungen vorgenommen haben, übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden.

1. Klicken Sie auf der Windows-Startseite oder auf der Apps-Seite auf die Kachel Citrix StoreFront.
2. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten Stores und im Ergebnisbereich einen Store aus. Klicken Sie im Bereich Aktionen auf **Remotezugriffeinstellungen** konfigurieren.
3. Geben Sie im Dialogfeld **Remotezugriffeinstellungen** konfigurieren an, ob und wie Benutzer, die eine Verbindung von öffentlichen Netzwerken aus herstellen, über NetScaler Gateway auf den Store zugreifen können.
   - Soll der Store Benutzern in öffentlichen Netzwerken nicht zur Verfügung stehen, stellen Sie sicher, dass die Option **Remotezugriff aktivieren** deaktiviert ist. Nur lokale Benutzer im internen Netzwerk können dann auf den Store zugreifen.
   - Um den Remotezugriff zu ermöglichen, aktivieren Sie **Remotezugriff aktivieren**.
     - Wenn Sie nur Ressourcen, die über den Store angeboten werden, über NetScaler Gateway verfügbar machen möchten, wählen Sie Kein VPN-Tunnel aus. Benutzer melden sich direkt bei NetScaler Gateway an und müssen das NetScaler Gateway-Plug-In nicht verwenden.
     - Wählen Sie Vollständiger VPN-Tunnel aus, um den Store und andere Ressourcen im internen Netzwerk über einen SSL-VPN-Tunnel (SSL = Secure Sockets Layer, VPN = virtuelles privates Netzwerk) verfügbar zu machen. Benutzer benötigen das NetScaler Gateway-Plug-In für das Erstellen des VPN-Tunnels.

   Falls noch nicht geschehen, wird automatisch die Passthrough-Authentifizierung von NetScaler Gateway aktiviert, wenn Sie Remotezugriff auf den Store konfigurieren. Benutzer authentifizieren sich bei NetScaler Gateway und werden beim Zugriff auf ihre Stores automatisch angemeldet.

4. Wenn Sie Remotezugriff aktiviert haben, wählen Sie in der Liste NetScaler Gateway-Geräte die Bereitstellungen aus, über die Benutzer auf den Store zugreifen können. Die Liste enthält alle Bereitstellungen, die zuvor für diesen und andere Stores konfiguriert wurden. Wenn Sie eine weitere Bereitstellung hinzufügen möchten, klicken Sie auf Hinzufügen. Fahren Sie andernfalls mit Schritt 16 fort.
5. Geben Sie auf der Seite Allgemeine Einstellungen einen Namen für die NetScaler Gateway-Bereitstellung an, über den die Benutzer sie erkennen können.
   Benutzern wird der Anzeigename angezeigt, den Sie in Citrix Receiver angegeben haben. Nehmen Sie deshalb relevante Informationen in den Namen auf, damit Benutzer leichter entscheiden können, ob sie die Bereitstellung verwenden möchten. Beispielsweise können Sie den geographischen Standort in die Anzeigenamen der NetScaler Gateway-Bereitstellungen einfügen, damit Benutzer problemlos das beste Gateway für ihren Standort identifizieren können.

6. Geben Sie die URL des virtuellen Servers oder Benutzeranmeldepunkts (für Access Gateway 5.0) für die Bereitstellung an. Geben Sie die Produktversion Ihrer Bereitstellung an.
   Der vollqualifizierte Domänenname (FQDN) für die StoreFront-Bereitstellung muss eindeutig sein und darf nicht dem

vollqualifizierten Domänennamen des virtuellen NetScaler Gateway-Servers entsprechen. Das Verwenden des selben vollqualifizierten Domänennamens für StoreFront und den virtuellen NetScaler Gateway-Server wird nicht unterstützt.

7. Wenn Sie eine Access Gateway 5.0-Bereitstellung hinzufügen, fahren Sie mit Schritt 9 fort. Andernfalls und geben Sie ggf. die Subnetz-IP-Adresse des NetScaler Gateway-Geräts an. Eine Subnetz IP-Adresse ist für Access Gateway 9.3-Geräte erforderlich, aber für neuere Produktversionen optional.
   Die Subnetzadresse ist die IP-Adresse, durch die NetScaler Gateway für die Kommunikation mit Servern im internen Netzwerk das Benutzergerät darstellt. Dies kann es sich auch die zugeordnete IP-Adresse des NetScaler Gateway-Geräts sein. Wenn angegeben, verwendet StoreFront die Subnetz-IP-Adresse, um zu überprüfen, ob eingehende Anfragen von einem vertrauenswürdigen Gerät stammen.

8. Wenn Sie ein Gerät mit NetScaler Gateway hinzufügen, wählen Sie aus der Liste Anmeldetyp die Authentifizierungsmethode aus, die Sie auf dem Gerät für Benutzer von Citrix Receiver konfiguriert haben.
   Die von Ihnen angegebenen Informationen über die Konfiguration des NetScaler Gateway-Geräts wird der Provisioningdatei für den Store hinzugefügt. Dies ermöglicht, dass Citrix Receiver die entsprechende Verbindungsanforderung schickt, wenn das Gerät zum ersten Mal kontaktiert wird.

   - Wenn Benutzer die Domänenanmeldeinformationen für Microsoft Active Directory eingeben müssen, wählen Sie Domäne.
   - WählenSie Sicherheitstoken, wenn Benutzer einen Tokencode von einem Sicherheitstoken eingeben müssen.
   - WählenSie Domäne und Sicherheitstoken aus, wenn Benutzer ihre Domänenanmeldeinformationen und einen Tokencode von einem Sicherheitstoken eingeben müssen.
   - Wählen Sie SMS-Authentifizierung, wenn Benutzer ein in einer Textnachricht gesendetes Einmalkennwort eingeben müssen.
   - Wenn Benutzer eine Smartcard vorlegen und eine PIN eingeben müssen, wählen Sie Smartcard.

   Wenn Sie die Smartcardauthentifizierung mit einer sekundären Authentifizierungsmethode konfigurieren, auf die Benutzer zurückgreifen können, wenn es Probleme mit den Smartcards gibt, wählen Sie die sekundäre Authentifizierungsmethode aus der Liste Smartcard-Fallback. Fahren Sie mit Schritt 10 fort.

9. Zum Hinzufügen einer Access Gateway 5.0-Bereitstellung geben Sie an, ob der Anmeldepunkt auf einem eigenständigen Gerät oder auf einem Access Controller-Server, der Teil eines Clusters ist, gehostet wird. Wenn Sie ein Cluster hinzufügen, klicken Sie auf Weiter und fahren Sie mit Schritt 11 fort.
10. Wenn Sie StoreFront für NetScaler Gateway oder ein einzelnes Access Gateway 5.0-Gerät konfigurieren, geben Sie in das Feld Callback-URL die URL des NetScaler Gateway-Authentifizierungsdiensts ein. StoreFront fügt automatisch den Standardteil der URL an. Klicken Sie auf Weiter und gehen Sie zu Schritt 13.
    Geben Sie die intern zugängliche URL des Geräts ein. StoreFront kontaktiert den NetScaler Gateway-Authentifizierungsdienst, um zu überprüfen, ob von NetScaler Gateway empfangene Anforderungen auch tatsächlich von diesem Gerät ausgehen.

11. Zum Konfigurieren von StoreFront für ein Access Gateway 5.0-Cluster listen Sie auf der Seite Geräte die IP-Adressen oder vollqualifizierten Domänennamen der Geräte im Cluster auf und klicken Sie auf Weiter.
12. Listen Sie auf der Seite Authentifizierung ohne Benutzereingriff aktivieren die URLs für den Authentifizierungsdienst, der auf den Access Controller-Servern ausgeführt wird, auf. Geben zur Aktivierung der Fehlertoleranz URLs mehrerer Server ein und führen Sie die Server dabei in der Reihenfolge ihrer Priorität auf, um die Failoversequenz festzulegen. Klicken Sie auf Weiter.
    StoreFront authentifiziert Remotebenutzer über den Authentifizierungsdienst, damit sie ihre Anmeldeinformationen nicht neu eingeben müssen, wenn sie auf Stores zugreifen.

13. Alle Bereitstellungen: Wenn Sie Ressourcen von XenDesktop oder XenApp im Store verfügbar machen, listen Sie auf der Seite Secure Ticket Authority (STA) URLs für Server auf, auf denen die STA ausgeführt wird. Geben Sie aus Gründen der Fehlertoleranz URLs für mehrere STAs ein und führen Sie die Server dabei in der Reihenfolge ihrer Priorität auf, um die Failoversequenz festzulegen.
    Die STA wird auf XenDesktop- und XenApp-Servern gehostet und gibt Sitzungstickets als Reaktion auf Verbindungsanforderungen aus. Auf diesen Sitzungstickets basiert die Authentifizierung und Autorisierung für den Zugriff auf XenDesktop- und XenApp-Ressourcen.

14. Aktivieren Sie das Kontrollkästchen Sitzungszuverlässigkeit aktivieren, wenn XenDesktop und XenApp getrennte Sitzungen aufrechterhalten sollen, während Citrix Receiver eine automatische Wiederverbindung versucht. Aktivieren Sie das Kontrollkästchen Tickets von zwei Secure Ticket Authoritys anfordern (falls verfügbar), wenn Sie mehrere STAs konfiguriert haben und sicherstellen möchten, dass Sitzungszuverlässigkeit immer gegeben ist.
    Wenn das Kontrollkästchen Tickets von zwei Secure Ticket Authoritys anfordern (falls verfügbar) aktiviert ist, ruft StoreFront Tickets von zwei verschiedenen Secure Ticket Authoritys ab, damit Benutzersitzungen nicht unterbrochen werden, wenn eine Secure Ticket Authority während der Sitzung ausfällt. Wenn StoreFront aus irgendeinem Grund keine Verbindung zu zwei Secure Ticket Authoritys herstellen kann, wird automatisch nur eine Secure Ticket Authority verwendet.

15. Klicken Sie auf Erstellen, um die NetScaler Gateway-Bereitstellung der Liste im Dialogfeld Remotezugriffeinstellungen hinzuzufügen.
16. Wiederholen Sie erforderlichenfalls die Schritte 4 bis 15 zum Hinzufügen weiterer NetScaler Gateway-Bereitstellungen zur Liste NetScaler Gateway-Geräte. Wenn Sie Zugriff über mehrere Bereitstellungen aktivieren, indem Sie mehr als einen Eintrag in der Liste auswählen, geben Sie die Standardbereitstellung für den Zugriff auf den Store an.

Integrieren von Citrix Online-Anwendungen in Stores

Nov 27, 2017

Hinweis

Ab StoreFront 3.12 kann dieses Feature nicht in der StoreFront-Verwaltungskonsole konfiguriert werden. Bei einem Upgrade auf StoreFront 3.12 können Sie dieses Feature weiterhin verwenden. Verwenden Sie das PowerShell-Cmdlet "Update DSGenericApplications", um Ihre Konfiguration anzupassen.

Informationen zum Konfigurieren dieses Features in der StoreFront-Verwaltungskonsole in früheren Versionen finden Sie im Artikel Citrix Online-Integration für StoreFront 3.11.

NAME
Update-DSGenericApplications

SYNOPSE
Aktualisieren der generischen Anwendungseinstellungen für einen Storedienst.

SYNTAX

Update-DSGenericApplications [[-StoreServiceSiteId]] [[-StoreServiceVirtualPath]] [[-GoToMeetingEnabled]] [[-GoToMeetingDeliveryOption]] [[-GoToWebinarEnabled]] [[-GoToWebinarDeliveryOption]] [[-GoToTrainingEnabled]] [[-GoToTrainingDeliveryOption]] []

DESCRIPTION

Cmdlet zum Aktualisieren der generischen (Citrix Online)-Funktionalität des Storedienstes.

Konfigurieren zweier StoreFront-Stores zur gemeinsamen Nutzung eines Abonnementdatenspeichers

Nov 27, 2017

Ab Version 2.0 wird in StoreFront keine SQL-Datenbank zur Pflege der Abonnementdaten mehr verwendet. Statt der SQL-Datenbank wird ein Windows-Datenspeicher verwendet, der bei der ersten Installation von StoreFront keine zusätzliche Konfiguration erfordert. Im Rahmen der Installation wird der Windows-Datenspeicher lokal auf jedem StoreFront-Server installiert. In Umgebungen mit StoreFront-Servergruppen hat jeder Server zudem eine Kopie der Abonnementdaten des Stores. Diese Daten werden an andere Servern verteilt, damit Benutzerabonnements gruppenweit gepflegt werden. Standardmäßig wird ein Datenspeicher für jeden Store erstellt. Jeder Abonnementdatenspeicher wird separat aktualisiert.

Wenn unterschiedliche Konfigurationseinstellungen erforderlich sind, konfigurieren Administratoren StoreFront häufig mit zwei separaten Stores: einem für den externen Zugriff auf Ressourcen über NetScaler Gateway und einem für den internen Zugriff über das Unternehmens-LAN. Sie können den externen und den internen Store so konfigurieren, dass beide einen Abonnementdatenspeicher gemeinsam nutzen, indem Sie eine einfache Änderung an der Datei web.config des Stores vornehmen.

Im Standardszenario mit zwei Stores und jeweils eigenem Abonnementdatenspeicher müssen Benutzer die gleiche Ressource zweimal abonnieren. Das Konfigurieren der beiden Stores zur gemeinsamen Nutzung eines Abonnementdatenspeichers verbessert und vereinfacht die Roamingerfahrung beim Zugriff auf die gleiche Ressource von innerhalb und außerhalb des Unternehmensnetzwerks. Bei einem gemeinsam genutzten Abonnementdatenspeicher ist es egal, ob der Benutzer beim ersten Abonnement einer neuen Ressource extern oder intern auf sie zugreift.

- Jeder Store hat eine web.config-Datei in C:\inetpub\wwwroot\citrix\<storename>.
- Jede web.config-Datei hat einen Clientendpunkt für den Abonnementstoredienst.

StoreName>" authenticationMode="windows" transferMode="Streamed">

Die Abonnementdaten für jeden Store sind in:

C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\SubscriptionsStore\1__Citrix_<StoreName>
Damit zwei Stores einen Abonnementdatenspeicher verwenden, müssen Sie nur einen Store auf den Abonnementdienst-Endpunkt des anderen Speichers verweisen. Bei einer Servergruppenbereitstellung sind für alle Server identische Storepaare und identische Kopien von deren gemeinsam genutzten Datenspeichern definiert.

Hinweis: Die für die einzelnen Stores konfigurierten XenApp-, XenDesktop- und AppC-Controller müssen genau übereinstimmen, da ansonsten u. U. ein inkonsistenter Satz Ressourcenabonnements zwischen Stores auftritt. Die gemeinsame Datenspeichernutzung wird nur unterstützt, wenn die beiden Stores auf demselben StoreFront-Server bzw. in derselben Servergruppenbereitstellung residieren.
Endpunkte der StoreFront-Abonnementdatenspeicher

1. Öffnen Sie bei einer einzelnen StoreFront-Bereitstellung die externe Store-web.config-Datei in Editor und suchen Sie "clientEndpoint". Beispiel:

   External" authenticationMode="windows" transferMode="Streamed">

2. Ändern Sie den externen Store-Endpunkt, sodass er dem internen entspricht:
   Internal" authenticationMode="windows" transferMode="Streamed">

3. Wenn Sie eine StoreFront-Servergruppe verwenden, übertragen Sie die an der Datei web.config des primären Knotens vorgenommenen Änderungen auf alle anderen Knoten.

Beide Stores verwenden nun den internen Abonnementdatenspeicher gemeinsam.

Erweiterte Storeeinstellungen

Nov 27, 2017

Sie können erweiterte Storeeigenschaften über "Erweiterte Einstellungen" auf der Seite "Storeeinstellungen konfigurieren" festlegen.

Adressauflösungstyp

Schriftartenglättung zulassen

Sitzungswiederverbindung zulassen

Umleitung spezieller Ordner zulassen

Intervall für Hintergrundsystemdiagnose

Kommunikationstimeoutdauer

Verbindungstimeout

Erweiterte Enumeration aktivieren

Socketpooling aktivieren

Ressourcen nach Ausschlussschlüsselwörtern filtern

Ressourcen nach Einschlussschlüsselwörtern filtern

Ressourcen nach Typ filtern

Maximum gleichzeitiger Enumerationen

Minimum Farmen für gleichzeitige Enumeration

ICA-Clientnamen überschreiben

Tokenkonsistenz erforderlich

Serverkommunikationsversuche

Desktop Viewer für Legacyclients anzeigen

Important

Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Wenn Sie die Änderungen vorgenommen haben, übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden.

1. Klicken Sie auf der Windows-Startseite oder auf der Apps-Seite auf die Kachel Citrix StoreFront.
2. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten Stores und im mittleren Bereich den Store aus und wählen Sie dann im Aktionsbereich **Storeeinstellungen konfigurieren** aus.
3. Wählen Sie auf der Seite **Storeeinstellungen konfigurieren** die Option **Erweiterte Einstellungen**, wählen Sie die erweiterte Einstellung, nehmen Sie die gewünschten Änderungen vor und klicken Sie auf **OK**.

Über **Erweiterte Einstellungen** können Sie festlegen, welche Adressart vom Server angefordert werden soll. Der Standardwert ist "DnsPort". Wählen Sie im Dropdownmenü **Adressauflösungstyp** auf der Seite **Erweiterte Einstellungen** eine der folgenden Optionen:

- Dns
- DnsPort
- IPV4
- IPV4Port
- Dot
- DotPort
- Uri
- NoChange

Sie können festlegen, ob bei HDX-Sitzungen die Schriftglättung verwendet werden soll. Die Standardeinstellung ist "Ein".

Aktivieren Sie über die Aufgabe **Erweiterte Einstellungen** das Kontrollkästchen **Schriftglättung zulassen** und klicken Sie auf **OK**.

Sie können festlegen, ob HDX-Sitzungen wiederverbunden werden sollen. Die Standardeinstellung ist "Ein".

Aktivieren Sie über die Aufgabe **Erweiterte Einstellungen** das Kontrollkästchen **Sitzungswiederverbindung zulassen** und klicken Sie auf **OK**.

Verwenden Sie die Aufgabe **Erweiterte Einstellungen** zum Aktivieren oder Deaktivieren der Umleitung spezieller Ordner.Wenn die Umleitung spezieller Ordner konfiguriert ist, können Benutzer spezielle Windows-Ordner auf dem Server den Ordnern auf ihrem lokalen Computer zuordnen. Unter speziellen Ordner versteht man Windows-Standardordner, z. B. \Dokumente oder \Desktop, die unabhängig vom Betriebssystem immer gleich angezeigt werden.

Aktivieren oder deaktivieren Sie über die Aufgabe **Erweiterte Einstellungen** das Kontrollkästchen **Umleitung spezieller Ordner zulassen** und klicken Sie auf **OK**.

StoreFront führt regelmäßig Systemdiagnosen an jedem XenDesktop-Broker und XenApp-Server durch, um Probleme durch zeitweilige Serverausfälle zu vermindern. Die Standardeinstellung ist jede Minute (00:01:00). Geben Sie über "Erweiterte Einstellungen" eine Zeit für **Abfragezeit für Systemdiagnose im Hintergrund** ein und klicken Sie auf **OK**, um die Häufigkeit der Diagnosen zu steuern.

Standardmäßig ist das Timeout für Anforderungen von StoreFront an den Server, der die Ressourcen für einen Store bereitstellt, 30 Sekunden. Der Server gilt als nicht verfügbar, wenn ein Kommunikationsversuch gescheitert ist.Wählen Sie die Aufgabe **Erweiterte Einstellungen**, ändern Sie die Standardzeit nach Bedarf und klicken Sie auf **OK**.

Sie können die Zeit in Sekunden festlegen, die beim Herstellen einer ersten Verbindung mit einem Delivery Controller gewartet werden soll. Der Standardwert ist 6.

Wählen Sie **Erweiterte Einstellungen**, geben Sie Zeit in Sekunden an, die beim Herstellen der ersten Verbindung gewartet werden soll, und klicken Sie auf **OK**.

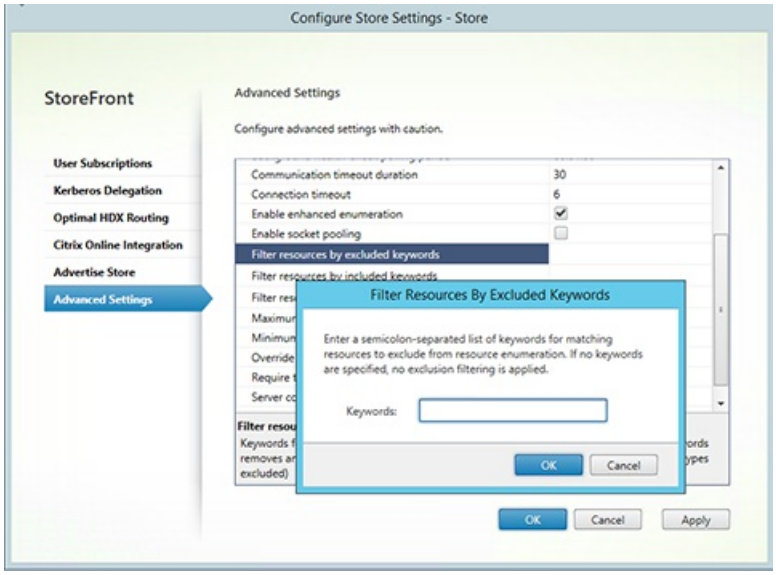
Sie können die parallele Kommunikation mit Delivery Controllern aktivieren oder deaktivieren. Die Standardeinstellung ist "Ein".

Aktivieren oder deaktivieren Sie über die Aufgabe **Erweiterte Einstellungen** das Kontrollkästchen **Erweiterte Enumeration** aktivieren und klicken Sie auf **OK.**

Socketpooling ist in Stores standardmäßig deaktiviert. Ist Socketpooling aktiviert, verwaltet StoreFront einen Socketpool, anstatt Sockets jedes Mal neu zu erstellen und die Sockets beim Trennen der Verbindung an das Betriebssystem zurückzugeben. Das Aktivieren von Socketpooling verbessert die Leistung, besonders für SSL-Verbindungen (Secure Sockets Layer). Bearbeiten Sie die Storekonfigurationsdatei, um Socketpooling zu aktivieren.Aktivieren Sie über die Aufgabe**Erweiterte Einstellungen** das Kontrollkästchen **Socketpooling aktivieren** und klicken Sie auf **OK**.

Sie können Ressourcen nach Ausschlussschlüsselwörtern filtern. Durch das Festlegen von Ausschlussschlüsselwörtern werden zuvor konfigurierte Einschlussschlüsselwörter entfernt. Der Standardwert ist "Kein Filtern (alle Ressourcentypen eingeschlossen)".

Wählen Sie über **Erweiterte Einstellungen** die Option **Ressourcen nach Ausschlussschlüsselwörtern filtern**, klicken Sie rechts daneben, geben Sie die Schlüsselwörter durch Semikola getrennt ein und klicken Sie auf **OK**.



Sie können Ressourcen nach Einschlussschlüsselwörtern filtern. Durch das Festlegen von Einschlussschlüsselwörtern werden zuvor konfigurierte Ausschlussschlüsselwörter entfernt. Der Standardwert ist "Kein Filtern (alle Ressourcentypen eingeschlossen)".

Wählen Sie über **Erweiterte Einstellungen** die Option **Ressourcen nach Einschlussschlüsselwörtern filtern**, klicken Sie rechts daneben, geben Sie die Schlüsselwörter durch Semikola getrennt ein und klicken Sie auf **OK**.

Wählen Sie die Ressourcentypen, die bei der Enumeration der Ressourcen berücksichtigt werden sollen.Der Standardwert ist "Kein Filtern (alle Ressourcentypen eingeschlossen)".

Wählen Sie über **Erweiterte Einstellungen** die Option **Ressourcen nach Typ filtern**, klicken Sie rechts daneben, wählen Sie die Ressourcentypen für die Enumeration aus und klicken Sie auf **OK**.

Legen Sie fest, wie viele Anforderungen gleichzeitig an verschiedene Delivery Controller gesendet werden sollen. Der Standardwert ist 0 (kein Maximum).

Wählen Sie über **Erweiterte Einstellungen** die Option **Maximum gleichzeitiger Enumerationen**, geben Sie einen Zahlenwert ein und klicken Sie auf **OK**.

Legen Sie die Mindestanzahl Delivery Controller fest, die für eine parallele Enumeration vorhanden sein muss. Der Standardwert ist 3.

Wählen Sie über **Erweiterte Einstellungen** die Option **Minimum an Farmen für die gleichzeitige Enumeration**, geben Sie einen Zahlenwert ein und klicken Sie auf **OK**.

Durch diese Option wird der Clientname in der ICA-Startdatei durch eine von Citrix Receiver für Web generierte ID ersetzt. Wenn die Option deaktiviert ist, wird der Clientname von Citrix Receiver festgelegt. Der Standardwert ist "Aus".

Aktivieren Sie über die Aufgabe **Erweiterte Einstellungen** das Kontrollkästchen **ICA-Clientnamen überschreiben** und klicken Sie auf **OK**.

Ist diese Option aktiviert, erzwingt StoreFront Konsistenz zwischen dem für die Authentifizierung verwendeten Gateway und dem für den Zugriff auf den Store verwendeten Gateway. Sind diese Werte nicht konsistent, müssen die Benutzer eine erneute Authentifizierung durchführen. Sie müssen diese Option für SmartAccess aktivieren. Die Standardeinstellung ist "Ein".

Aktivieren Sie über die Aufgabe **Erweiterte Einstellungen** das Kontrollkästchen **Tokenkonsistenz erforderlich** und klicken Sie auf **OK**.

Legen Sie die Anzahl der Kommunikationsversuche mit Delivery Controllern fest, bevor diese als nicht verfügbar markiert werden. Der Standardwert ist 1.

Wählen Sie über **Erweiterte Einstellungen** die Option **Serverkommunikationsversuche**, geben Sie einen Zahlenwert ein und klicken Sie auf **OK**.

Legen Sie fest, ob Fenster und Symbolleiste von Desktop Viewer angezeigt werden sollen, wenn Benutzer von Legacyclients aus auf ihre Desktops zugreifen. Der Standardwert ist "Aus".

Aktivieren Sie über die Aufgabe **Erweiterte Einstellungen** das Kontrollkästchen **Desktop Viewer für Legacyclients anzeigen** und klicken Sie auf **OK**.

Verwalten einer Citrix Receiver für Web-Site

Nov 27, 2017

Citrix Receiver für Web ermöglicht von vielfältigen Geräten aus den mühelosen und sicheren Zugriff auf Anwendungen, Daten und Desktops. Verwenden Sie StoreFront zum Konfigurieren der App-Auswahl für Citrix Receiver für Web.

Verwenden Sie die StoreFront-Verwaltungskonsole zur Ausführung folgender Aufgaben für Citrix Receiver für Web:

Erstellen einer Citrix Receiver für Web-Site	Erstellen Sie Citrix Receiver für Web-Sites, damit Benutzer über eine Webseite auf Stores zugreifen können.
Konfigurieren von Citrix Receiver für Web-Sites	Ändern Sie die Einstellungen für Receiver für Web-Sites.
Konfigurieren der Unterstützung der einheitlichen Citrix Receiver-Benutzeroberfläche	StoreFront unterstützt die klassische und die einheitliche Benutzeroberfläche. Die einheitliche Benutzeroberfläche liefert eine zentral verwaltete HTML5-Benutzererfahrung.
Erstellen und Verwalten empfohlener Apps	Erstellen Sie App-Gruppen mit empfohlenen Apps (sogenannte Highlights) für die Benutzer, die einer bestimmten Kategorie angehören oder zu ihr passen.
Konfigurieren von Workspace Control	Mit Workspace Control folgen Anwendungen dem Benutzer, wenn er das Gerät wechselt.
Konfigurieren der Verwendung der Browserregisterkarten für Citrix Receiver für HTML5	Zum Festlegen, ob der Desktop bzw. die Anwendung beim Start von Ressourcen über Verknüpfungen mit Citrix Receiver für HTML5 die Citrix Receiver für Web-Site in der geöffneten Browserregisterkarte ersetzt anstatt eine neue Registerkarte anzuzeigen.
Konfigurieren von Kommunikationstimeoutdauer und Wiederholungsversuchen	Standardmäßig erfolgt bei Anforderungen von einer Receiver für Web-Site an den zugeordneten Store nach drei Minuten ein Timeout. Nach einem gescheiterten Kommunikationsversuch gilt der Store als nicht verfügbar.Sie können die Standardeinstellungen ändern.

Erstellen einer Citrix Receiver für Web-Site

Nov 27, 2017

Mit der Aufgabe Website erstellen können Sie Receiver für Web-Sites hinzufügen, sodass Benutzer über eine Webseite auf Stores zugreifen können.

Wichtig: Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Wenn Sie die Änderungen vorgenommen haben, übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden.

1. Klicken Sie auf der Windows-Startseite oder auf der Apps-Seite auf die Kachel Citrix StoreFront.
2. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten Store, wählen Sie im BereichAktionen den Store, für den Sie die Citrix Receiver für Web-Site erstellen möchten, und klicken Sie auf Receiver für Web-Sites verwalten.
3. Klicken Sie auf **Hinzufügen**, um die Citrix Receiver für Web-Site zu erstellen. Geben Sie die gewünschte URL in das Websitepfadfeld ein und klicken Sie auf **Weiter**.
4. Wählen Sie die Citrix Receiver-Benutzeroberfläche und klicken Sie auf **Weiter**.
5. Wählen Sie die Authentifizierungsmethode, klicken Sie auf Erstellen und auf Fertig stellen nachdem die Site erstellt wurde.
   Die URL, über die Benutzer auf die Citrix Receiver für Web-Site zugreifen, wird angezeigt. Weitere Informationen zum Ändern der Einstellungen für Citrix Receiver für Web-Sites finden Sie unter Konfigurieren von Citrix Receiver für Web-Sites.

Standardmäßig versucht die Site zu ermitteln, ob Citrix Receiver auf dem Benutzergerät installiert ist, wenn ein Benutzer über einen Computer unter Windows oder Mac OS X auf Receiver für Web-Sites zugreift. Wenn Citrix Receiver nicht erkannt wird, wird der Benutzer aufgefordert, die entsprechende Citrix Receiver-Version für seine Plattform von der Citrix Website herunterzuladen und zu installieren. Weitere Informationen über das Ändern dieses Verhaltens finden Sie unter Deaktivieren von Erkennung und Bereitstellung von Citrix Receiver.

Die Standardkonfiguration für Receiver für Web-Sites erfordert, dass Benutzer eine kompatible Version von Citrix Receiver installieren, um auf ihre Desktops und Anwendungen zuzugreifen. Sie können jedoch Receiver für HTML5 auf den Receiver für Web-Sites aktivieren, sodass Benutzer, die Citrix Receiver nicht installieren können, weiterhin Zugriff auf Ressourcen haben. Weitere Informationen finden Sie unter Konfigurieren von Citrix Receiver für Web-Sites.

Konfigurieren von Citrix Receiver für Web-Sites

Nov 27, 2017

MitCitrix ReceiverfürWeb-Sites können Benutzer über eine Webseite auf Stores zugreifen. Mit den folgenden Anleitungen können Sie die Einstellungen für Citrix Receiver für Web-Sites ändern. Einige erweiterte Einstellungen können nur durch Bearbeitung der Sitekonfigurationsdateien geändert werden. Weitere Informationen finden Sie unter Konfigurieren von Citrix Receiver für Web-Sites mithilfe von Konfigurationsdateien.

Wichtig: Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Wenn Sie die Änderungen vorgenommen haben, übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden.

Verwenden Sie die Aufgabe Authentifizierungsmethoden , um Benutzern Authentifizierungsmethoden für die Verbindung mit der Citrix Receiver für Web-Site zuzuweisen. Mit dieser Aktion können Sie eine Untergruppe mit Authentifizierungsmethoden für jede Receiver für Web-Site festlegen.

1. Klicken Sie auf der Windows-Startseite oder auf der Apps-Seite auf die Kachel Citrix StoreFront.
2. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores** und im Ergebnisbereich den Store, den Sie ändern möchten.
3. Klicken Sie im Bereich Aktionen auf **Receiver für Web-Sites verwalten**, klicken Sie auf **Konfigurieren** und wählen Sie **Authentifizierungsmethoden**, um die Zugriffsmethoden für die Benutzer festzulegen.
   - AktivierenSie das Kontrollkästchen Benutzername und Kennwort, um die explizite Authentifizierung zu aktivieren. Benutzer geben beim Zugriff auf ihre Stores ihre Anmeldeinformationen ein.
   - Wählen Sie das Kontrollkästchen **SAML-Authentifizierung**, um die Integration eines SAML-Identitätsanbieters zu ermöglichen. Benutzer authentifizieren sich bei Access Gateway und werden beim Zugriff auf ihre Stores automatisch angemeldet. Dropdownmenü "Einstellungen":
     - Wählen Sie **Identitätsanbieter**, um die Vertrauensstellung mit dem Identitätsanbieter zu konfigurieren.
     - Wählen Sie **Dienstanbieter**, um die Vertrauensstellung mit dem Dienstanbieter zu konfigurieren. Diese Informationen sind für den Identitätsanbieter erforderlich.
   - Aktivieren Sie das Kontrollkästchen Domänen-Passthrough, um Passthrough für Active Directory-Domänenanmeldeinformationen von Benutzergeräten zu aktivieren. Benutzer authentifizieren sich bei den Windows-Computern, die der Domäne angehören, und werden beim Zugriff auf ihre Stores automatisch angemeldet. Um diese Option verwenden zu können, muss Passthrough-Authentifizierung aktiviert sein, wenn Citrix Receiver für Windows auf den Benutzergeräten installiert ist. Beachten Sie, dass Domänenpassthrough für Citrix Receiver für Web auf Windows-Betriebssysteme mit Chrome, Firefox, Internet Explorer und Edge beschränkt ist.
   - Aktivieren Sie das Kontrollkästchen Smartcard, um die Smartcardauthentifizierung zu aktivieren. Benutzer authentifizieren sich mit Smartcards und PINs beim Zugriff auf ihre Stores.
   - Aktivieren Sie das Kontrollkästchen Passthrough-Authentifizierung von NetScaler Gateway zum Aktivieren der Passthrough-Authentifizierung von NetScaler Gateway. Benutzer authentifizieren sich bei NetScaler Gateway und werden beim Zugriff auf ihre Stores automatisch angemeldet.
4. Klicken Sie nach der Auswahl der Authentifizierungsmethode auf OK.
   Weitere Informationen zum Ändern der Einstellungen für Authentifizierungsmethoden finden Sie unter Konfigurieren des Authentifizierungsdiensts.

Verwenden Sie die Aufgabe Websites Verknüpfungen hinzufügen, um Benutzern schnellen Zugriff auf Desktops und Anwendungen über Websites, die im internen Netzwerk gehostet werden, zu gestatten. Dafür generieren Sie URLs für Ressourcen, die über eine CitrixReceiver für Web-Site verfügbar sind, und betten diese Links in die Websites ein. Die Benutzer klicken auf einen Link und werden an die Receiver für Web-Site weitergeleitet, wo sie sich anmelden, wenn sie dies nicht bereits getan haben. Die Receiver für Web-Site startet automatisch die Ressource. Im Fall von Anwendungen wird zudem ein Abonnement für die Benutzer erstellt, wenn diese eine Anwendung noch nicht abonniert haben.

1. Klicken Sie auf der Windows-Startseite oder auf der Apps-Seite auf die Kachel Citrix StoreFront.
2. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores** und wählen Sie im Ergebnisbereich die Site.
3. Klicken Sie im Bereich **Aktionen** auf **Receiver für Web-Sites verwalten**, klicken Sie auf **Konfigurieren** und wählen Sie **Websiteverknüpfungen**.
4. Klicken Sie auf **Hinzufügen**, um die URL für eine Website hinzuzufügen, auf der Sie Verknüpfungen hosten möchten. URLs müssen in dem Format http[s]://hostname[:port], angegeben werden, wobei hostname der vollqualifizierte Domänenname des Websitehosts und port der Port für die Kommunikation mit dem Host ist, der verwendet wird, wenn der Standardport für das Protokoll nicht verfügbar ist. Pfade zu spezifischen Seiten auf der Website sind nicht erforderlich. Wenn Sie eine URL ändern möchten, wählen Sie den Eintrag in der Liste Websites aus und klicken Sie auf Bearbeiten. Wählen Sie einen Eintrag in der Liste aus und klicken Sie auf Entfernen, wenn Sie die URL einer Website löschen möchten, auf der Sie keine Verknüpfungen zu über Citrix Receiver für Web-Site verfügbaren Ressourcen mehr hosten möchten.
5. Klicken Sie auf Verknüpfungen abrufen und dann auf Speichern, wenn Sie dazu aufgefordert werden, die Konfigurationsänderungen zu speichern.
6. Melden Sie sich bei der Receiver für Web-Site an und kopieren Sie die erforderlichen URLs in Ihre Website.

Standardmäßig werden Benutzersitzungen auf Citrix Receiver für Web-Sites nach 20 Minuten Inaktivität beendet. Wenn eine Sitzung beendet wird, können Benutzer weiterhin bereits ausgeführte Desktops oder Anwendungen verwenden. Sie müssen sich jedoch neu anmelden, um auf Funktionen von Citrix Receiver für Web-Sites zugreifen zu können, z. B. das Abonnieren von Anwendungen.

Verwenden Sie die Aufgabe Sitzungstimeout im Bildschirm **Receiver für Web-Sites verwalten** zum Ändern des Sitzungstimeoutwerts.

1. Klicken Sie auf derWindows-Startseite oder auf der Seite **Apps** auf die Kachel **Citrix StoreFront**.
2. Wählen Sie im linken Bereich den Knoten **Stores**, klicken Sie im Bereich **Aktionen** auf **Receiver für Web-Sites verwalten**, klicken Sie auf **Konfigurieren** und wählen Sie **Sitzungseinstellungen**. Für das **Sitzungstimeout** können Sie Minuten und Stunden festlegen. Der Mindestwert ist für alle Zeitintervalle 1. Der Höchstwert entspricht 1 Jahr für jedes Zeitintervall.

Verwenden Sie die Aufgabe **Anwendungs- und Desktopansicht in Receiver für Web** im Bildschirm **Receiver für Web-Sites verwalten** zum Ändern des Sitzungstimeoutwerts.

1. Klicken Sie auf derWindows-Startseite oder auf der Seite **Apps** auf die Kachel **Citrix StoreFront**.
2. Wählen Sie im linken Bereich den Knoten **Stores**, klicken Sie im Bereich **Aktionen** auf "Receiver für Web-Sites verwalten", klicken Sie auf **Konfigurieren** und wählen Sie **Einstellungen für die Clientoberfläche**.
3. Wählen Sie in den Dropdownmenüs **Ansicht auswählen** und **Standardansicht** die Ansichten aus, die angezeigt

werden sollen.

Aktivieren der Ordneransicht:

1. Klicken Sie auf derWindows-Startseite oder auf der Seite **Apps** auf die Kachel **Citrix StoreFront**.
2. Wählen Sie im linken Bereich den Knoten **Stores**, klicken Sie im Bereich **Aktionen** auf **Receiver für Web-Sites verwalten** und klicken Sie dann auf **Konfigurieren**.
3. Wählen Sie **Erweiterte Eigenschaften** aus und aktivieren Sie **Ordneransicht aktivieren**.

Standardmäßig werden von Citrix Receiver für Web-Sites Provisioningdateien angeboten, damit Benutzer Citrix Receiver automatisch für den zugeordneten Store konfigurieren können. Die Provisioningdateien enthalten Verbindungsinformationen für den Store, über den die Ressourcen auf der Website bereitgestellt werden, einschließlich Details jeglicher für den Store konfigurierter NetScaler Gateway-Bereitstellungen und Beacons.

Verwenden Sie die Aufgabe **Receiver-Konfiguration aktivieren** im Bildschirm **Receiver für Web-Sites verwalten** zum Ändern des Sitzungstimeoutwerts.

1. Klicken Sie auf der Windows-**Startseite** oder auf der **Apps**-Seite auf die Kachel **Citrix StoreFront**.
2. Wählen Sie im linken Bereich den Knoten **Stores**, klicken Sie im Bereich **Aktionen** auf **Receiver für Web-Sites verwalten**, klicken Sie auf **Konfigurieren** und wählen Sie **Einstellungen für die Clientoberfläche**.
3. Wählen Sie **Receiver-Konfiguration aktivieren**.

Verwenden Sie die Aufgabe **Citrix Receiver bereitstellen** zum Konfigurieren der Funktionsweise einer Citrix Receiver für Web-Site,wenn ein Windows- oder Mac OS X-Benutzer ohne Citrix Receiver auf die Site zugreift. Standardmäßig wird bei einem Zugriff von einem Computer mit Windows oder mit Mac OS X von Citrix Receiver für Web-Sites automatisch versucht, zu ermitteln, ob Citrix Receiver installiert ist.

Wenn Citrix Receiver nicht erkannt wird, wird der Benutzer aufgefordert, die entsprechende Citrix Receiver-Version für seine Plattform herunterzuladen und zu installieren. Der Standardort für den Download ist die Citrix Website; Sie können jedoch auch die Installationsdateien auf den StoreFront-Server kopieren und Benutzern diese lokalen Dateien anbieten.

Für Benutzer, die Citrix Receiver nicht installieren können, können Sie Citrix Receiver für HTML5 auf Citrix Receiver für Web-Sites aktivieren. Mit Citrix Receiver für HTML5 können Benutzer auf Desktops und Anwendungen direkt über einen HTML5-kompatiblen Webbrowser zugreifen, ohne dass Citrix Receiver installiert werden muss. Es werden sowohl interne Netzwerkverbindungen als auch Verbindungen über NetScaler Gateway unterstützt. Bei Verbindungen über das interne Netzwerk unterstützt Citrix Receiver für HTML5 allerdings nur den Zugriff auf Ressourcen, die von bestimmten Produkten bereitgestellt werden. Außerdem sind bestimmte Versionen von NetScaler Gateway erforderlich, um Verbindungen von außerhalb des Unternehmensnetzwerks zu ermöglichen. Weitere Informationen finden Sie unter Anforderungen an die Infrastruktur.

Für lokale Benutzer im internen Netzwerk ist der Zugriff über Citrix Receiver für HTML5 auf Ressourcen, die von XenDesktop und XenApp bereitgestellt werden, standardmäßig deaktiviert. Sie aktivieren den lokalen Zugriff auf Desktops und Anwendungen über Citrix Receiver für HTML5, indem Sie die ICA-Richtlinie WebSockets-Verbindungen auf den XenDesktop- und XenApp-Servern aktivieren. Port 8008 wird sowohl von XenDesktop als auch von XenApp für Verbindungen über Citrix Receiver für HTML5 verwendet. Stellen Sie sicher, dass Firewalls und andere Netzwerkgeräte den Zugriff auf diesen Port zulassen. Weitere Informationen finden Sie unter Einstellungen der Richtlinie "WebSockets".

Citrix Receiver für HTML5 kann nur mit Internet Explorer über HTTP-Verbindungen verwendet werden. Wenn Benutzer Citrix Receiver für HTML5 mit Mozilla Firefox über HTTPS-Verbindungen verwenden möchten, müssen sie **about:config** in die Adressleiste von Firefox eingeben und die Einstellung **network.websocket.allowInsecureFromHTTPS** auf **true** setzen.

1. Klicken Sie auf derWindows-Startseite oder auf der Seite **Apps** auf die Kachel Citrix StoreFront.
2. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores** aus und wählen Sie im Ergebnisbereich eine Site aus. Klicken Sie im Bereich **Aktionen** auf **Receiver für Web-Sites verwalten** und dann auf **Konfigurieren**.
3. Wählen Sie **Citrix Receiver bereitstellen** und geben Sie die Antwort der Citrix Receiver für Web-Site ein, wenn Citrix Receiver nicht auf einem Gerät des Benutzers erkannt werden kann.

- Sollen die Benutzer aufgefordert werden, die für ihre Plattform geeignete Citrix Receiver-Version herunterzuladen und zu installieren, wählen Sie **Lokal installieren**. Benutzer müssen dann Citrix Receiver installieren, um Zugriff auf Desktops und Anwendungen über die Site zu erhalten.
  - Wenn Sie **Benutzer können HDX Engine (Plug-In) herunterladen** auswählen, können Benutzer Citrix Receiver herunterladen und auf dem Endbenutzer-Client installieren, wenn Citrix Receiver nicht verfügbar ist.
  - Wenn Sie **Plug-In beim Anmelden aktualisieren** auswählen, wird der Citrix Receiver-Client von Citrix Receiver für Web aktualisiert, wenn sich der Benutzer anmeldet. Zur Verwendung dieses Features müssen Sie sicherstellen, dass die Citrix Receiver-Dateien auf dem StoreFront-Server verfügbar sind.
  - Wählen Sie in der Dropdownliste eine Quelle aus.
- Sollen die Benutzer aufgefordert werden, Citrix Receiver herunterzuladen und zu installieren, wobei die Verwendung von Citrix Receiver für HTML5 möglich ist, wenn Citrix Receiver nicht installiert werden kann, wählen Sie **Receiver für HTML5verwenden, wenn lokaler Receiver nicht verfügbar ist**. Benutzer ohne Citrix Receiver werden dann bei jeder Anmeldung bei der Site aufgefordert, Citrix Receiver herunterzuladen und zu installieren.
- Wenn Sie möchten, dass der Zugriff auf Ressourcen über Citrix Receiver für HTML5 möglich ist, ohne den Benutzer aufzufordern, Citrix Receiver herunterzuladen und zu installieren, wählen Sie **Immer Receiver für HTML5 verwenden** aus. Wenn diese Option aktiviert ist, greifen Benutzer immer über Citrix Receiver für HTML5 auf Desktops und Anwendungen auf der Site zu, sofern sie einen HTML5-kompatiblen Browser haben. Benutzer, die keinen HTML5-kompatiblen Browser haben, müssen den nativen Citrix Receiver installieren.

Standardmäßig versucht die Site zu ermitteln, ob Citrix Receiver auf dem Benutzergerät installiert ist, wenn ein Benutzer über einen Computer unter Windows oder Mac OS X auf Receiver für Web-Sites zugreift. Wenn Citrix Receiver nicht erkannt wird, wird der Benutzer aufgefordert, die entsprechende Citrix Receiver-Version für seine Plattform von der Citrix Website herunterzuladen und zu installieren.

1. Klicken Sie auf der Windows-**Startseite** oder auf der **Apps**-Seite auf die Kachel **Citrix StoreFront**.
2. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores** aus und wählen Sie im Ergebnisbereich eine Site aus. Klicken Sie im Bereich **Aktionen** auf **Receiver für Web-Sites verwalten** und dann auf **Konfigurieren**.
3. Wählen Sie **Citrix Receiver bereitstellen** und **Quelle für Receiver** und navigieren Sie dann zu den Installationsdateien.

Vor dem Anmelden an StoreFront fordert Citrix Receiver für Web die Benutzer zur Installation der aktuellen Version von Citrix Receiver auf, wenn Citrix Receiver nicht bereits auf dem Computer des Benutzers installiert ist (für Internet Explorer-, Firefox- und Safari-Benutzer) oder wenn Benutzer das erste Mal die Site besuchen (für Chrome-Benutzer). Abhängig von der

Konfiguration wird diese Aufforderung auch angezeigt, wenn die Installation von Citrix Receiver aktualisiert werden kann.

Sie können Citrix Receiver für Web so konfigurieren, dass die Aufforderung nach dem Anmelden an StoreFront angezeigt wird.

1. Klicken Sie auf derWindows-Startseite oder auf der Seite **Apps** auf die Kachel **Citrix StoreFront**.
2. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores** aus und wählen Sie im Ergebnisbereich die Site aus.
3. Klicken Sie im Bereich **Aktionen** auf **Receiver für Web-Sites verwalten** und dann auf **Konfigurieren**.
4. Wählen Sie **Erweiterte Einstellungen** und aktivieren Sie **Aufforderung zum Installieren von Citrix Receiver nach der Anmeldung**.

Verwenden Sie **Receiver für Web-Sites verwalten** im Bereich **Aktionen** zum Löschen von Citrix Receiver für Web-Sites. Wenn Sie eine Site entfernen, können Benutzer diese nicht mehr für den Zugriff auf den Store verwenden.

Unterstützung der einheitlichen Citrix Receiver-Benutzeroberfläche

Nov 27, 2017

StoreFront unterstützt die **klassische** und die **einheitliche** Benutzeroberfläche. In einer Umgebung mit klassischer Benutzeroberfläche liefert jede Citrix Receiver-Plattform ihre eigene Benutzeroberfläche. In einer Umgebung mit der neuen einheitlichen Benutzeroberfläche erhalten alle Web- und systemeigenen Citrix Receiver eine zentral verwaltete HTML5-Benutzeroberfläche. Dies ermöglicht die Anpassung und das Verwalten von App-Gruppen mit Highlights.

Stores, die mit dieser Version von StoreFront erstellt wurden, haben standardmäßig die einheitliche Benutzeroberfläche, für Upgrades wird von Citrix jedoch standardmäßig die klassische Benutzeroberfläche beibehalten. ZurUnterstützung der einheitlichen Benutzeroberfläche müssen Sie einen StoreFront-Store einer Receiver für Web-Site zuweisen, die zur Verwendung der einheitlichen Benutzeroberfläche konfiguriert ist.

Wichtig: Die einheitliche Benutzeroberfläche wird nicht unterstützt, wenn die Receiver für Web-Site einer eingeschränkten Zone hinzugefügt wird. Wenn die Receiver für Web-Site in einer eingeschränkten Zone sein muss, konfigurieren Sie die klassische Benutzeroberfläche für den Store.

VerwendenSie die StoreFront-Verwaltungskonsole zur Ausführung folgender Aufgaben für Citrix Receiver für Web:

- Erstelleneiner Citrix Receiver für Web-Site
- Ändern der Benutzeroberfläche der Citrix Receiver für Web-Site
- Auswähleneiner Citrix Receiver für Web-Site mit einheitlicher Benutzeroberfläche zur Zuweisung zum Store
- Anpassen der Receiver-Darstellung

Wichtig: Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Wenn Sie die Änderungen vorgenommen haben, übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden.

> ## Hinweis
>
> Bei Verwendung von XenApp 6.x-Anwendungen wird **Stream zum Client** bzw. **Streaming (falls möglich), sonst Zugriff von einem Server** nicht unterstützt, wenn die einheitliche Benutzeroberfläche aktiviert ist.

Eine Citrix Receiverfür Web-Site wird automatisch mit jedem neuen Store erstellt. Sie können mit diesem Verfahren auch zusätzliche Receiver für Web-Sites erstellen.

1. Klicken Sie auf der Windows-Startseite oder auf der Apps-Seite auf die Kachel Citrix StoreFront.
2. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten Stores, klicken Sie im Bereich Aktionen auf Receiver für Web-Sites verwalten > Hinzufügen und befolgen Sie die Anweisungen im Assistenten.

Sie können wählen, ob eine Citrix Receiver für Web-Website eine **klassische** oder **einheitliche** Benutzeroberfläche hat. Bei

Aktivieren der klassischen Benutzeroberfläche werden die erweiterte Anpassung und die Verwaltung von App-Gruppen mit Highlights deaktiviert.

1. Klicken Sie auf der Windows-Startseite oder auf der Apps-Seite auf die Kachel Citrix StoreFront.
2. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten Stores und dann im mittleren Bereich den Store, den Sie ändern möchten, klicken Sie im Bereich **Aktionen auf** Receiver für Web-Sites verwalten und dann auf Konfigurieren.
3. Wählen Sie **Receiver-Oberfläche** und dann **Klassische Receiver-Benutzeroberfläche deaktivieren** oder **Klassische Receiver-Benutzeroberfläche aktivieren**.

Auswählen einer Citrix Receiver für Web-Site mit einheitlicher Benutzeroberfläche zur Zuweisung zum Store

Bei der Erstellung eines neuen Stores mit StoreFront wird automatisch eine Citrix Receiver für Web-Site im einheitlichen Modus erstellt und dem Store zugewiesen.WennSie jedoch ein Upgrade einer früheren Version von StoreFront durchführen, erfolgt standardmäßig eine Rückkehr zur klassischen Benutzeroberfläche.

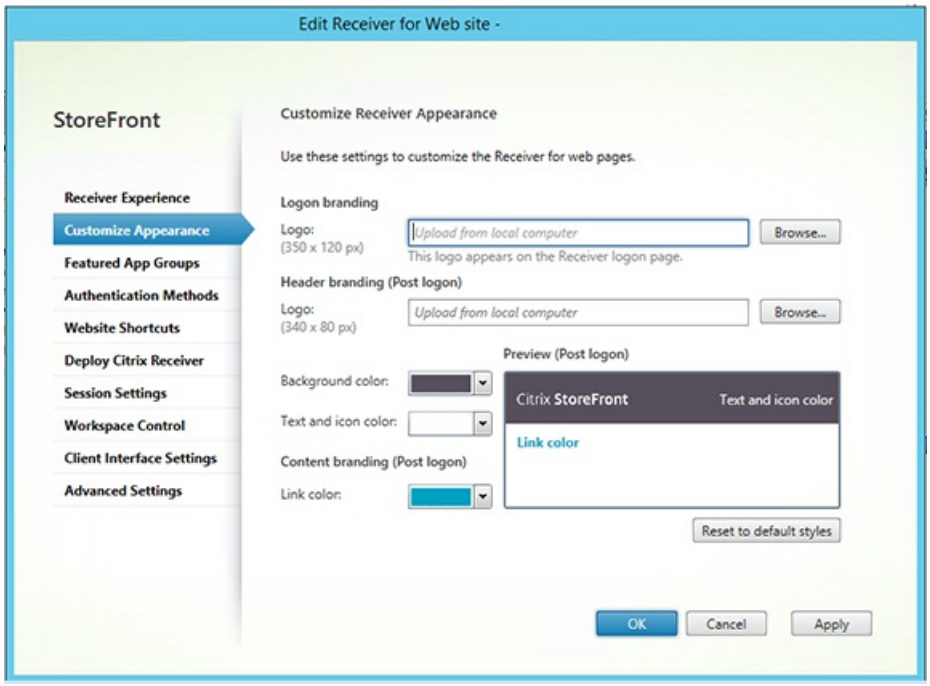
Zum Auswählen einer Citrix Receiver für Web-Site für die Bereitstellung einer einheitlichen Benutzeroberfläche für einen Store müssen Sie mindestens eine Citrix Receiver für Web-Site haben, bei der die klassische Benutzeroberfläche deaktiviert ist.

1. Klicken Sie auf derWindows-Startseite oder auf der Seite **Apps** auf die Kachel **Citrix StoreFront**.
2. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores** und dann im mittleren Bereich den Store aus und klicken Sie im Bereich **Aktionen** auf **Einheitliche Benutzeroberfläche konfigurieren**. Nur Websites, die den einheitlichen Modus unterstützen (klassische Benutzeroberfläche deaktiviert) können als Standard für einen Store verwendet werden. Wenn Sie keine Citrix Receiver für Web-Website erstellt haben, wird eine entsprechende Meldung mit einem Link zum Erstellen einer neuen Receiver für Web-Website angezeigt. Sie können auch eine vorhandene Receiver für Web-Site in eine Receiver für Web- Website umwandeln. Weitere Informationen finden Sie unter Ändern der Citrix Receiver-Benutzeroberfläche.
3. Wenn Sie eine Receiver für Web-Site erstellt haben, wählen Sie **Einheitliche Benutzeroberfläche konfigurieren** und dann die Website.

> **Important**
>
> Wenn Sie für eine Receiver für Web-Site von der einheitlichen Benutzeroberfläche zu der klassischen Benutzeroberfläche wechseln, kann sich dies auf die nativen Citrix Receiver-Clients auswirken. Wechseln zurück zu der einheitlichen Benutzeroberfläche für diese Receiver für Web-Site aktualisiert nicht die Benutzeroberfläche für native Citrix Receiver-Clients auf die einheitliche Benutzeroberfläche. Sie müssen die einheitlichen Benutzererfahrung in der Verwaltungskonsole im Knoten "Stores" zurücksetzen.

Zum Anpassen der Citrix Receiver-Darstellung muss für die Citrix Receiver für Web-Website die klassische Benutzeroberfläche deaktiviert sein.

1. Klicken Sie auf der Windows-Startseite oder auf der Seite **Apps** auf die Kachel **Citrix StoreFront**.
2. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores**, klicken Sie im Aktionsbereich auf **Receiver für Web-Sites verwalten** und klicken Sie auf **Konfigurieren**.
3. Wählen Sie **Receiver-Oberfläche** und dann **Klassische Receiver-Benutzeroberfläche deaktivieren**.
4. Wählen Sie **Benutzeroberfläche anpassen** und legen Sie fest, wie die Website nach der Anmeldung angezeigt werden soll.



Erstellen und Verwalten empfohlener Apps

Nov 27, 2017

Sie können App-Gruppen mit empfohlenen Apps (sogenannte Highlights) für die Benutzer erstellen, die einer bestimmten Kategorie angehören oder zu ihr passen. Beispielsweise können Sie eine App-Gruppe mit Highlights unter dem Namen "Vertriebsabteilung" für Apps erstellen, die von dieser Abteilung verwendet werden. Sie können empfohlene Apps in der StoreFront-Verwaltungskonsole über Anwendungsnamen definieren oder mit Schlüsselwörtern oder Anwendungskategorien, die in der Studio-Konsole festgelegt wurden.

Verwenden Sie die Aufgabe App-Gruppen mit Highlights zum Hinzufügen, Bearbeiten und Entfernen von App-Gruppen mit Highlights.

Wichtig: Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Wenn Sie die Änderungen vorgenommen haben, übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden.
Diese Funktion ist nur verfügbar, wenn die klassische Benutzeroberfläche deaktiviert wurde.

1. Klicken Sie auf der Windows-Startseite oder auf der Seite **Apps** auf die Kachel **Citrix StoreFront**.
2. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten "Stores", klicken Sie im Aktionsbereich auf **Receiver für Web-Sites verwalten** und klicken Sie auf **Konfigurieren**.
3. Wählen Sie **App-Gruppen mit Highlights**.
4. Klicken Sie im Dialogfeld **App-Gruppen mit Highlights** auf **Erstellen**, um eine neue App-Gruppe mit Highlights zu erstellen.
5. Geben Sie im Dialogfeld **App-Gruppe mit Highlights erstellen** einen Namen, eine Beschreibung (optional), einen Hintergrund und die Methode an, mit der Sie die App-Gruppen mit Highlights definieren. Sie können Schlüsselwörter, Anwendungsnamen oder Anwendungskategorien auswählen; klicken Sie dann auf **OK**.

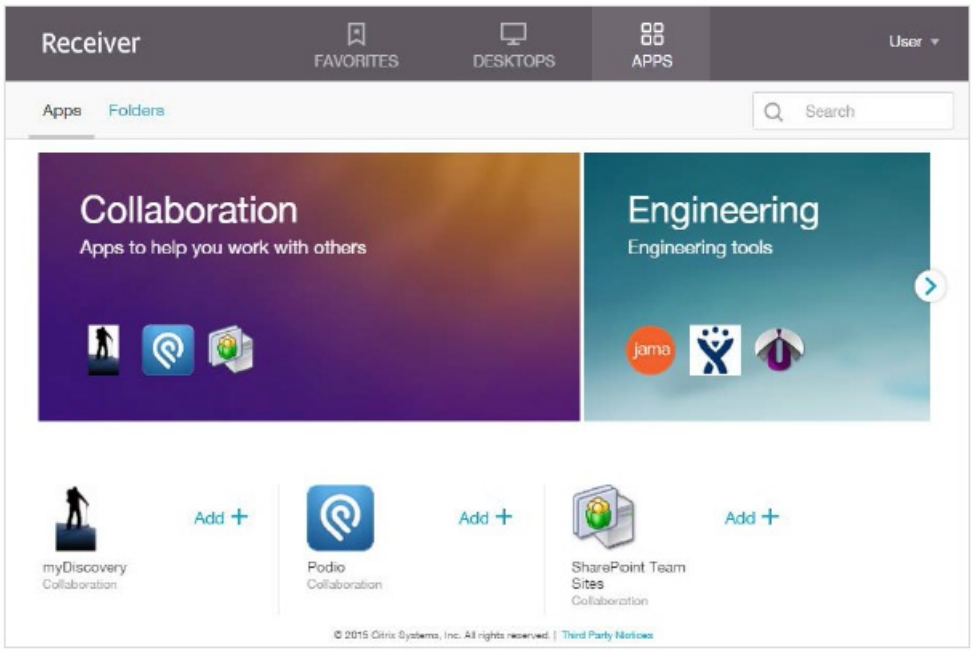
Option	Beschreibung
Schlüsselwörter	Definieren Sie die Schlüsselwörter in Studio.
Anwendungskategorie	Definieren Sie die Anwendungskategorie in Studio.
Anwendungsnamen	Verwenden Sie den Anwendungsnamen zum Definieren der App-Gruppe mit Highlights. Alle Anwendungen, deren Name dem in diesem Dialogfeld angegebenen Namen entsprechen, werden in die App-Gruppe mit Highlights aufgenommen. StoreFront unterstützt keine Platzhalter in Anwendungsnamen. Bei den Namen wird nicht zwischen Groß- und Kleinschreibung unterschieden, es werden jedoch vollständige Wörter gesucht. Wenn Sie beispielsweise "Excel" eingeben, wird in StoreFront die veröffentlichte Anwendung Microsoft Excel 2013 gefunden, doch bei Eingabe von "Exc" wird keine Übereinstimmung gefunden.

Beispiel:

Wir haben zwei App-Gruppen mit Highlights erstellt:

- Collaboration: erstellt durch Zuordnung von Apps der Kategorie **Collaboration** in Studio.

- Engineering: erstellt unter Benennung der App-Gruppe und Angabe einer App-Sammlung.



Konfigurieren von Workspace Control

Nov 27, 2017

Mit Workspace Control folgen Anwendungen dem Benutzer, wenn er das Gerät wechselt. So können etwa Krankenhausärzte von einer Arbeitsstation zu einer anderen wechseln, ohne ihre Anwendungen auf jedem einzelnen Gerät neu starten zu müssen. Workspace Control ist für Citrix Receiver für Web-Sites standardmäßig aktiviert. Bearbeiten Sie die Sitekonfigurationsdatei, um Workspace Control zu deaktivieren oder zu konfigurieren.

Wichtig: Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Wenn Sie die Änderungen vorgenommen haben, übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden.

1. Klicken Sie auf der Windows-Startseite oder auf der Seite **Apps** auf die Kachel Citrix StoreFront.
2. Wählen Sie links **Stores** und dann im Aktionsbereich **Receiver für Web-Sites verwalten** und klicken Sie auf **Konfigurieren**.
3. Wählen Sie **Workspace Control**.
4. Konfigurieren Sie die Standardeinstellungen für Workspace Control für folgende Elemente:

    Aktivieren von Workspace Control

    Optionen für die Wiederverbindung von Sitzungen

    Abmeldeaktion

Konfigurieren der Verwendung der Browserregisterkarten für Citrix Receiver für HTML5

Nov 27, 2017

Standardmäßig werden Desktops und Anwendungen in Citrix Receiver für HTML5 in einer neuen Browserregisterkarte gestartet. Beim Start von Ressourcen über Verknüpfungen mit Citrix Receiver für HTML5 ersetzt der Desktop bzw. die Anwendung jedoch die Citrix Receiver für Web-Site in der geöffneten Browserregisterkarte anstatt eine neue Registerkarte anzuzeigen.

Wichtig: Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Wenn Sie die Änderungen vorgenommen haben, übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden.

1. Klicken Sie auf der Windows-**Startseite** oder auf der **Apps-Seite** auf die Kachel Citrix StoreFront.
2. Wählen Sie links **Stores** und dann im Aktionsbereich **Receiver für Web-Sites verwalten** und klicken Sie auf **Konfigurieren**.
3. Wählen Sie **Citrix Receiver bereitstellen**.
4. Wählen Sie **Immer Receiver für HTML5 verwenden** im Dropdownmenü **Bereitstellungsoption** und aktivieren oder deaktivieren Sie je nachdem, auf welcher Registerkarte Anwendungen gestartet werden sollen, die Option **Anwendungen auf der gleichen Registerkarte starten wie Receiver für Web**.

Konfigurieren von Kommunikationstimeoutdauer und Wiederholungsversuchen

Nov 27, 2017

Standardmäßig erfolgt bei Anforderungen von einer Receiver für Web-Site an den zugeordneten Store nach drei Minuten ein Timeout. Nach einem gescheiterten Kommunikationsversuch gilt der Store als nicht verfügbar. Verwenden Sie die Aufgabe **Sitzungseinstellungen**, um die Anwendungseinstellungen zu ändern.

Wichtig: Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Wenn Sie die Änderungen vorgenommen haben, übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden.

1. Klicken Sie auf derWindows-Startseite oder auf der Seite **Apps** auf die Kachel **Citrix StoreFront**.
2. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores** und im mittleren Bereich den Store, wählen Sie dann im Aktionsbereich **Receiver für Web-Sites verwalten** und klicken Sie auf **Konfigurieren**.
3. Wählen Sie **Sitzungseinstellungen** aus, nehmen Sie Ihre Änderungen vor und klicken Sie auf **OK/Anwenden**, um die Änderungen zu speichern.

Konfigurieren des Benutzerzugriffs

Nov 27, 2017

Dieser Artikel enthält folgende Informationen:

> **Important**
>
> Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Wenn Sie die Änderungen vorgenommen haben, übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden.

Konfigurieren der Unterstützung für Verbindungen über XenApp Services-URLs

Mit der Aufgabe **XenApp Services-Support konfigurieren** konfigurieren Sie Zugriff auf Ihre Stores über XenApp Services-URLs. Benutzer domänengebundener Desktopgeräte und umfunktionierter PCs, auf denen Citrix Desktop Lock ausgeführt wird, sowie Benutzer mit älteren Citrix Clients, die nicht aktualisiert werden können, können über die XenApp-Services-URL direkt auf Stores zugreifen. Wenn Sie einen neuen Store erstellen, wird die XenApp Services-URL standardmäßig aktiviert.

Wichtig: Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Wenn Sie die Änderungen vorgenommen haben, übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden.

1. Klicken Sie auf der Windows-Startseiteoder auf der Seite **Apps** auf die Kachel **Citrix StoreFront**.
2. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores** aus und wählen Sie im Ergebnisbereich einen Store aus. Klicken Sie im Bereich **Aktionen** auf **XenApp Services-Support konfigurieren**.
3. Aktivieren oder deaktivieren Sie das Kontrollkästchen **XenApp Services-Support aktivieren**, um den Benutzerzugriff auf den Store über die angezeigte XenApp Services-URL zu aktivieren oder zu deaktivieren.
   Die XenApp Services-URL für einen Store hat das Format *//serveradresse/Citrix/storename/PNAgent/config.xml*, wobei *serveradresse* der vollqualifizierte Domänenname des Servers oder der Lastausgleichsumgebung für die StoreFront-Bereitstellung ist und *storename* der Name, den Sie beim Erstellen für den Store angegeben haben.
4. Wenn Sie die Unterstützung von XenApp Services aktivieren, geben Sie optional einen Standardstore in der StoreFront-Bereitstellung für Benutzer mit dem Citrix Online Plug-In an.
   Geben Sie einen Standardstore an, sodass die Benutzer das Citrix Online Plug-In statt mit der XenApp Services-URL für einen bestimmten Store mit der Server-URL oder der Lastausgleichs-URL der StoreFront-Bereitstellung konfigurieren können.

Deaktivieren oder Aktivieren der Verbindungswiederherstellung über Workspace Control für alle Citrix Receiver

Mit Workspace Control folgen Anwendungen dem Benutzer, wenn er das Gerät wechselt. So können etwa Krankenhausärzte von einer Arbeitsstation zu einer anderen wechseln, ohne ihre Anwendungen auf jedem einzelnen Gerät neu starten zu müssen.

StoreFront enthält eine Konfiguration zum Deaktivieren der Wiederverbindung über Workspace Control im Storedienst für alle Citrix Receiver-Versionen. Dieses Feature wird über die StoreFront-Konsole oder PowerShell verwaltet.

Verwenden der StoreFront-Verwaltungskonsole

1. Klicken Sie auf der Windows-Startseite oder auf der Seite **Apps** auf die Kachel **Citrix StoreFront**.
2. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores** und klicken Sie im Bereich **Aktionen** auf **Storeeinstellungen konfigurieren**.
3. Wählen Sie **Erweiterte Einstellungen** und aktivieren oder deaktivieren Sie nach Bedarf das Kontrollkästchen **Sitzungswiederverbindung zulassen**.

Verwenden von PowerShell

Schließen Sie die Verwaltungskonsole. Führen Sie folgenden Codeausschnitt zum Importieren der StoreFront-PowerShell-Module aus:

```
$dsInstallProp = Get-ItemProperty `
-Path HKLM:\SOFTWARE\Citrix\DeliveryServicesManagement -Name InstallDir
$dsInstallDir = $dsInstallProp.InstallDir
& $dsInstallDir\..\Scripts\ImportModules.ps1
```

Die Wiederverbindung über Workspace Control kann nun mit dem PowerShell-Befehl **Set-DSAllowSessionReconnect** aktiviert bzw. deaktiviert werden.

Syntax

```
Set-DSAllowSessionReconnect [[-SiteId] ] [[-VirtualPath]  ] `
[[-IsAllowed] ]
```

Zum Deaktivieren der Wiederverbindung über Workspace Control für einen Store in /Citrix/Store konfigurieren Sie beispielsweise den Store mit folgendem Befehl:

```
Set-DSAllowSessionReconnect -SiteId 1 -VirtualPath /Citrix/Store ` -IsAllowed $false
```

Konfigurieren von Benutzerabonnements

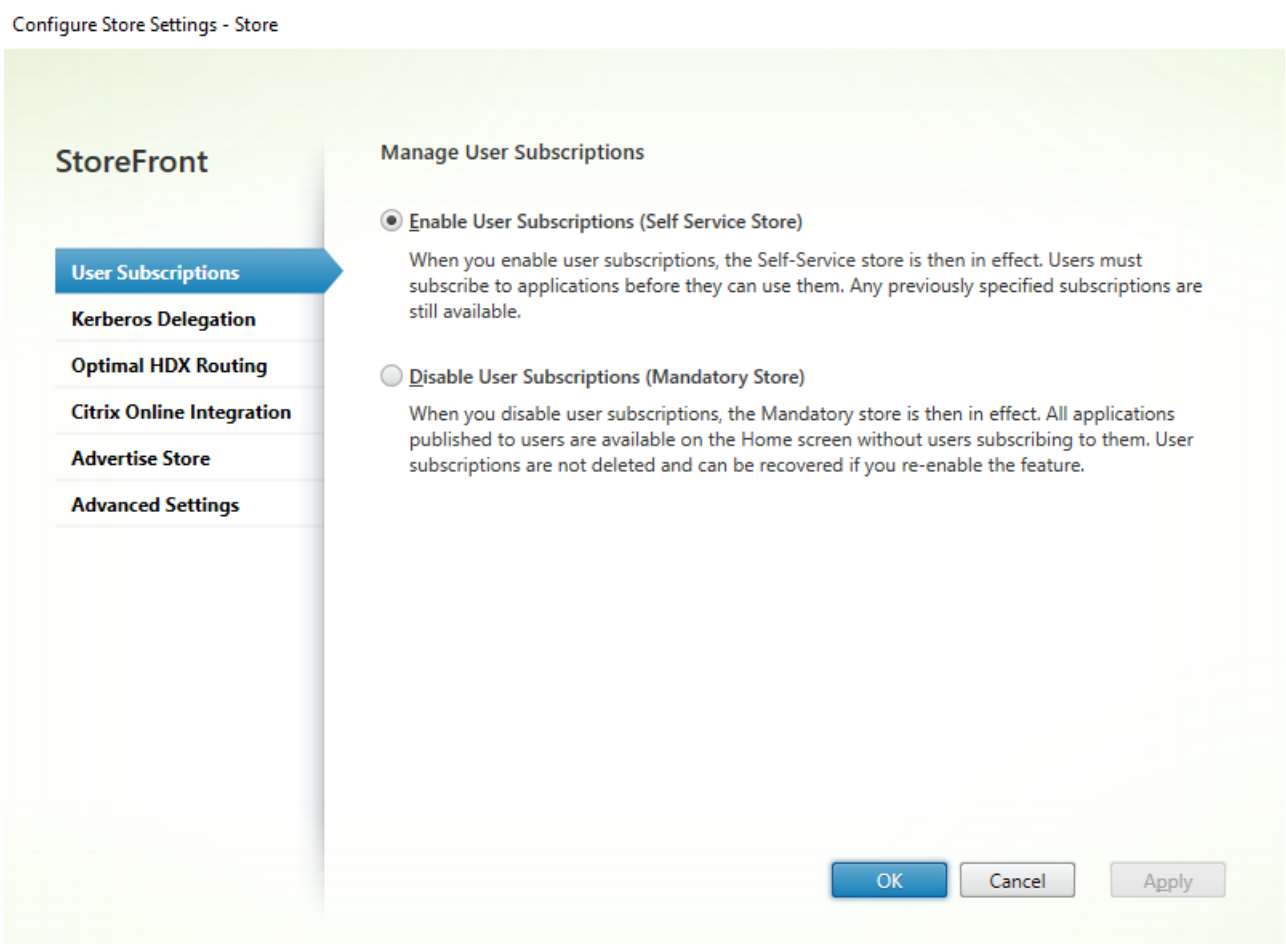
Mit der Aufgabe "Benutzerabonnements" können Sie eine der folgenden Optionen auswählen:

- Benutzer müssen Anwendungen vor der Verwendung abonnieren (Self-Service-Store).
- Benutzer können alle Anwendungen empfangen, wenn sie eine Verbindung mit dem Store herstellen (vorgegebener Store).

Sind Benutzerabonnements für einen Store in StoreFront deaktiviert, wird Benutzern nicht die Registerkarte "Favoriten" in Citrix Receiver angezeigt. Die Abonnementdaten im Store werden beim Deaktivieren von Abonnements nicht gelöscht. Werden Abonnements für den Store reaktiviert, können Benutzer ihre abonnierten Apps in den Favoriten anzeigen, sobald

sie sich das nächste Mal anmelden.

1. Klicken Sie auf derWindows-Startseite oder auf der Seite **Apps** auf die Kachel **Citrix StoreFront**.
2. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores** aus und wählen Sie im Ergebnisbereich einen Store aus. Klicken Sie im Bereich **Aktionen** auf **Storeeinstellungen konfigurieren** > **Benutzerabonnements**, um das Benutzerabonnementfeature zu aktivieren bzw. zu deaktivieren.
3. Wählen Sie **Benutzerabonnements aktivieren (Self-Service-Store)** aus, damit Benutzer Anwendungen vor der Verwendung abonnieren müssen. Alle bestehenden Abonnements sind weiterhin verfügbar.
4. Wählen Sie **Benutzerabonnements deaktivieren (vorgegebener Store)** aus, damit alle auf dem Homebildschirm veröffentlichten Anwendungen ohne Abonnement zur Verfügung stehen. Bestehende Abonnements werden nicht gelöscht und können bei Reaktivieren dieses Features wiederhergestellt werden.



In StoreFront 3.5 oder höher können Sie mit dem folgenden PowerShell-Skript Benutzerabonnements für einen Store konfigurieren:

```
$StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/citrix/"

Set-STFStoreService -StoreService $StoreObject -LockedDown $True -Confirm:$False
```

Weitere Informationen zu Get-STFStoreService finden Sie unter https://citrix.github.io/storefront-sdk/Citrix.StoreFront.Stores/Get-STFStoreService/

Verwalten von Abonnementdaten für einen Store

Verwalten Sie Abonnementdaten für einen Store mit PowerShell-Cmdlets.

Hinweis

Verwenden Sie entweder die StoreFront-Verwaltungskonsole oder PowerShell zum Verwalten von StoreFront. Verwenden Sie nicht beide Methoden zur gleichen Zeit. Schließen Sie immer erst die StoreFront-Verwaltungskonsole, bevor Sie PowerShell zum Ändern der StoreFront-Konfiguration öffnen. Es empfiehlt sich zudem, ein Backup aller Abonnementdaten zu erstellen, bevor Sie Änderungen vornehmen, damit bei Bedarf ein Rollback auf einen früheren Zustand möglich ist.

Löschen von Abonnementdaten

Für jeden Store in der Bereitstellung gibt es einen Ordner und Datenspeicher mit den Abonnementdaten.

1. Halten Sie den Citrix Abonnementstoredienst auf dem StoreFront-Server an. Solange der Citrix Abonnementstoredienst ausgeführt wird, können keine Abonnementdaten für einen Store gelöscht werden.
2. Navigieren Sie auf dem StoreFront-Server zum Ordner des Abonnementstores: C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\SubscriptionsStore\1__Citrix_
3. Löschen Sie den Inhalt des Ordners für den Abonnementstore, jedoch nicht den Ordner selbst.
4. Starten Sie den Citrix Abonnementstoredienst auf dem StoreFront-Server neu.

In StoreFront 3.5 oder höher können Sie mit dem folgenden PowerShell-Skript Abonnementdaten für einen Store löschen. Zum Ausführen dieser PowerShell-Funktion benötigen Sie Administratorrechte zum Beenden oder Starten von Diensten und zum Löschen von Dateien. Diese PowerShell-Funktion führt zum selben Ergebnis wie die oben beschriebene manuelle Schrittfolge.

Um die Cmdlets erfolgreich auszuführen, muss der Citrix Abonnementstoredienst auf dem Server ausgeführt werden.

Code KOPIEREN

```
function Remove-SubscriptionData

{

    [CmdletBinding()]

    [Parameter(Mandatory=$False)][String]$Store = "Store"

    $SubsService = "Citrix Subscriptions Store"

    # Path to Subscription Data in StoreFront version 2.6 or higher

    $SubsPath = "C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\SubscriptionsStore\1__Citrix_$Store\*"

    Stop-Service -displayname $SubsService

    Remove-Item $SubsPath -Force -Verbose

    Start-Service -displayname $SubsService

    Get-Service -displayname $SubsService

}



Remove-SubscriptionData -Store "YourStore"
```

Exportieren von Abonnementdaten

Mit dem folgenden PowerShell-Cmdlet können Sie Storeabonnementdaten in einer tabulatorgetrennten TXT-Backupdatei sichern.

```
$StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/citrix/<yourstore>"

Export-STFStoreSubscriptions -StoreService $StoreObject -FilePath "$env:USERPROFILE\Desktop\Subscriptions.txt"
```

In einer Multiserverbereitstellung können Sie dieses PowerShell-Cmdlet auf einem beliebigen Server in der StoreFront-Servergruppe ausführen. Auf jedem Server in der Servergruppe ist eine identische synchronisierte Kopie der Abonnementdaten aller Peers gespeichert. Bei eventuellen Problemen mit der Abonnementsynchronisierung zwischen Storefront-Servern können Sie die Daten aller Server in der Gruppe exportieren und auf Unterschiede überprüfen.

Wiederherstellen von Abonnementdaten

Mit Restore-STFStoreSubscriptions können Sie vorhandene Abonnementdaten überschreiben. Sie können die Abonnementdaten eines Stores mit der tabulatorgetrennten TXT-Backupdatei wiederherstellen, die Sie zuvor mit Export-STFStoreSubscriptions erstellt haben.

```
$StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/citrix/<yourstore>"

Restore-STFStoreSubscriptions -StoreService $StoreObject -FilePath "$env:USERPROFILE\Desktop\Subscriptions.txt"
```

Weitere Informationen zu Restore-STFStoreSubscriptions finden Sie unter https://citrix.github.io/storefront-sdk/Citrix.StoreFront.SubscriptionsStore/Restore-STFStoreSubscriptions/#restore-stfstoresubscriptions.

Wiederherstellen von Daten auf einem einzelnen StoreFront-Server

In einer Einzelserverbereitstellung ist nicht erforderlich, den Abonnementstoredienst herunterzufahren. Sie müssen auch nicht die vorhandenen Abonnementdaten löschen, bevor Sie die Abonnementdaten wiederherstellen.

Wiederherstellen von Daten in einer StoreFront-Servergruppe

Zum Wiederherstellen von Abonnementdaten in einer Servergruppe sind folgende Schritte erforderlich.

Beispiel einer Servergruppenbereitstellung mit drei StoreFront-Servern.

StoreFrontA

StoreFrontB

StoreFrontC

1. Erstellen Sie ein Backup der vorhandenen Abonnementdaten von einem der drei Server.
2. Beenden Sie den Abonnementstoredienst auf den Servern StoreFrontB und C, damit diese Server während der Aktualisierung von StoreFrontA keine Abonnementdaten senden oder empfangen.
3. Löschen Sie die Abonnementdaten der Server StoreFrontB und C, um Unterschiede zu den wiederhergestellten Abonnementdaten zu vermeiden.
4. Stellen Sie die Daten auf StoreFrontA mit dem Cmdlet "Restore-STFStoreSubscriptions" wieder her. Hierfür ist es nicht erforderlich, den Abonnementstoredienst anzuhalten oder Abonnementdaten auf StoreFrontA zu löschen, da diese beim Wiederherstellen überschrieben werden.
5. Starten Sie den Abonnementstoredienst auf den Servern StoreFrontB und StoreFrontC neu. Die Server können dann eine Kopie der Daten von StoreFrontA erhalten.
6. Warten Sie, bis die Synchronisierung zwischen allen Servern erfolgt. Die erforderliche Zeit hängt von der Anzahl der Datensätze auf StoreFrontA ab. Wenn alle Server in einem lokalen Netzwerk sind, geschieht die Synchronisierung normalerweise schnell. Die Synchronisierung von Abonnements über eine WAN-Verbindung kann länger dauern.
7. Exportieren Sie die Daten von StoreFrontB und C, um den Abschluss der Synchronisierung zu bestätigen oder die Gesamtanzahl an Storeabonnements anzuzeigen.

Importieren von Abonnementdaten

Verwenden Sie Import-STFStoreSubscriptions, wenn keine Abonnementdaten für den Store vorhanden sind. Mit diesem Cmdlet können Sie Abonnementdaten auch von einem Store auf einen anderen übertragen oder auf neu bereitgestellte StoreFront-Server importieren.

Code KOPIEREN

```
$StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/citrix/<yourstore>"


Import-STFStoreSubscriptions -StoreService $StoreObject -FilePath "$env:USERPROFILE\Desktop\Subscriptions.txt"
```

Weitere Informationen zu Import-STFStoreSubscriptions finden Sie unter https://citrix.github.io/storefront-sdk/Citrix.StoreFront.SubscriptionsStore/Import-STFStoreSubscriptions/#import-stfstoresubscriptions.

Informationen zur Abonnementdatendatei

Die Abonnementdatendatei ist eine Textdatei mit einer Zeile für jedes Benutzerabonnement. Jede Zeile besteht aus einer Reihe tabulatorgetrennter Werte:

...

Die Werte sind wie folgt definiert:

- <*user-identifier*>: erforderlich. Zeichenfolge zur Identifizierung des Benutzers. Dies ist die Windows-Sicherheits-ID des Benutzers.
- <*resource-id*>: erforderlich. Zeichenfolge zur Identifizierung der abonnierten Ressource.
- <*subscription-id*>: erforderlich. Zeichenfolge zur eindeutigen Identifizierung des Abonnements. Dieser Wert wird nicht verwendet (er muss jedoch in der Datendatei vorhanden sein).
- <*subscription-status*>: erforderlich. Status des Abonnements: abonniert/nicht abonniert.
- <*property-name*> und <*property-value*>: optional. Null oder mehr -/-Wertepaare. Diese repräsentieren Eigenschaften eines Abonnements durch einen StoreFront-Client (normalerweise ein Citrix Receiver). Eine Eigenschaft mit mehreren Werten, die durch mehrere Namen-/Wert-Paare mit dem gleichen Namen dargestellt wird (z. B. "... MyProp A MyProp B ...." stellt die Eigenschaft "MyProp" mit den Werten "A", "B" dar).

Beispiel:

S-0-0-00-0000000000-0000000000-0000000000-0000 XenApp.Excel 21EC2020-3AEA-4069-A2DD-08002B30309D Subscribed dazzle:position 1

Größe der Abonnementdaten auf dem Datenträger des StoreFront-Servers

Subscription Datastore Size	
No of Records	Size MB
0	6.02
1000	7.02
10000	40.00
100000	219.00
200000	358.00
500000	784.00
800000	1213.02
1000000	1497.15
1300000	1919.15
1500000	2205.15
1700000	2487.15
2000000	2915.15

Größe der TXT-Dateien für Import und Export

Subscriptions Import/Export.txt	
No of Records	Size MB
0	0.00
1000	0.13
10000	1.30
100000	12.80
200000	25.60
500000	64.10
800000	102.00
1000000	128.00
1300000	166.00
1500000	192.00
1700000	218.00
2000000	256.00

Storeabonnementszähler

Mit dem Systemmonitor von Microsoft Windows (Start > Ausführen > Perfmon) können Sie die Gesamtanzahl aller Abonnementsdatensätze auf einem Server oder die Zahl der zwischen StoreFront-Servergruppen synchronisierten Datensätze anzeigen.

Anzeige der Abonnementzähler mit PowerShell

Code KOPIEREN

```
Get-Counter -Counter "\Citrix Subscription Store(1__citrix_store)\Subscription Entries Count (including unpurged deleted records)"

Get-Counter -Counter "\Citrix Subscription Store Synchronization\Subscriptions Store Synchronizing"

Get-Counter -Counter "\Citrix Subscription Store Synchronization\Number Subscriptions Synchronized"

Get-Counter -Counter "\Citrix Subscription Store Synchronization\Number Subscriptions Transferred"
```

Einrichten hoch verfügbarer Stores mit mehreren Sites

Nov 27, 2017

Dieser Artikel enthält folgende Themen:

Für Stores mit Ressourcen aus mehreren Bereitstellungen, insbesondere wenn die Bereitstellungen sich an verschiedenen geografischen Standorten befinden, können Sie Lastausgleich und Failover zwischen Bereitstellungen konfigurieren, den Bereitstellungen Benutzer zuordnen und spezifische Bereitstellungen für die Notfallwiederherstellung mit hoch verfügbaren Ressourcen konfigurieren. Wenn Sie konfigurierte separate NetScaler Gateway-Geräte für die Bereitstellungen haben, können Sie das optimale Gerät für den Zugriff auf die Bereitstellungen definieren.

Seit StoreFront 3.5 unterstützt die StoreFront-Verwaltungskonsole häufige Szenarios mit mehreren Sites. Citrix empfiehlt, die Verwaltungskonsole zu verwenden, wenn sie die Anforderungen erfüllt.

Konfigurieren von Benutzerzuordnung und Aggregation

Mit der StoreFront-Verwaltungskonsole können Sie Folgendes:

- **Benutzer Bereitstellungen zuordnen:** Basierend auf der Active Directory-Gruppenmitgliedschaft können Sie einschränken, welche Benutzer auf bestimmte Bereitstellungen haben.
- **Bereitstellungen aggregieren:** Sie können angeben, welche Bereitstellungen Ressourcen haben, die Sie aggregieren möchten. Übereinstimmende Ressourcen aus aggregierten Bereitstellungen werden Benutzern als eine einzige hochverfügbare Ressource angezeigt.
- **Eine Zone einer Bereitstellung zuordnen:** Beim Zugriff über NetScaler Gateway in einer Konfiguration mit globalem Lastausgleich priorisiert StoreFront beim Ressourcenstarten Bereitstellungen in Zonen, die der Zone des Gateways entsprechen.

Wichtig: Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Wenn Sie die Änderungen vorgenommen haben, übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden.

1. Stellen Sie sicher, dass Sie den Store mit Details aller XenDesktop- und XenApp-Bereitstellungen, die Sie in der Konfiguration verwenden möchten, konfiguriert haben. Weitere Informationen zum Hinzufügen von Bereitstellungen zu Stores finden Sie unter Verwalten der durch Stores zur Verfügung gestellten Ressourcen.
2. Klicken Sie auf der Windows-Startseiteoder auf der Seite **Apps** auf die Kachel **Citrix StoreFront**.

3. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores** und klicken Sie im Bereich **Aktionen** auf **Delivery Controller verwalten**.
4. Sind mehrere Controller definiert, klicken Sie auf **Konfiguration der Benutzerzuordnung und der Multisiteaggregation > Konfigurieren**.
5. Klicken Sie auf **Benutzer Controllern zuordnen** und wählen Sie aus, welche Delivery Controller welchen Benutzern zur Verfügung stehen sollen.
6. Klicken Sie auf **Ressourcen aggregieren**, wählen Sie Controller und klicken Sie auf **Aggregieren**, um anzugeben, ob die Delivery Controller aggregiert werden sollen. Wenn Sie die Aggregation von Delivery Controllern aktivieren, werden Anwendungen und Desktops von Delivery Controllern mit dem gleichen Anzeigenamen und Pfad als Einzelanwendung/-desktop in Citrix Receiver angezeigt.
7. Wählen Sie eines oder beide der Kontrollkästchen für **Aggregierte Controllereinstellungen** und klicken Sie auf **OK**.

   Controller veröffentlichen identische Ressourcen: Bei Aktivierung listet StoreFront nur die Ressourcen von einem der Controller in dem aggregierten Satz auf. Ist diese Option deaktiviert, enumeriert StoreFront die Ressourcen von allen Controllern im aggregierten Satz (sodass alle für den Benutzer verfügbaren Ressourcen angesammelt werden). Aktivieren dieser Option führt zu einer verbesserten Leistung beim Enumerieren der Ressourcen. Wir empfehlen sie aber nur, wenn Sie sind ganz sicher sind, dass die Ressourcenliste in allen aggregierten Bereitstellungen identisch ist.

   Lastausgleich für Ressourcen über Controller hinweg: Bei Aktivierung werden Starts gleichmäßig auf die verfügbaren Controller verteilt. Ist diese Option deaktiviert, werden Starts an den ersten Controller geleitet, der im Benutzerzuordnungsdialogfeld angegeben wurde. Es wird ein Failover auf weitere Controller durchgeführt, wenn der Start fehlschlägt.

Erweiterte Konfigurationen

Sie können zwar viele Multisite- und Hochverfügbarkeitsvorgänge mit der StoreFront-Verwaltungskonsole festlegen, es ist jedoch auch bei der neuen Version weiterhin möglich, StoreFront mit den Konfigurationsdateien zu konfigurieren.

Zusätzliche Funktionalität mit PowerShell oder durch Bearbeiten der StoreFront-Konfigurationsdateien:

- Möglichkeit, mehrere Gruppierungen von Bereitstellungen für die Aggregation anzugeben.
  - Die Verwaltungskonsole lässt nur eine einzige Gruppierung von Bereitstellungen zu. Dies reicht in den meisten Fällen.
  - Für Stores mit vielen Bereitstellungen mit ungleichen Ressourcensätzen, verbessern mehrere Gruppierungen möglicherweise die Leistung.
- Möglichkeit, komplexe Prioritätsreihenfolgen für aggregierte Bereitstellungen anzugeben. Die Verwaltungskonsole ermöglicht den Lastausgleich für aggregierte Bereitstellungen oder ein einzelne Failoverliste.
- Die Möglichkeit Bereitstellungen für die Notfallwiederherstellung zu definieren (Bereitstellungen, auf die nur zugegriffen wird, wenn alle anderen Bereitstellungen nicht verfügbar sind).

Warnung: Nach dem Konfigurieren der erweiterten Multisiteoptionen durch manuelles Bearbeiten der Konfigurationsdatei sind einige Aufgaben in der Citrix StoreFront-Verwaltungskonsole nicht mehr verfügbar, um Konfigurationsfehler zu verhindern.

Wichtig: Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Wenn Sie die Änderungen vorgenommen haben, übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden.

1. Stellen Sie sicher, dass Sie den Store mit Details aller XenDesktop- und XenApp-Bereitstellungen, die Sie in der Konfiguration verwenden möchten (einschließlich der Notfallwiederherstellung), konfiguriert haben. Weitere

Informationen zum Hinzufügen von Bereitstellungen zu Stores finden Sie unter Verwalten der durch Stores zur Verfügung gestellten Ressourcen.

2. Öffnen Sie die Datei web.config für den Store mit einem Text-Editor. Die Datei ist normalerweise im Verzeichnis C:\inetpub\wwwroot\Citrix\storename\, wobei "storename" für den Namen steht, der beim Erstellen des Stores angegeben wurde.
3. Suchen Sie den folgenden Abschnitt in der Datei.

4. Geben Sie Ihre Konfiguration wie unten gezeigt an.

...

aggregationGroup="aggregationgroupname">

...

...

...

...

Verwenden Sie die folgenden Elemente zum Definieren der Konfiguration.

- **userFarmMapping**
  Dient zum Angeben von Bereitstellungsgruppen und zum Festlegen der Funktionsweise von Lastausgleich und Failover zwischen diesen Bereitstellungen. Dient zum Identifizieren der für die Notfallwiederherstellung zu verwendenden Bereitstellungen. Steuert den Zugriff auf Ressourcen durch Zuordnen von Microsoft Active Directory-Benutzergruppen zu den angegebenen Bereitstellungsgruppen.
- **groups**
  Namen und Sicherheits-IDs (SIDs) der Active Directory-Benutzergruppen, auf die die Zuordnung angewendet wird. Benutzergruppennamen müssen im Format *Domäne**Benutzergruppe* eingegeben werden. Werden mehrere Gruppen aufgeführt, gilt die Zuordnung nur für Benutzer, die Mitglieder aller angegebenen Gruppen sind. Zum Aktivieren des Zugriffs für alle Active Directory-Benutzerkonten legen Sie als Gruppennamen & SID **Jeder** fest.
- **equivalentFarmSet**
  Dient zum Angeben einer Gruppe äquivalenter Bereitstellungen, deren aggregierte Ressourcen für Lastausgleich bzw. Failover verwendet werden, sowie einer optional zugeordneten Gruppe von Bereitstellungen für die Notfallwiederherstellung.

  Das Attribut **loadBalanceMode** bestimmt die Zuweisung von Benutzern zu Bereitstellungen. Legen Sie den Wert des Attributs **loadBalanceMode** auf **LoadBalanced** fest, um Benutzer per Zufallsprinzip Bereitstellungen in dem Satz der äquivalenten Bereitstellungen zuzuweisen, sodass alle Benutzer gleichmäßig auf alle verfügbaren Bereitstellungen verteilt werden. Wenn Sie den Wert des Attributs **loadBalanceMode** auf **Failover** festlegen, werden die Benutzer mit der ersten verfügbaren Bereitstellung verbunden, und zwar gemäß der Reihenfolge, in der Bereitstellungen in der Konfiguration aufgelistet sind. Auf diese Weise wird die Anzahl gleichzeitig verwendeter Bereitstellungen minimiert. Geben Sie Namen für Aggregationsgruppen an, um äquivalente Bereitstellungssätze mit zu aggregierenden Ressourcen zu identifizieren. Ressourcen aus äquivalenten Bereitstellungssätzen, die zur gleichen Aggregationsgruppe gehören, werden aggregiert. Um anzugeben, dass die Bereitstellungen eines bestimmten äquivalenten Bereitstellungssatzes nicht mit anderen aggregiert werden sollen, legen Sie den Namen der Aggregationsgruppe auf die leere Zeichenfolge **""** fest.

  Für das Attribut **identical** können die Werte **true** und **false** angegeben werden. Es gibt an, ob alle Bereitstellungen in einem äquivalenten Bereitstellungssatz exakt den gleichen Ressourcensatz bieten. Sind die Bereitstellungen identisch, enumeriert StoreFront die Ressourcen des Benutzers aus nur einer primären Bereitstellung im Satz. Bieten die Bereitstellungen überlappende, aber nicht identische Ressourcen, enumeriert StoreFront aus jeder Bereitstellung, um den vollständigen Satz der Ressourcen zu erhalten, die dem Benutzer zur Verfügung stehen. Lastausgleich (zur Startzeit) kann unabhängig davon stattfinden, ob die Bereitstellungen identisch sind. Der Standardwert für das Attribut **identical** ist "false", obwohl es bei einem Upgrade für StoreFront auf **true** eingestellt ist, damit das vorhandene Verhalten nicht durch ein Upgrade geändert wird.

- **primaryFarmRefs**
  Gibt einen Satz mit äquivalenten XenDesktop- oder XenApp-Sites an, in dem manche oder alle der Ressourcen übereinstimmen. Geben Sie Namen von Bereitstellungen an, die Sie dem Store bereits hinzugefügt haben. Die hier eingegebenen Namen müssen genau mit denen übereinstimmen, die Sie beim Hinzufügen der Bereitstellungen zum Store angegeben haben.
- **optimalGatewayForFarms**
  Dient zum Angeben von Bereitstellungsgruppen und zum Definieren der optimalen NetScaler Gateway-Geräte, über die Benutzer auf die Ressourcen dieser Bereitstellungen zugreifen können. Normalerweise ist das optimale Gerät für eine Bereitstellung an demselben geografischen Standort wie die Bereitstellung. Sie müssen optimale NetScaler Gateway-Geräte für Bereitstellungen nur definieren, wenn das Gerät, über das Benutzer auf StoreFront zugreifen, nicht das optimale Gerät ist.

Konfigurieren der Abonnementsynchronisierung

Zum Konfigurieren der regelmäßigen Pullsynchronisierung von Anwendungsabonnements von Stores in unterschiedlichen StoreFront-Bereitstellungen führen Sie Windows PowerShell-Befehle aus.

Hinweis: Die StoreFront- und PowerShell-Konsolen können nicht gleichzeitig geöffnet sein. Schließen Sie immer zuerst die StoreFront-Verwaltungskonsole, bevor Sie die PowerShell-Konsole zum Verwalten der StoreFront-Konfiguration öffnen. Schließen Sie gleichermaßen immer alle Instanzen von PowerShell, bevor Sie die StoreFront-Konsole öffnen.
Wichtig: Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Wenn Sie die Änderungen vorgenommen haben, übertragen Sie die Konfigurationsänderungen auf die Servergruppen, sodass die anderen Server der Bereitstellung aktualisiert werden.
Für die Abonnementsynchronisierung müssen die konfigurierten Delivery Controller der synchronisierten Stores identische Namen haben. Beachten Sie bei den Namen der Delivery Controller die Groß-/Kleinschreibung. Wenn die Namen der Delivery Controller nicht identisch sind, haben Benutzer in den synchronisierten Stores möglicherweise unterschiedliche Abonnements.

1. Starten Sie Windows PowerShell von einem Konto mit lokalen Administratorrechten und geben Sie an der Eingabeaufforderung die folgenden Befehle ein, damit die StoreFront-Module importiert werden.
   ```
   Import-Module "installationlocation\Management\Cmdlets\UtilsModule.psm1"
   Import-Module "installationlocation\Management\Cmdlets\
     SubscriptionSyncModule.psm1"
   ```
   installationlocation ist das Verzeichnis, in dem StoreFront installiert ist (in der Regel C:\Programme\Citrix Receiver StoreFront\).

2. Zum Angeben der Remote-StoreFront-Bereitstellung, deren Store synchronisiert werden soll, geben Sie den folgenden Befehl ein.
   ```
   Add-DSSubscriptionsRemoteSyncCluster -clusterName deploymentname
     -clusterAddress deploymentaddress
   ```
   deploymentname ist ein Name zum Identifizieren der Remote-Bereitstellung und deploymentaddress ist die extern zugängliche Adresse des StoreFront-Servers oder der Lastausgleichsservergruppe für die Remotebereitstellung.

3. Zum Angeben des Remotestores, mit dem die Anwendungsabonnements der Benutzer synchronisiert werden sollen, geben Sie den folgenden Befehl ein.
   ```
   Add-DSSubscriptionsRemoteSyncStore -clusterName deploymentname
     -storeName storename
   ```
   deploymentname ist der Name, den Sie für die Bereitstellung im vorherigen Schritt angegeben haben und storename der bei der Erstellung des lokalen und des remoten Stores verwendete Name. Anwendungsabonnements zwischen Stores können nur synchronisiert werden, wenn die Namen beider Stores in der jeweiligen StoreFront-Bereitstellung identisch sind.

4. Zum Konfigurieren eines bestimmten Zeitpunkts für die Synchronisierung geben Sie den folgenden Befehl ein.
   ```
   Add-DSSubscriptionsSyncSchedule -scheduleName
     synchronizationname -startTime hh:mm
   ```
   synchronizationname ist der Name zur Identifizierung des Zeitplans, der erstellt werden soll. Legen Sie mit der Einstellung -startTime den Zeitpunkt fest, zu dem Abonnements zwischen Stores synchronisiert werden sollen. Konfigurieren Sie weitere Zeitpläne zum Festlegen zusätzlicher Synchronisierungszeiten.

5. Alternativ können Sie regelmäßige Synchronisierung in bestimmten Intervallen konfigurieren, indem Sie folgenden Befehl

eingeben.
Add-DSSubscriptionsSyncReoccuringSchedule -scheduleName
synchronizationname -startTime hh:mm:ss -repeatMinutes interval
synchronizationname ist der Name zur Identifizierung des Zeitplans, der erstellt werden soll. Legen Sie mit der Einstellung -startTime den Zeitpunkt fest, zu dem der Zeitplan beginnen soll. interval ist das Zeitintervall in Minuten zwischen den einzelnen Synchronisierungen.

6. Fügen Sie dann die Microsoft Active Directory-Domänenmaschinenkonten jedes StoreFront-Servers der Remote-Bereitstellungsgruppe der lokalen Windows-Benutzergruppe "CitrixSubscriptionSyncUsers" auf dem aktuellen Server hinzu.
   Dadurch können die Server in der Remote-Bereitstellung auf den Abonnementstoredienst der lokalen Bereitstellung zugreifen, nachdem Sie einen Synchronisierungszeitplan für die Remote-Bereitstellung konfiguriert haben. Die Gruppe "CitrixSubscriptionSyncUsers" wird automatisch erstellt, wenn Sie das Abonnementsynchronisierungsmodul gemäß Schritt 1 importieren. Weitere Informationen zum Ändern der lokalen Benutzergruppen finden Sie unter http://technet.microsoft.com/en-us/library/cc772524.aspx.

7. Wenn die lokale StoreFront-Bereitstellung aus mehreren Servern besteht, verwenden Sie die Citrix StoreFront-Managementkonsole, um die Konfigurationsänderungen auf die anderen Server in der Gruppe zu übertragen.
   Weitere Informationen über die Übertragung von Änderungen in einer StoreFront-Multiserverbereitstellung finden Sie unter Konfigurieren von Servergruppen.

8. Wiederholen Sie die Schritte 1 bis 7 für die Remotebereitstellung von StoreFront, um einen Zeitplan für die Abonnementsynchronisierung von der Remotebereitstellung zur lokalen Bereitstellung zu konfigurieren.
   Achten Sie bei der Konfiguration von Zeitplänen für die Synchronisierung von StoreFront-Bereitstellungen darauf, dass es nicht zu einer gleichzeitigen Synchronisierung kommen kann.

9. Zum Starten der Synchronisierung der Anwendungsabonnements zwischen den Stores starten Sie den Abonnementstoredienst für die lokale und die remote Bereitstellung neu. Geben Sie an einer Windows PowerShell-Eingabeaufforderung auf einem Server in jeder Bereitstellung folgenden Befehl ein.
   Restart-DSSubscriptionsStoreSubscriptionService
10. Geben Sie zum Entfernen eines Abonnements aus dem Synchronisierungszeitplan folgenden Befehl ein. Verteilen Sie dann die Konfigurationsänderungen auf die anderen StoreFront-Server in der Bereitstellung und starten Sie den Abonnementstoredienst neu.
    Remove-DSSubscriptionsSchedule -scheduleName synchronizationname
    synchronizationname ist der Name des Zeitplans, den Sie bei dessen Erstellung angegeben haben.

11. Um die derzeit für die StoreFront-Bereitstellung konfigurierten Zeitpläne der Abonnementsynchronisierung aufzulisten, geben Sie den folgenden Befehl ein.
    Get-DSSubscriptionsSyncScheduleSummary

Konfigurieren des optimalen HDX-Routings für einen Store

Wichtig: Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Wenn Sie die Änderungen vorgenommen haben, übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden.

Unterschied zwischen einer Farm und einer Zone beim Definieren optimaler Gatewayzuordnungen für einen Store

In StoreFront-Versionen vor 3.5 konnte ein optimales Gateway nur Farmen zugeordnet werden. Basierend auf dem Datencenter oder dem geografischen Standort der XenApp- oder XenDesktop-Controller und veröffentlichten Ressourcen können Sie nun XenApp 7.8- oder XenDesktop 7.8-Bereitstellungen in Zonen aufteilen. Zonen werden in XenApp oder XenDesktop 7.8 Studio definiert. StoreFront funktioniert nun mit XenApp 7.8 und XenDesktop 7.8. In StoreFront definierte Zonen müssen genau mit den in XenApp und XenDesktop definierten Zonennamen übereinstimmen.

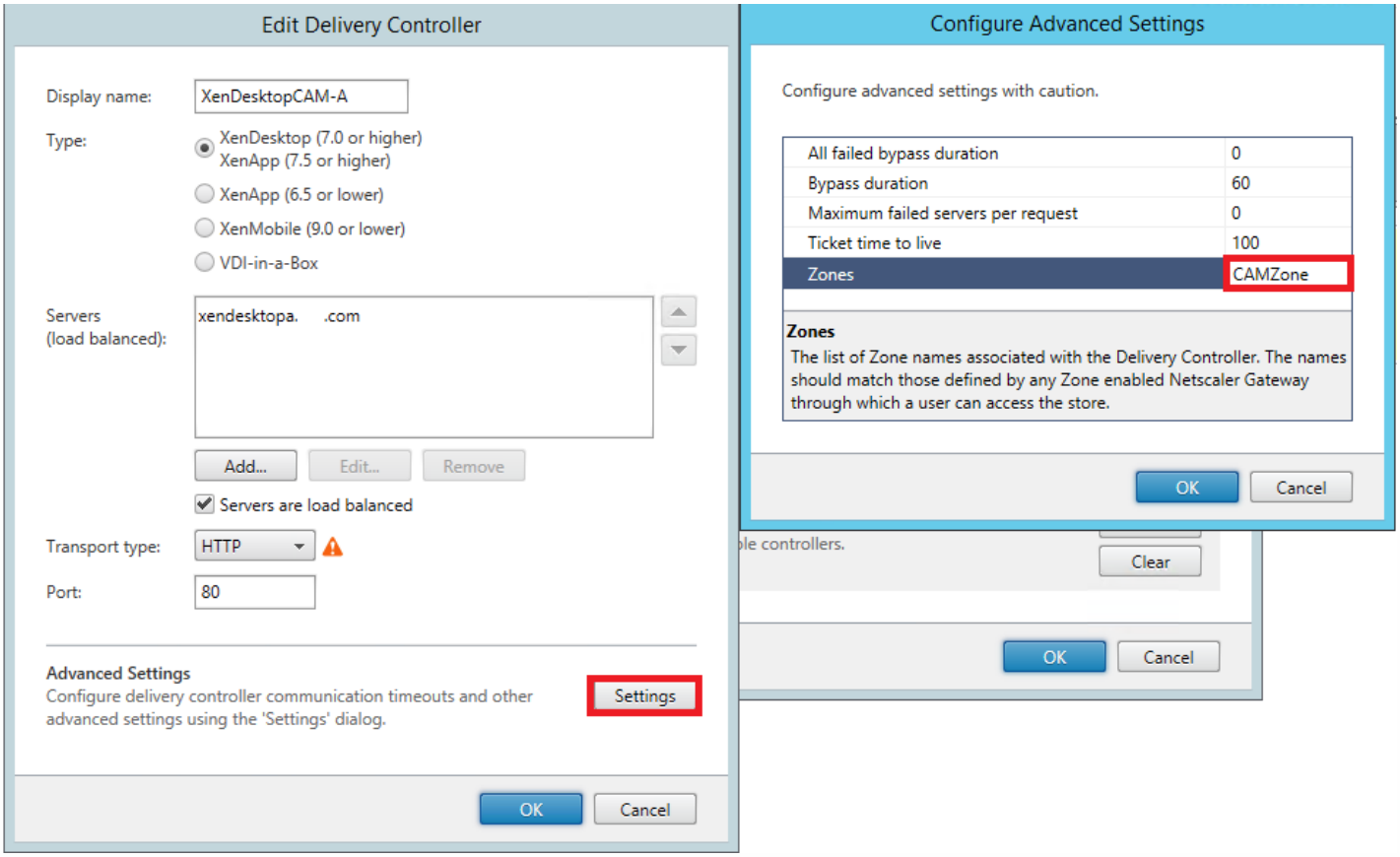
Mit dieser Version von StoreFront können Sie zudem eine optimale Gatewayzuordnung für alle Delivery Controller in der definierten Zone erstellen. Das Zuordnen einer Zone zu einem optimalen Gateway funktioniert fast genauso wie das Erstellen von Zuordnungen bei Farmen. Der einzige Unterschied ist, dass Zonen normalerweise viel größere Container mit viel mehr Delivery Controllern repräsentieren. Es ist nicht nötig, jeden Delivery Controller einer optimalen Gatewayzuordnung hinzuzufügen. Um die Delivery Controller in der gewünschten Zone zu platzieren, markieren Sie jeden Controller mit einem Zonennamen, der mit einer bereits in XenApp oder XenDesktop definierten Zone übereinstimmt. Ein optimales Gateway kann mehr als einer Zone zugeordnet werden, aber es empfiehlt sich, nur eine Zone zu verwenden. Eine Zone repräsentiert normalerweise ein Datencenter an einem geografischen Standort. Es wird erwartet, dass jede Zone mindestens ein optimales NetScaler Gateway hat, das für HDX-Verbindungen mit Ressourcen in der Zone verwendet wird.

Weitere Informationen zu Zonen finden Sie unter Zonen.

Platzieren eines Delivery Controllers in einer Zone

Legen Sie das Zonenattribut auf jedem Delivery Controller fest, den Sie in einer Zone platzieren.

1. Klicken Sie auf der Windows-Startseite oder auf der Seite **Apps** auf die Kachel **Citrix StoreFront**.
2. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores** und klicken Sie im Bereich **Aktionen** auf **Delivery Controller verwalten**.
3. Wählen Sie einen Controller, klicken Sie auf **Bearbeiten** und dann im Bildschirm **Delivery Controller bearbeiten** auf **Einstellungen**.
4. Klicken Sie in der Zeile **Zonen** auf die zweite Spalte.
5. Klicken Sie im Bildschirm **Delivery Controller Zonennamen** auf **Hinzufügen** und fügen Sie einen Zonennamen hinzu.



Konfigurieren Sie mit StoreFront das optimale NetScaler Gateway-Routing zum Optimieren der Handhabung von ICA-Verbindungsrouting von der HDX Engine zu veröffentlichten Ressourcen, wie XenDesktop-VDAs oder mit XenApp oder XenDesktop veröffentlichte Anwendungen. Normalerweise ist das optimale Gateway für eine Site am selben geografischen Standort.

Sie müssen optimale NetScaler Gateway-Geräte für Bereitstellungen nur definieren, wenn das Gerät, über das Benutzer auf StoreFront zugreifen, nicht das optimale Gateway ist. Wenn Starts über das Gateway, das die Startanforderung durchführt, zurückgeleitet werden sollen, macht StoreFront das automatisch.

Beispielszenario mit Farmen

1 x DE-Gateway –> 1 x DE-StoreFront	–> DE-lokale Apps und Desktops
	–> US Apps und Desktops ausschließlich für DE-Failover
1 x US-Gateway–> 1 x US-StoreFront	–> US-lokale Apps und Desktops
	–> DE Apps und Desktops ausschließlich für US-Failover

Ein DE-Gateway bietet Remotezugriff auf DE gehostete Ressourcen wie Apps und Desktops über DE-StoreFront.

Für das DE-StoreFront ist ein DE-basierter und ein US-basierter NetScaler Gateway definiert und sowohl DE- als auch US-Farmen sind auf seiner Delivery Controller-Liste. DE-Benutzer greifen über den Gateway, StoreFront und die Farmen, die sich am selben Standort befinden, auf Remoteressourcen zu. Wenn kein Zugriff auf die DE-Ressourcen möglich ist, können sie

als temporäre Failoverlösung auf US-Ressourcen zugreifen.

Ohne optimales Gateway-Routing würden alle ICA-Starts über das DE-Gateway geleitet, das die Startanforderung stellte, unabhängig vom geografischen Standort der Ressourcen. Standardmäßig werden die für die Startanforderungen verwendeten Gateways dynamisch von StoreFront identifiziert, wenn die Anforderung gestellt wird. Das optimale Gateway-Routing überschreibt die Standardeinstellung und erzwingt die Leitung von US-Verbindungen über das Gateway, das den US-Farmen, die die Apps und Desktops verfügbar machen, am nächsten ist.

Hinweis: Sie können für einen StoreFront-Store nur ein optimales Gateway pro Site zuordnen.

Beispielszenario mit Zonen

1 x CAMZone -> 2 x UK-StoreFronts	-> Cambridge, UK: Apps und Desktops -> Fort Lauderdale, Ost-USA: Apps und Desktops -> Bangalore, Indien: Apps und Desktops
1 x FTLZone -> 2 x USA-StoreFronts	-> Fort Lauderdale, Ost-USA: Apps und Desktops -> Cambridge, UK: Apps und Desktops -> Bangalore, Indien: Apps und Desktops
1 x BGLZone -> 2 x IN-StoreFronts	-> Bangalore, Indien: Apps und Desktops -> Cambridge, UK: Apps und Desktops -> Fort Lauderdale, Ost-USA: Apps und Desktops

Abbildung 1 Suboptimales Gateway-Routing

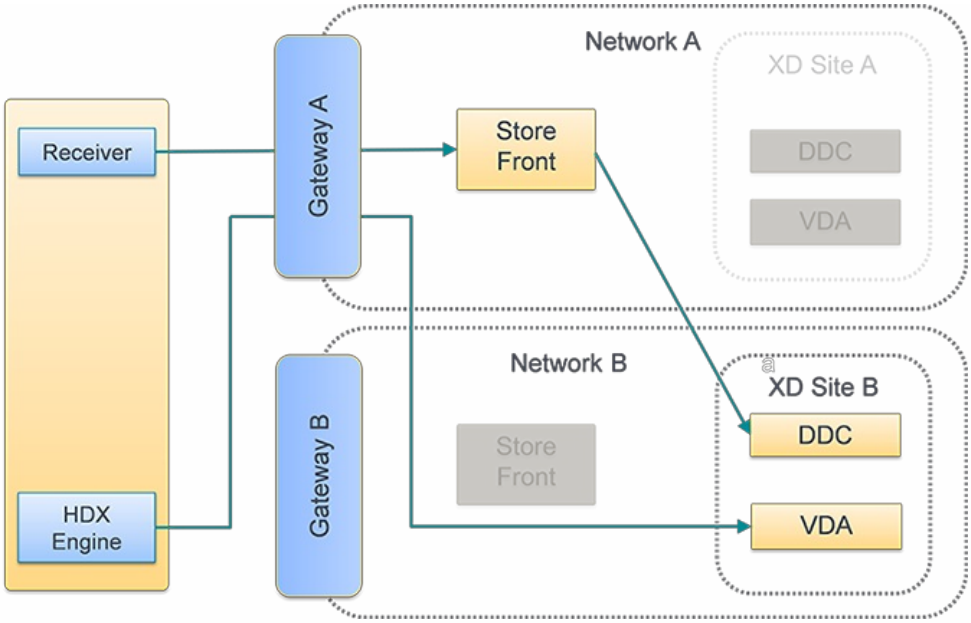
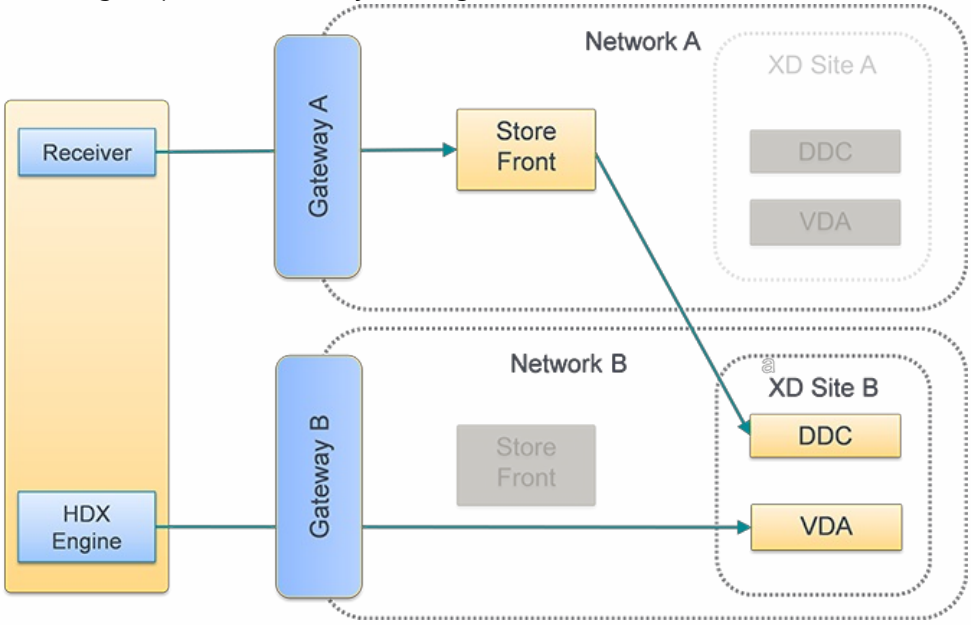


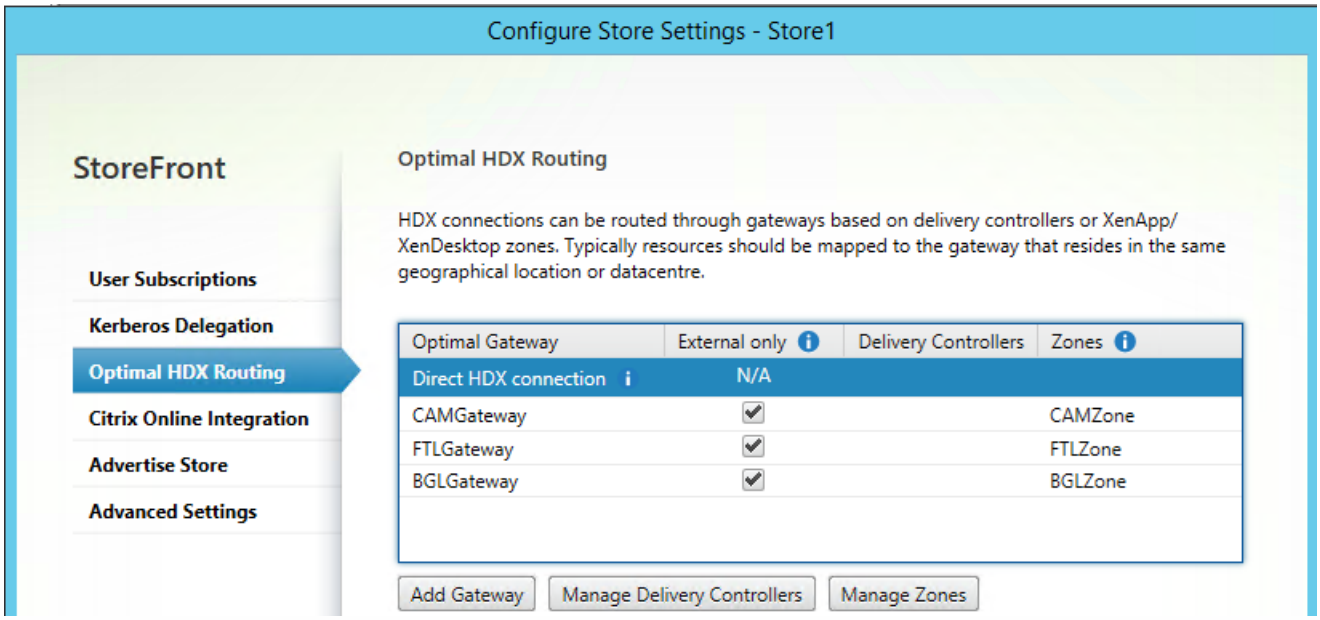
Abbildung 2 Optimales Gateway-Routing



Verwenden der Citrix StoreFront-Verwaltungskonsole

Wenn Sie separate NetScaler Gateway-Geräte für die Bereitstellungen konfiguriert haben, können Sie das optimale Gerät für den Zugriff auf die Bereitstellungen definieren.

1. Klicken Sie auf derWindows-Startseite oder auf der Seite **Apps** auf die Kachel **Citrix StoreFront**.
2. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores** und im Ergebnisbereich einen Store aus. Klicken Sie im Bereich **Aktionen** auf **Storeeinstellungen konfigurieren**.
3. Klicken Sie auf **Einstellungen** > **Optimales HDX-Routing** und wählen Sie ein Gateway aus.
4. Wenn Sie das Kontrollkästchen **Nur externe** aktivieren, entspricht es **-enabledOnDirectAccess = false**, und "Direkte HDX-Verbindung" entspricht der Verwendung von **Set-DSFarmsWithNullOptimalGateway** für Farmen oder Zonen.



Hinzufügen eines neuen Gateways

Im vorherigen Schritt gibt es auch die Option **Gateway hinzufügen**. Nach der Auswahl von **Gateway hinzufügen** wird der Bildschirm zum Hinzufügen eines NetScaler Gateways angezeigt.

1. Geben Sie im Bildschirm **Allgemeine Einstellungen** den Anzeigenamen, die NetScaler Gateway-URL und die Verwendung oder Rolle an, um für Benutzer, die über öffentliche Netzwerke eine Verbindung herstellen, den Zugriff auf Stores über NetScaler Gateway zu konfigurieren. Remotezugriff über NetScaler Gateway ist nicht für Stores ohne Authentifizierung möglich.
2. Treffen Sie im Bildschirm **Secure Ticket Authority (STA)** eine Auswahl unter den angezeigten Optionen.Die STA wird auf XenDesktop- und XenApp-Servern gehostet und gibt Sitzungstickets als Reaktion auf Verbindungsanforderungen aus. Auf diesen Sitzungstickets basiert die Authentifizierung und Autorisierung für den Zugriff auf XenDesktop- und XenApp-Ressourcen.
3. Legen Sie im Bildschirm **Authentifizierungseinstellungen** fest, wie Remotebenutzer ihre Anmeldeinformationen für die Authentifizierung angeben.

Konfigurieren des optimalen NetScaler Gateway-Routings für einen Store mit PowerShell

PowerShell-API-Parameter

Parameter	Description
-SiteId (Int)	Site-ID in IIS. Der Wert ist normalerweise 1 für die Site in IIS, wo StoreFront standardmäßig installiert ist.
-ResourcesVirtualPath (String)	Pfad für den Store, der konfiguriert werden muss, damit eine Farm zur optimalen Gateway-Zuordnung verwendet werden kann. Beispiel: "/Citrix/Store"
-GatewayName (String)	Name zum Identifizieren von NetScaler Gateway innerhalb von StoreFront. Beispiel 1: ExternalGateway Beispiel 2: InternalGateway
	Dient zur Angabe des vollqualifizierten Domänennamens (FQDN) und des Ports des optimalen NetScaler

Parameter	Beschreibung
(Zeichenfolgenarray)	Beispiel 1 für den vServer-Standardport 443: gateway.example.com Beispiel 2 für den nicht standardmäßigen vServer-Port 500: gateway.example.com:500
-Farms (Zeichenfolgenarray)	Gibt einen Satz (normalerweise am selben Standort) XenDesktop-, XenApp- und App Controller-Bereitstellungen an, die ein optimales NetScaler Gateway-Gerät gemeinsam verwenden. Eine Farm kann nur einen oder mehrere Delivery Controller enthalten, der bzw. die veröffentlichte Ressourcen bereitstellen. Sie können eine XenDesktop-Site in StoreFront unter "Delivery Controller" als "XenDesktop" konfigurieren. Dies repräsentiert eine einzelne Farm. Sie kann mehrere Delivery Controller in ihrer Failover-Liste enthalten: Beispiel: "XenDesktop" XenDesktop-A.example.com XenDesktop-B.example.com XenDesktop-C.example.com
-Zones (Zeichenfolgenarray)	Gibt ein oder mehrere Datencenter an, in denen viele Delivery Controller sind. Dazu müssen Sie Delivery Controller-Objekte in StoreFront mit der entsprechenden Zone markieren, der Sie die Controller zuordnen.
-staUrls (String Array)	Dient zur Angabe der URLs für XenDesktop- und XenApp-Server, auf denen die Secure Ticket Authority (STA) ausgeführt wird. Wenn Sie mehrere Farmen verwenden, listen Sie die jeweiligen STA-Server durch Kommas getrennt auf: Beispiel: "http://xenapp-a.example.com/scripts/ctxsta.dll","http://xendesktop-a.example.com/scripts/ctxsta.dll"
-StasUseLoadBalancing (Boolean)	Wert ist "true": Sitzungstickets werden nach dem Zufallsprinzip aus allen STAs abgerufen, sodass alle Anforderungen gleichmäßig über alle STAs verteilt werden. Wert ist "false": Benutzer werden mit der ersten verfügbaren STA verbunden, und zwar in der Reihenfolge, in der diese in der Konfiguration aufgelistet sind. Auf diese Weise wird die Anzahl gleichzeitig verwendeter STAs minimiert.
-StasBypassDuration	Legen Sie den Zeitraum in Stunden, Minuten und Sekunden fest, für den eine STA im Anschluss an eine fehlgeschlagene Anforderung als nicht verfügbar gilt. Beispiel: 02:00:00
-EnableSessionReliability (Boolean)	Wert ist "true": Getrennte Sitzungen bleiben geöffnet, während Receiver versucht, die Verbindung automatisch wiederherzustellen. Wenn Sie mehrere STAs konfiguriert haben und sicherstellen möchten, dass Sitzungszuverlässigkeit immer verfügbar ist, setzen Sie den Wert des Attributs useTwoTickets auf true fest, um Tickets von zwei verschiedenen STAs zu erhalten, falls eine STA während der Sitzung ausfällt.
-UseTwoTickets (Boolean)	Wert ist "true": Sitzungstickets werden von zwei verschiedenen STAs abgerufen, falls eine STA während der Sitzung ausfällt. Wert ist "false": Es wird nur ein STA-Server verwendet.
-EnabledOnDirectAccess (Boolean)	Wert ist "true": Stellt sicher, dass die Verbindungen zu Ressourcen weiterhin durch das optimale, für die Farm festgelegte Gerät geleitet werden, wenn lokale Benutzer im internen Netzwerk sich direkt bei StoreFront anmelden. Wert ist "false": Die Verbindungen zu Ressourcen werden nicht durch das optimale, für die Farm festgelegte Gerät geleitet, es sei denn, Benutzer greifen auf StoreFront über NetScaler Gateway zu.

Wenn PowerShell-Skripts wie unten dargestellt mehrere Zeilen umfassen, muss jede Zeile mit einem Graviszeichen enden.

Citrix empfiehlt, Codebeispiele in Windows PowerShell Integrated Scripting Environment (ISE) zu kopieren, um den PowerShell-Code vor dem Ausführen mit der Formatprüfung zu verifizieren.

Konfigurieren eines optimalen Gateways für eine Farm

> **Hinweis**
>
> Die Konfiguration des optimalen HDX-Routings mit dem alten PowerShell-Cmdlet "Set-DSOptimalGatewayForFarms" funktioniert nicht.
>
> So umgehen Sie dieses Problem:
>
> 1. Konfigurieren Sie ein globales Gateway mit den gewünschten Einstellungen für optimales HDX-Routing. Verwenden Sie dazu den Befehl "Add-DSGlobalV10Gateway" und Standardwerte für die Authentifizierungseinstellungen.
> 2. Fügen Sie die optimale Gatewaykonfiguration mit dem Befehl Add-DSStoreOptimalGateway hinzu.
>
> Beispiel:
>
> Add-DSGlobalV10Gateway -Id 2eba0524-af40-421e-9c5f-a1ccca80715f -Name LondonGateway -Address "http://example" -Logon Domain -SecureTicketAuthorityUrls @("http://staurl1", "http://staurl2")
>
> Add-DSStoreOptimalGateway -SiteId 1 -VirtualPath /Citrix/Store1 -GatewayId 2eba0524-af40-421e-9c5f-a1ccca80715f -Farms @("Controller") -EnabledOnDirectAccess $true

Beispiel:

Erstellen oder überschreiben Sie die Zuordnungen optimaler Gateways für Farmen für den Store **Internal**.

```
& "$Env:PROGRAMFILES\Citrix\Receiver StoreFront\Scripts\ImportModules.ps1"

Set-DSOptimalGatewayForFarms -SiteId 1 `

        -ResourcesVirtualPath /Citrix/Internal `
        -GatewayName "gateway1" `
        -Hostnames "gateway1.example.com:500" `
        -Farms "XenApp","XenDesktop" `
        -StaUrls
        "https://xenapp.example.com/scripts/ctxsta.dll","https://xendesktop.example.com/scripts/ctxsta.dll" `
        -StasUseLoadBalancing:$false `
        -StasBypassDuration 02:00:00 `
        -EnableSessionReliability:$false `
        -UseTwoTickets:$false `
        -EnabledOnDirectAccess:$true
```

Konfigurieren eines optimalen Gateways für eine Zone

Beispiel:

Erstellen oder überschreiben Sie die Zuordnungen optimaler Gateways für Farmen für die Zone "CAMZone".

```
& "$Env:PROGRAMFILES\Citrix\Receiver StoreFront\Scripts\ImportModules.ps1"

Set-DSOptimalGatewayForFarms -SiteId 1 `

        -ResourcesVirtualPath /Citrix/Internal `
        -GatewayName "gateway1" `
        -Hostnames "gateway1.example.com:500" `
        -Zones "CAMZone" `
        -StaUrls
        "https://xenapp.example.com/scripts/ctxsta.dll","https://xendesktop.example.com/scripts/ctxsta.dll" `
        -StasUseLoadBalancing:$false `
        -StasBypassDuration 02:00:00 `
        -EnableSessionReliability:$false `
        -UseTwoTickets:$false `
        -EnabledOnDirectAccess:$true
```

Beispiel:

Dieses Skript gibt alle optimalen Gateways für Farmzuordungen für den Store "Internal" zurück.

```
Get-DSOptimalGatewayForFarms -SiteId 1 –ResourcesVirtualPath "/Citrix/Internal"
```

Beispiel:

Entfernen Sie alle optimalen Gateways für Farmzuordungen für den Store namens "Internal".

```
Remove-DSOptimalGatewayForFarms -SiteId 1 -ResourcesVirtualPath "/Citrix/Internal"
```

Konfigurieren direkter HDX-Verbindungen für Farmen

Beispiel:

Dieses Skript verhindert für den Store "Internal", dass ICA-Starts für die angegebenen Farmen ein Gateway passieren.

```
Set-DSFarmsWithNullOptimalGateway -SiteId 1 -ResourcesVirtualPath /Citrix/Store -Farms "Farm1","Farm2"
```

Beispiel:

Dieses Skript gibt alle Farmen zurück, die so konfiguriert sind, dass ICA-Starts am Passieren eines Gateways für den Store "Internal" gehindert werden.

```
Get-DSFarmsWithNullOptimalGateway -SiteId 1 -ResourcesVirtualPath "/Citrix/Internal"
```

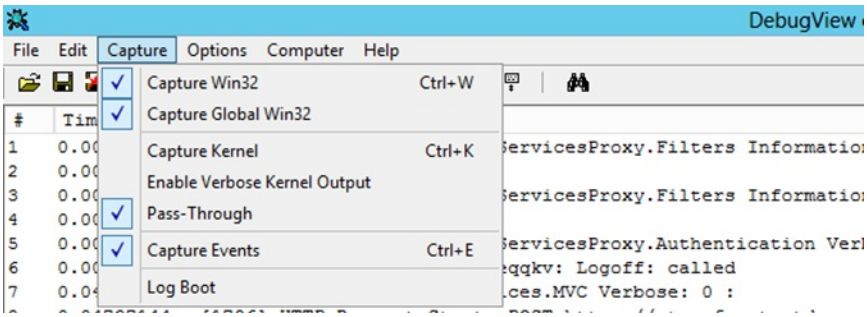
Ermitteln, ob optimale Gateways für Farmzuordungen von StoreFront verwendet werden

1. Aktivieren Sie StoreFront-Ablaufverfolgung auf allen Servergruppenknoten, die PowerShell ausführen, indem Sie Folgendes ausführen:

   ```
   & "$Env:PROGRAMFILES\Citrix\Receiver StoreFront\Scripts\ImportModules.ps1"

   #Traces output is to c:\Program Files\Citrix\Receiver Storefront\admin\trace\
   Set-DSTraceLevel -All -TraceLevel Verbose
   ```


2. Öffnen Sie auf dem Desktop eines StoreFront-Servers das Programm "DebugView". Wenn Sie eine StoreFront-Servergruppe verwenden, müssen Sie diese Schritte möglicherweise für alle Knoten ausführen, damit Sie den Ablauf des Knotens verfolgen können, der die Startanforderungen erhält.
3. Aktivieren Sie die Option "Capture Global Win32".



4. Speichern Sie die Ausgabe der Ablaufverfolgung als LOG-Datei und öffnen Sie die Datei mit dem Editor. Suchen Sie nach den Einträgen, die in den Beispielszenarios unten angezeigt werden.
5. Deaktivieren Sie die Ablaufverfolgung danach, da sie sehr viel Speicherplatz auf den StoreFront-Servern benötigt.
   Set-DSTraceLevel -All -TraceLevel Off

   Getestete optimale Gateway-Szenarios

   - Ein externer Client meldet sich an **Gateway1** an. Der Start wird über das dedizierte optimale Gateway **Gateway2** für die Farm **Farm2** geleitet.
     Set-DSOptimalGatewayForFarms -onDirectAccess=false

     Farm2 ist zur Verwendung des optimalen Gateways "Gateway2" konfiguriert.

     Für Farm2 ist das optimale Gateway bei direktem Zugriff deaktiviert.

     Das optimale Gateway "Gateway2" wird für den Start verwendet.

   - Ein interner Client meldet sich über StoreFront an. Der Start wird über das dedizierte optimale Gateway "Gateway1" für die Farm "Farm1" geleitet.
     Set-DSOptimalGatewayForFarms -onDirectAccess=true

     Kein dynamisch identifiziertes Gateway wird angefordert. StoreFront wurde direkt kontaktiert.

     Farm1 ist zur Verwendung des optimalen Gateways Gateway1 konfiguriert.

     Für Farm1 ist das optimale Gateway bei direktem Zugriff aktiviert.

     Das optimale Gateway "Gateway1" wird für den Start verwendet.

   - Ein interner Client meldet sich über Gateway1 an. Die Starts von Ressourcen auf Farm1 können keinen Gateway passieren und StoreFront wird direkt kontaktiert.
     Set-DSFarmsWithNullOptimalGateway

     Angefordertes dynamisch identifiziertes Gateway: Gateway1.

     Farm1 ist nicht zum Verwenden eines Gateways konfiguriert. Zum Start wird kein Gateway verwendet.

Integration in NetScaler Gateway und NetScaler

Nov 27, 2017

Durch Verwendung von NetScaler Gateway mit StoreFront können Sie Benutzern außerhalb des Unternehmensnetzwerks einen sicheren Remotezugriff ermöglichen, während NetScaler für den Lastausgleich eingesetzt werden kann.

Planen des Einsatzes von Gateway- und Serverzertifikaten

Die Integration von NetScaler Gateway und NetScaler in StoreFront erfordert einen Plan für den Einsatz von Gateways und Serverzertifikaten. Überlegen Sie, welche Citrix Komponenten Serverzertifikate in der Bereitstellung benötigen:

- Planen Sie die Beschaffung von Zertifikaten für internetseitige Server und Gateways von externen Zertifizierungsstellen. Clientgeräte vertrauen von einer internen Zertifizierungsstelle signierten Zertifikaten möglicherweise nicht automatisch.
- Planen Sie die Namen externer und interner Server. Viele Organisationen führen getrennte Namespaces für die interne und die externe Verwendung (z. B. "example.com" für extern und "example.net" für intern). Ein einzelnes Zertifikat kann bei Verwendung der SAN-Erweiterung (Subject Alternative Name) Namen beider Art enthalten. Hiervon wird in der Regel abgeraten. Eine öffentliche Zertifizierungsstelle stellt nur dann ein Zertifikat aus, wenn die Top-Level-Domäne (TLD) bei IANA registriert ist. In diesem Fall können einige häufig verwendete interne Namen (z. B. "example.local") nicht verwendet werden und es sind separate Zertifikate für externe und interne Namen erforderlich.
- Verwenden Sie nach Möglichkeit separate Zertifikate für externe und interne Server. Ein Gateway kann mehrere Zertifikate durch Binden eines eigenen Zertifikats an jede Schnittstelle unterstützen.
- Verwenden Sie nicht dasselbe Zertifikat für internetseitige und nicht internetseitige Server. Solche Zertifikate unterscheiden sich in der Regel bezüglich Gültigkeitsdauer und Sperrrichtlinien von den Zertifikaten, die Ihre internen Zertifizierungsstellen ausstellen.
- Verwenden Sie das gleiche Platzhalterzertifikat nur für äquivalente Dienste. Verwenden Sie nicht dasselbe Zertifikat für verschiedene Servertypen (z. B. StoreFront-Server und andere Servertypen). Verwenden Sie nicht dasselbe Zertifikat für Server, die verschiedenen Verwaltungsfunktionen unterstehen oder unterschiedliche Sicherheitsrichtlinien haben. Beispiele für Server mit äquivalenten Diensten:
  - StoreFront-Servergruppe und der für deren Lastenausgleich verwendete Server
  - Gruppe internetseitiger Gateways im GSLB
  - Gruppe von XenApp- und XenDesktop 7.x-Controller, die äquivalente Ressourcen bereitstellen
- Planen Sie eine durch Hardware geschützte Speicherung privater Schlüssel. Bei Gateways und Servern, einschließlich einigen NetScaler-Modellen, ist die sichere Speicherung privater Schlüssel in einem Hardwaresicherheitsmodul (HSM) oder Trusted Platform Module (TPM) möglich. Aus Sicherheitsgründen sind diese Konfigurationen in der Regel nicht für die gemeinsame Nutzung von Zertifikaten und ihren privaten Schlüssel vorgesehen (siehe Dokumentation der einzelnen Komponenten). Wenn Sie GSLB mit NetScaler Gateway implementieren, erfordert eventuell jedes Gateway in GSLB ein identisches Zertifikat, das alle verwendeten FQDNs enthält.

Weitere Informationen zum Schützen der Citrix Bereitstellung finden Sie in dem Whitepaper End-To-End Encryption with XenApp and XenDesktop und dem Abschnitt Sicherheit der Dokumentation zu XenApp und XenDesktop.

Hinzufügen einer NetScaler Gateway-Verbindung

Jun 04, 2018

Verwenden Sie die Aufgabe NetScaler Gateway-Gerät hinzufügen zum Hinzufügen von NetScaler Gateway-Bereitstellungen, über die Benutzer auf Ihre Stores zugreifen können. Sie müssen die Passthrough-Authentifizierungsmethode von NetScaler Gateway aktivieren, um Remotezugriff auf die Stores über NetScaler Gateway konfigurieren zu können. Weitere Informationen über die Konfiguration von NetScaler Gateway für StoreFront finden Sie unter Using WebFront to Integrate with StoreFront.

Wichtig: Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Wenn Sie die Änderungen vorgenommen haben, übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden.

1. Klicken Sie auf der Windows-Startseite oder auf der Apps-Seite auf die Kachel Citrix StoreFront.
2. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten Stores aus und klicken Sie im Aktionsbereich auf Authentifizierungsmethoden verwalten.
3. Klicken Sie auf **Hinzufügen** gefolgt von Allgemeine Einstellungen und geben Sie einen Namen für die NetScaler Gateway-Bereitstellung an, über den die Benutzer sie erkennen können.
   Benutzern wird der Anzeigename angezeigt, den Sie in Citrix Receiver angegeben haben. Nehmen Sie deshalb relevante Informationen in den Namen auf, damit Benutzer leichter entscheiden können, ob sie die Bereitstellung verwenden möchten. Beispielsweise können Sie den geographischen Standort in die Anzeigenamen der NetScaler Gateway-Bereitstellungen einfügen, damit Benutzer problemlos das beste Gateway für ihren Standort identifizieren können.

4. Geben Sie die URL des virtuellen Servers oder Benutzeranmeldepunkts (für Access Gateway 5.0) für die Bereitstellung an. Geben Sie die Produktversion Ihrer Bereitstellung an.
   Der vollqualifizierte Domänenname (FQDN) für die StoreFront-Bereitstellung muss eindeutig sein und darf nicht dem vollqualifizierten Domänennamen des virtuellen NetScaler Gateway-Servers entsprechen. Das Verwenden des selben vollqualifizierten Domänennamens für StoreFront und den virtuellen NetScaler Gateway-Server wird nicht unterstützt.

5. Wenn Sie eine Access Gateway 5.0-Bereitstellung hinzufügen, fahren Sie mit Schritt 7 fort. Andernfalls und geben Sie ggf. die Subnetz-IP-Adresse des NetScaler Gateway-Geräts an. Eine Subnetz IP-Adresse ist für Access Gateway 9.3-Geräte erforderlich, aber für neuere Produktversionen optional.
   Die Subnetzadresse ist die IP-Adresse, durch die NetScaler Gateway für die Kommunikation mit Servern im internen Netzwerk das Benutzergerät darstellt. Dies kann es sich auch die zugeordnete IP-Adresse des NetScaler Gateway-Geräts sein. Wenn angegeben, verwendet StoreFront die Subnetz-IP-Adresse, um zu überprüfen, ob eingehende Anfragen von einem vertrauenswürdigen Gerät stammen.

6. Wenn Sie ein Gerät mit NetScaler Gateway hinzufügen, wählen Sie aus der Liste Anmeldetyp die Authentifizierungsmethode aus, die Sie auf dem Gerät für Benutzer von Citrix Receiver konfiguriert haben.
   Die von Ihnen angegebenen Informationen über die Konfiguration des NetScaler Gateway-Geräts wird der Provisioningdatei für den Store hinzugefügt. Dies ermöglicht, dass Citrix Receiver die entsprechende Verbindungsanforderung schickt, wenn das Gerät zum ersten Mal kontaktiert wird.

   - Wenn Benutzer die Domänenanmeldeinformationen für Microsoft Active Directory eingeben müssen, wählen Sie Domäne.
   - WählenSie Sicherheitstoken, wenn Benutzer einen Tokencode von einem Sicherheitstoken eingeben müssen.
   - WählenSie Domäne und Sicherheitstoken aus, wenn Benutzer ihre Domänenanmeldeinformationen und einen

Tokencode von einem Sicherheitstoken eingeben müssen.
- Wählen Sie SMS-Authentifizierung, wenn Benutzer ein in einer Textnachricht gesendetes Einmalkennwort eingeben müssen.
- Wenn Benutzer eine Smartcard vorlegen und eine PIN eingeben müssen, wählen Sie Smartcard.

Wenn Sie die Smartcardauthentifizierung mit einer sekundären Authentifizierungsmethode konfigurieren, auf die Benutzer zurückgreifen können, wenn es Probleme mit den Smartcards gibt, wählen Sie die sekundäre Authentifizierungsmethode aus der Liste Smartcard-Fallback. Fahren Sie mit Schritt 8 fort.

7. Zum Hinzufügen einer Access Gateway 5.0-Bereitstellung geben Sie an, ob der Anmeldepunkt auf einem eigenständigen Gerät gehostet wird. Wenn Sie ein Cluster hinzufügen, klicken Sie auf Weiter und fahren Sie mit Schritt 9 fort.
8. Wenn Sie StoreFront für NetScaler Gateway oder ein einzelnes Access Gateway 5.0-Gerät konfigurieren, geben Sie in das Feld Callback-URL die URL des NetScaler Gateway-Authentifizierungsdiensts ein. StoreFront fügt automatisch den Standardteil der URL an. Klicken Sie auf Weiter und gehen Sie zu Schritt 11.
   Geben Sie die intern zugängliche URL des Geräts ein. StoreFront kontaktiert den NetScaler Gateway-Authentifizierungsdienst, um zu überprüfen, ob von NetScaler Gateway empfangene Anforderungen auch tatsächlich von diesem Gerät ausgehen.
9. Zum Konfigurieren von StoreFront für ein Access Gateway 5.0-Cluster listen Sie auf der Seite Geräte die IP-Adressen oder vollqualifizierten Domänennamen der Geräte im Cluster auf und klicken Sie auf Weiter.
10. Listen Sie auf der Seite Authentifizierung ohne Benutzereingriff aktivieren die URLs für den Authentifizierungsdienst, der auf den Access Controller-Servern ausgeführt wird, auf. Geben zur Aktivierung der Fehlertoleranz URLs mehrerer Server ein und führen Sie die Server dabei in der Reihenfolge ihrer Priorität auf, um die Failoversequenz festzulegen. Klicken Sie auf Weiter.
    StoreFront authentifiziert Remotebenutzer über den Authentifizierungsdienst, damit sie ihre Anmeldeinformationen nicht neu eingeben müssen, wenn sie auf Stores zugreifen.
11. Alle Bereitstellungen: Wenn Sie Ressourcen von XenDesktop oder XenApp im Store verfügbar machen, listen Sie auf der Seite Secure Ticket Authority (STA) URLs für Server auf, auf denen die STA ausgeführt wird. Geben Sie aus Gründen der Fehlertoleranz URLs für mehrere STAs ein und führen Sie die Server dabei in der Reihenfolge ihrer Priorität auf, um die Failoversequenz festzulegen.
    Die STA wird auf XenDesktop- und XenApp-Servern gehostet und gibt Sitzungstickets als Reaktion auf Verbindungsanforderungen aus. Auf diesen Sitzungstickets basiert die Authentifizierung und Autorisierung für den Zugriff auf XenDesktop- und XenApp-Ressourcen.
12. Aktivieren Sie das Kontrollkästchen Sitzungszuverlässigkeit aktivieren, wenn XenDesktop und XenApp getrennte Sitzungen aufrechterhalten sollen, während Citrix Receiver eine automatische Wiederverbindung versucht. Aktivieren Sie das Kontrollkästchen Tickets von zwei Secure Ticket Authoritys anfordern (falls verfügbar), wenn Sie mehrere STAs konfiguriert haben und sicherstellen möchten, dass Sitzungszuverlässigkeit immer gegeben ist.
    Wenn das Kontrollkästchen Tickets von zwei Secure Ticket Authoritys anfordern (falls verfügbar) aktiviert ist, ruft StoreFront Tickets von zwei verschiedenen Secure Ticket Authoritys ab, damit Benutzersitzungen nicht unterbrochen werden, wenn eine Secure Ticket Authority während der Sitzung ausfällt. Wenn StoreFront aus irgendeinem Grund keine Verbindung zu zwei Secure Ticket Authoritys herstellen kann, wird automatisch nur eine Secure Ticket Authority verwendet.
13. Klicken Sie auf Erstellen, um Details der NetScaler Gateway-Bereitstellung hinzuzufügen. Nach der Bereitstellung hinzugefügt wurde, klicken Sie auf Fertig stellen.
    Weitere Informationen zum Aktualisieren der Details der Bereitstellungen finden Sie unter Konfigurieren von NetScaler Gateway-Verbindungseinstellungen.

Für den Zugriff auf Stores über NetScaler Gateway sind ein interner und mindestens zwei externe Beacons erforderlich. Citrix Receiver verwendet Beacons, um zu ermitteln, ob Benutzer mit einem lokalen oder öffentlichen Netzwerk verbunden sind, und wählt daraufhin die richtige Zugriffsmethode aus. Standardmäßig verwendet StoreFront die Server-URL oder die Lastausgleichs-URL der Bereitstellung als internen Beacon. Die URLs der Citrix Website und des virtuellen Servers oder Benutzeranmeldepunkts (Access Gateway 5.0) der zuerst hinzugefügten NetScaler Gateway-Bereitstellung werden standardmäßig als externe Beacons verwendet. Weitere Informationen zum Ändern der Beacons finden Sie unter Konfigurieren von Beacons.

Damit Benutzer auf Stores über NetScaler Gateway zugreifen können, stellen Sie sicher, dass Sie den Remotebenutzerzugriff für diese Stores konfigurieren.

Importieren eines NetScaler Gateways

Nov 27, 2017

Die Remotezugriffeinstellungen in der NetScaler-Verwaltungskonsole müssen mit denen in StoreFront identisch sein. In diesem Artikel wird erläutert, wie Sie ein NetScaler Gateway importieren, sodass NetScaler und StoreFront richtig für die Zusammenarbeit konfiguriert sind.

Anforderungen

- Zum Exportieren mehrerer virtueller Gateway-Server in eine ZIP-Datei ist NetScaler 11.1.51.21 oder höher erforderlich. **Hinweis**: NetScaler kann nur mit dem XenApp- und XenDesktop-Assistenten erstellte virtuelle Gateway-Server exportieren.
- Die Server-URLs aller STAs (Secure Ticket Authority) in der Datei GatewayConfig.json in der von NetScaler generierten ZIP-Datei müssen von DNS aufgelöst und von StoreFront kontaktiert werden können.
- Die Datei GatewayConfig.json in der von NetScaler generierten ZIP-Datei muss die URL einer Citrix Receiver für Web-Site auf dem StoreFront-Server enthalten. Ab NetScaler 11.1 wird dies gewährleistet, indem der StoreFront-Server kontaktiert und alle vorhandenen Stores und Citrix Receiver für Web-Sites aufgelistet werden, bevor die ZIP-Datei generiert wird.
- StoreFront muss unter Einsatz des importierten Gateways die Rückruf-URL in DNS in die IP-Adresse des virtuellen Gateway-VPN-Servers zur Authentifizierung auflösen können.

    Normalerweise wird für den Rückruf die gleiche Kombination aus URL und Port verwendet wie für das Gateway, vorausgesetzt, StoreFront kann diese URL auflösen.

    oder

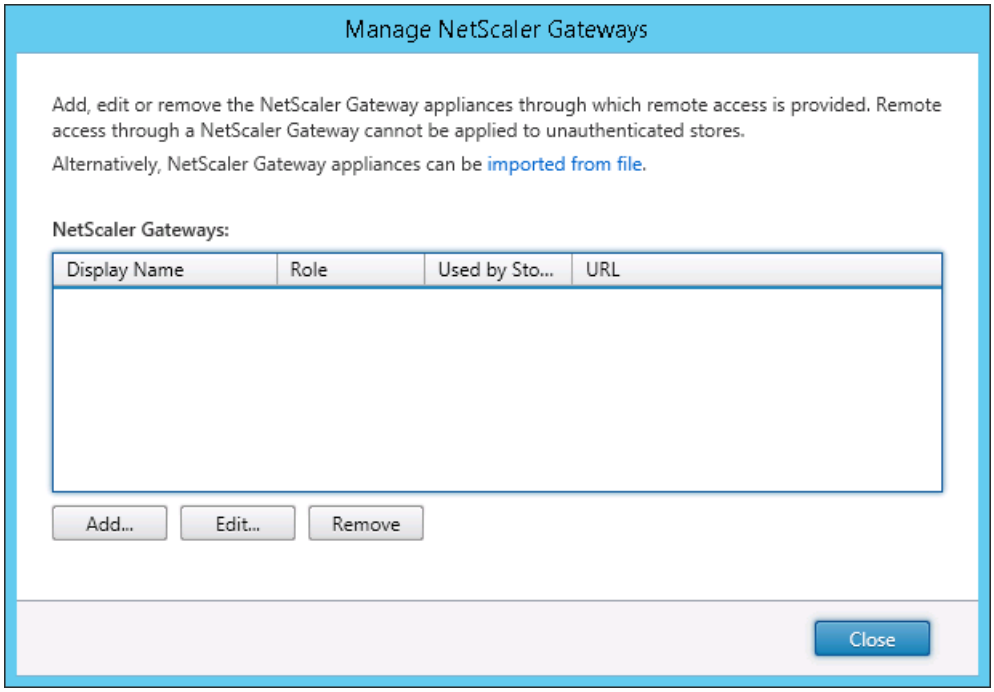
    Die Kombination aus URL und Port für den Rückruf darf sich von der für das Gateway unterscheiden, wenn Sie verschiedene externe und interne DNS-Namespaces in Ihrer Umgebung verwenden. Ist das Gateway in einer DMZ und hat eine -URL und StoreFront ist im privaten Unternehmensnetzwerk und hat eine -URL, können Sie eine -Rückruf-URL verwenden, die auf den virtuellen Gateway-Server in der DMZ verweist.

Importieren eines NetScaler Gateways mit der Konsole

Sie können ein oder mehrere NetScaler Gateway-Geräte importieren, indem Sie eine NetScaler-Konfigurationssdatei importieren.

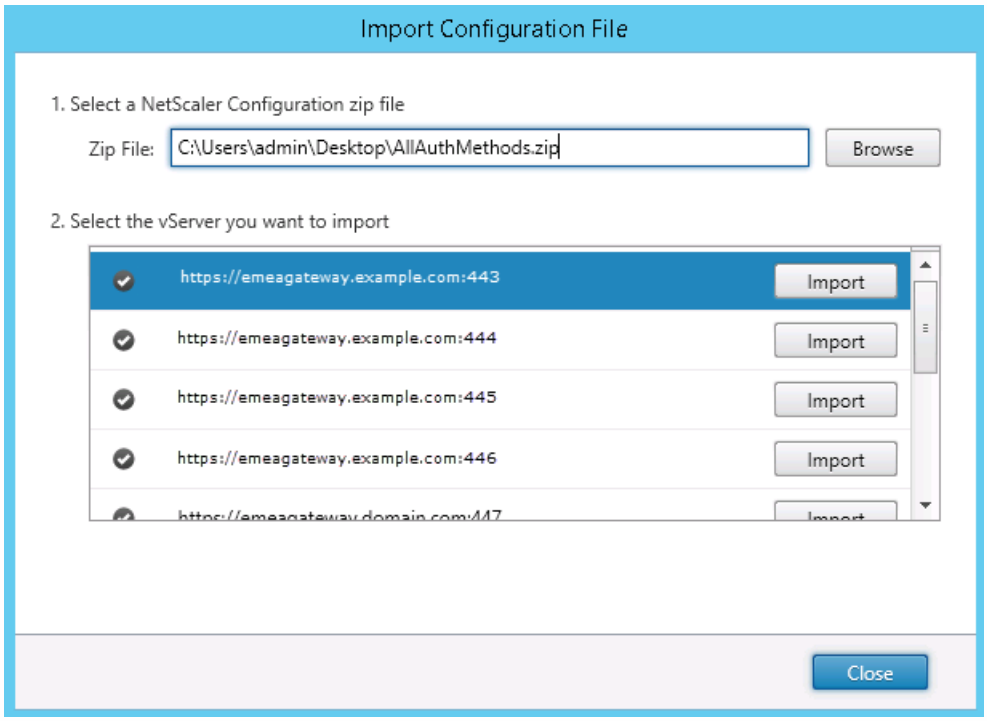
> ### Important
>
> Manuelles Bearbeiten der Konfigurationsdatei, die aus NetScaler exportiert wurde, wird nicht unterstützt.

1. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten**Stores** aus und klicken Sie im Aktionsbereich auf **Authentifizierungsmethoden verwalten**.
2. Klicken Sie auf dem Bildschirm **NetScaler Gateways verwalten** auf den Importiert-aus-Datei-Link.



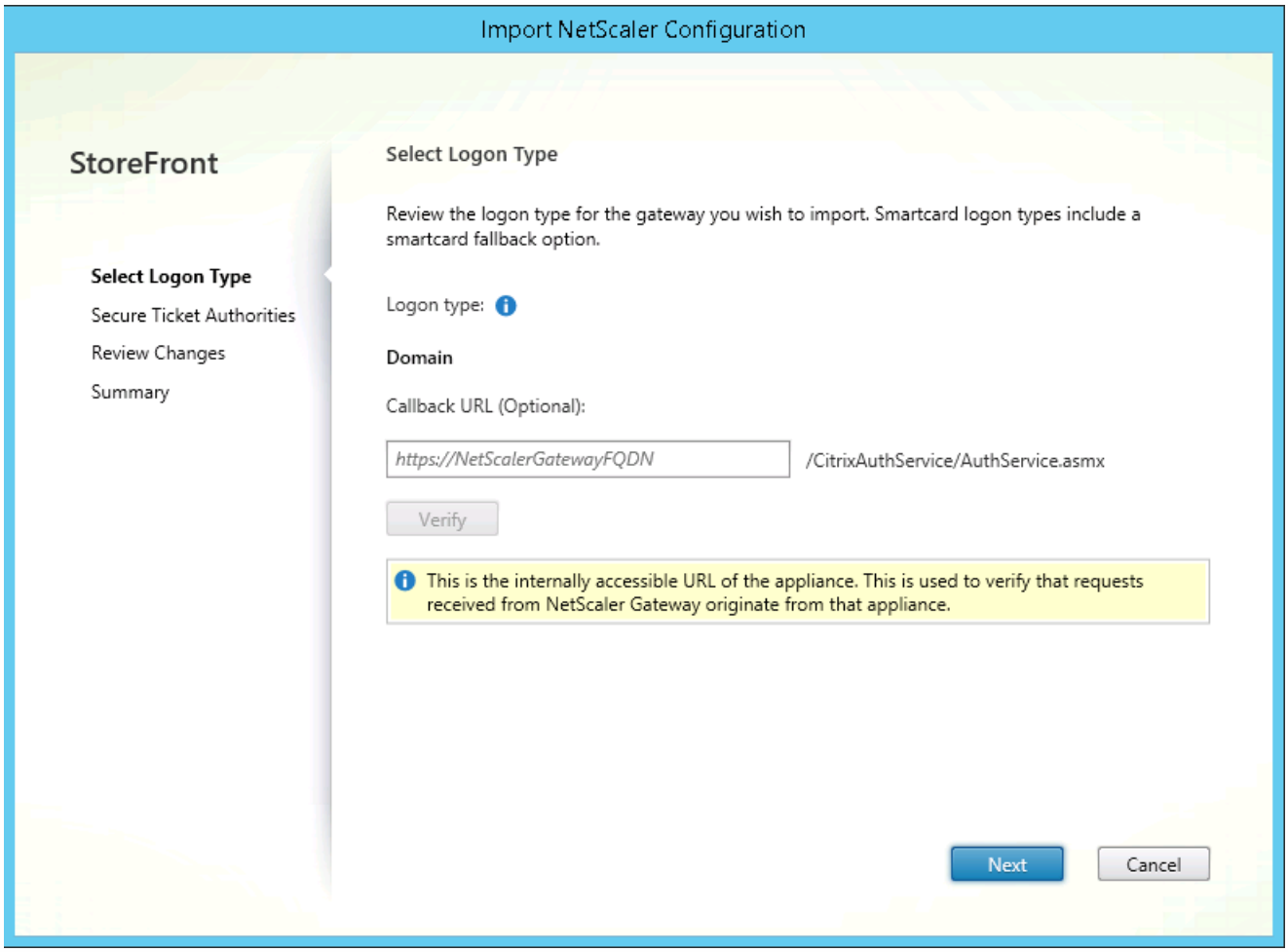
3. Navigieren Sie zur ZIP-Datei mit der NetScaler-Konfiguration.

4. Eine Liste der virtuellen Gateway-Server aus der ausgewählten ZIP-Datei wird angezeigt. Wählen Sie den gewünschten virtuellen Gateway-Server und klicken Sie auf **Importieren**. Wenn Sie den Import eines virtuellen Servers wiederholen, heißt die Schaltfläche "Update". Bei Auswahl von **Update** erhalten Sie später die Option, das Gateway zu überschreiben oder ein neues Gateway zu erstellen.



5. Überprüfen Sie den Anmeldetyp für das ausgewählte Gateway und geben Sie bei Bedarf eine Rückruf-URL an. Der Anmeldetyp ist die Authentifizierungsmethode, die Sie auf dem Netscaler Gateway-Gerät für Benutzer von Citrix Receiver konfiguriert haben. Einige Anmeldetypen erfordern Rückruf-URLs (siehe Tabelle).

- Klicken Sie auf **Überprüfen**, um zu prüfen, ob die Rückruf-URL gültig und vom StoreFront-Server erreichbar ist.



Anmeldetyp in der Konsole	LogonType in der JSON-Datei	Rückruf-URL erforderlich
Domäne	Domäne	Nein
Domäne und Sicherheitstoken	DomainAndRSA	Nein
Sicherheitstoken	RSA	Ja
Smartcard - Kein Fallback	SmartCard	Ja
Smartcard - Domäne	SmartCardDomain	Ja
Smartcard - Domäne und Sicherheitstoken	SmartCardDomainAndRSA	Ja
Smartcard - Sicherheitstoken	SmartCardRSA	Ja
Smartcard - SMS-Authentifizierung	SmartCardSMS	Ja

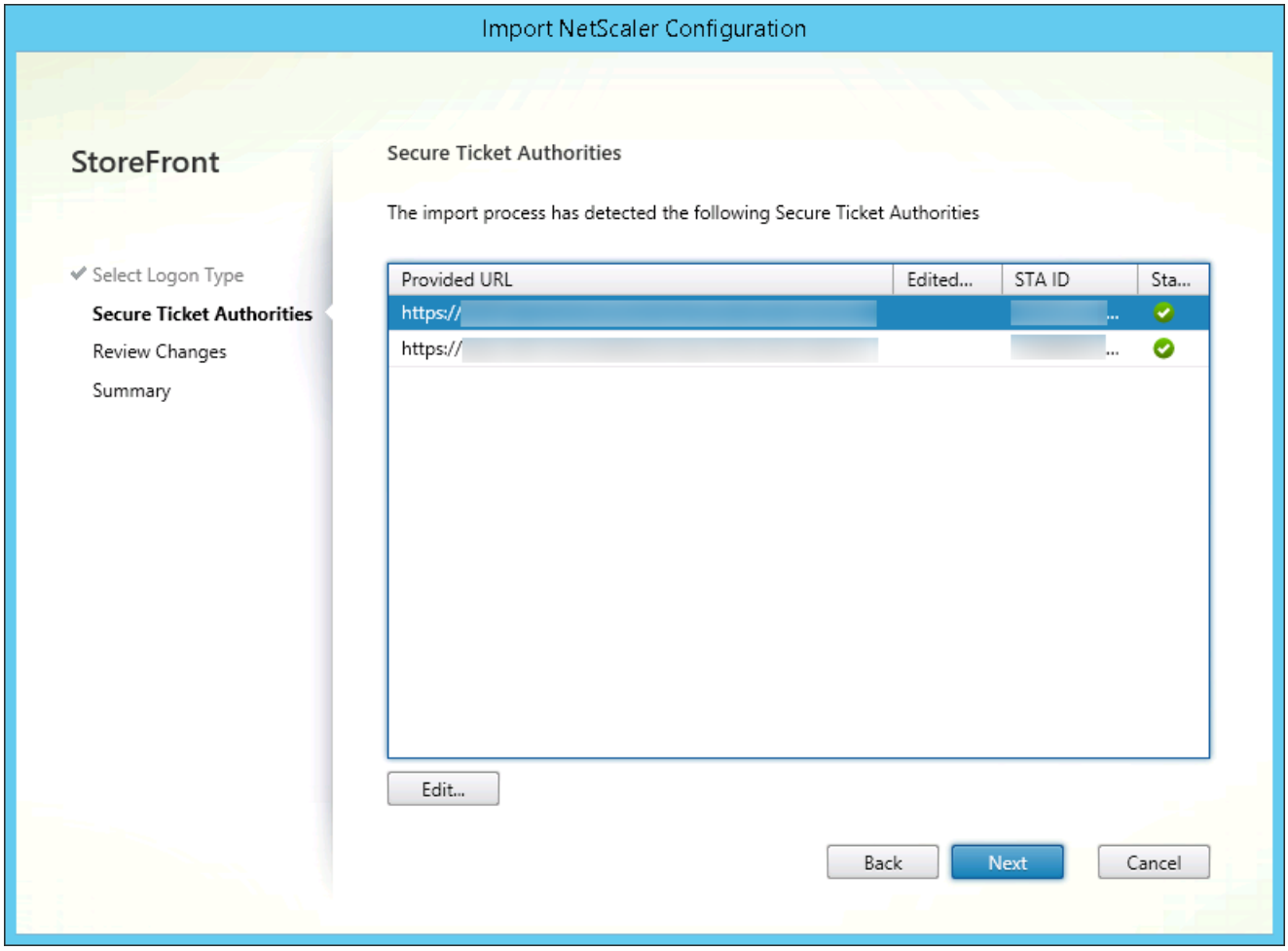
SMS-Authentifizierung	SMS	Ja

Wenn eine Rückruf-URL erforderlich ist, wird sie automatisch basierend auf der Gateway-URL in der ZIP-Datei eingetragen. Sie können sie in eine beliebige gültige URL ändern, die auf die IP-Adresse des virtuellen NetScaler Gateway-Servers verweist.

Wenn Sie SmartAccess verwenden möchten, ist eine Rückruf-URL erforderlich.

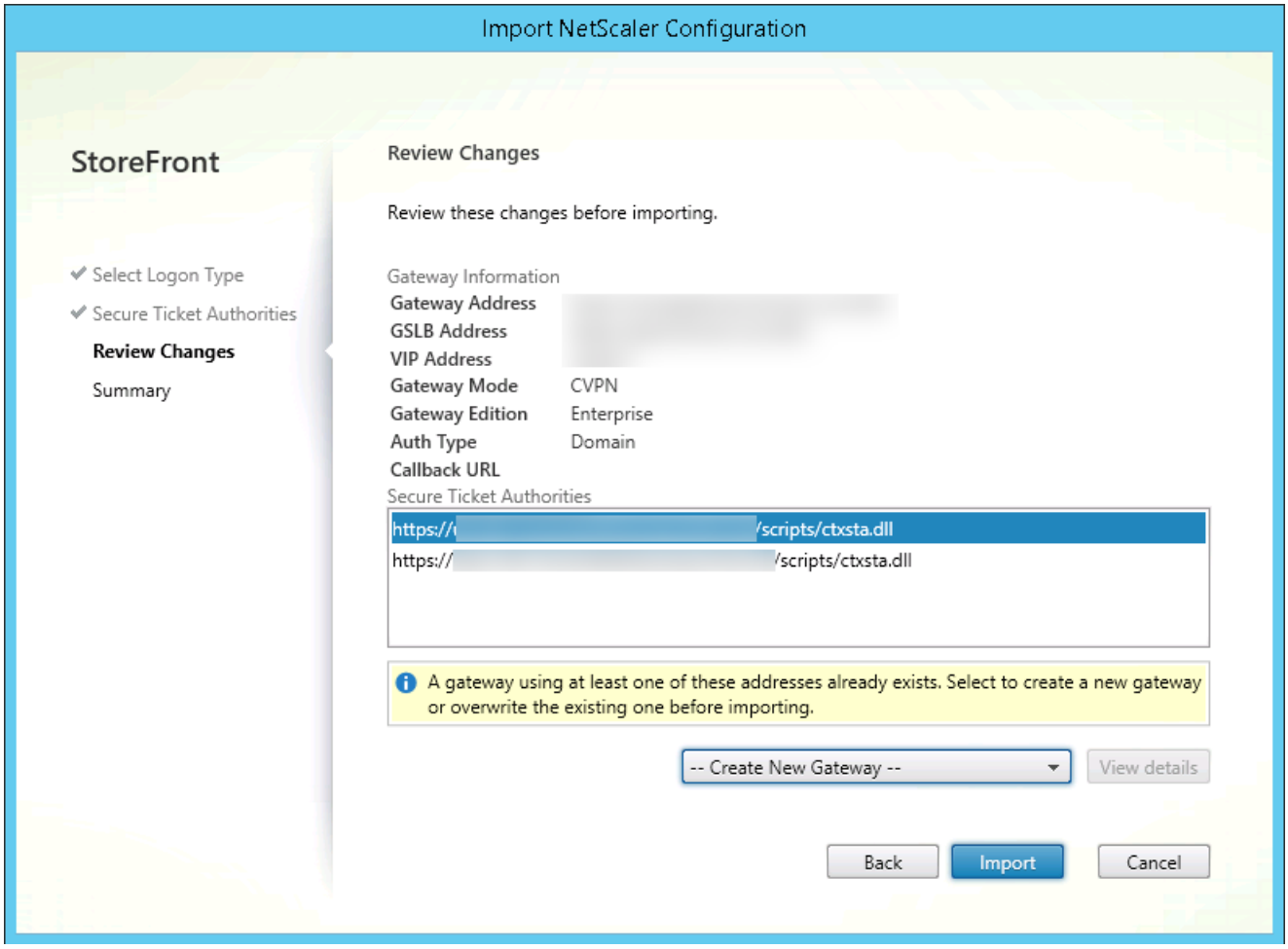
6. Klicken Sie auf **Weiter**.

7. StoreFront kontaktiert über DNS alle STA-Server-URLs (Secure Ticket Authority), die in die ZIP-Datei aufgelistet sind, und prüft, ob es sich um funktionierende STA-Ticketing-Server handelt. Der Import wird nicht fortgesetzt, wenn eine STA-URL ungültig ist.



8. Klicken Sie auf **Weiter**.

9. Überprüfen Sie die Details für den Import. Wenn ein Gateway mit der gleichen URL-/Portkombination (Gateway:port) vorhanden ist, verwenden Sie das Dropdownmenü zur Auswahl eines Gateways zum Überschreiben oder Erstellen eines neuen Gateways.



StoreFront prüft anhand der GatewayURL:port-Kombination, ob ein Gateway, das Sie importieren möchten, einem vorhandenen Gateway entspricht, das aktualisiert werden soll. Hat ein Gateway eine andere GatewayURL:port-Kombination, wird es als neues Gateway behandelt. Die folgende Tabelle zeigt, welche Gateway-Einstellungen Sie aktualisieren können.

Gateway-Einstellungen	**Aktualisierbar**
Gateway-URL:Port-Kombination	Nein
GSLB-URL	Ja
Zertifikat und Fingerabdruck der Netscaler-Vertrauensstellung	Ja
Rückruf-URL	Ja
URL der Receiver für Web-Site	Ja
Gatewayadresse/-VIP	Ja

URL und ID der Secure Ticket Authority	Ja
Alle Anmeldetypen	Ja

10.Klicken Sie auf **Importieren**. Wenn der StoreFront-Server Teil einer Servergruppe ist, erinnert Sie eine Meldung daran, die importierten Gateway-Einstellungen auf die anderen Server in der Gruppe zu übertragen.

11. Klicken Sie auf **Finish**.

Zum Importieren einer weiteren Konfiguration eines virtuellen Servers wiederholen Sie die Schritte oben.

> ## Hinweis
>
> Das Standardgateway eines Stores ist das Gateway, über das systemeigene Citrix Receiver eine Verbindung herstellen, es sei denn, sie sind zur Verwendung eines anderen Gateways konfiguriert. Wenn keine Gateways für den Store konfiguriert sind, wird das erste aus der ZIP-Datei importierte Gateway zum Standardgateway für die systemeigenenen Citrix Receiver. Durch den Import nachfolgender Gateways ändert sich nichts an dem für den Store festgelegten Standardgateway.

Importieren mehrerer NetScaler Gateways mit PowerShell

Read-STFNetScalerConfiguration

- Kopieren Sie die ZIP-Datei auf den Desktop des aktuell angemeldeten StoreFront-Administrators.
- Lesen Sie den Inhalt der NetScaler ZIP-Datei in den Speicher ein und suchen Sie die drei Gateways anhand ihrer Indexwerte.

command KOPIEREN

```
$ImportedGateways = Read-STFNetScalerConfiguration -path "$env:USERPROFILE\desktop\GatewayConfig.zip"
```

Zeigen Sie die drei Gateway-Objekte aus dem Netscaler-ZIP-Importpaket mit dem Cmdlet "STFNetScalerConfiguration" im Speicher an.

command KOPIEREN

```
$ImportedGateways.Document.Gateways[0]

$ImportedGateways.Document.Gateways[1]

$ImportedGateways.Document.Gateways[2]
```

```
GatewayMode           : CVPN
CallbackUrl           :
GslbAddressUri        : https://gslb.example.com/
AddressUri            : https://emeagateway.example.com/
Address               : https://emeagateway.example.com:443
GslbAddress           : https://gslb.example.com:443
VipAddress            : 10.0.0.1
Stas                  : {STA298854503, STA909374257}
StaLoadBalance        : True
CertificateThumbprints : {F549AFAA29EBF61E8709F2316B3981AD503AF387}
GatewayAuthType       : Domain
GatewayEdition        : Enterprise
ReceiverForWebSites   : {Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.ReceiverForWebSite}



GatewayMode           : CVPN
CallbackUrl           :
GslbAddressUri        : https://gslb.example.com/
AddressUri            : https://emeagateway.example.com/
Address               : https://emeagateway.example.com:444
```

```
GslbAddress           : https://gslb.example.com:443

VipAddress            : 10.0.0.2

Stas                  : {STA298854503, STA909374257}

StaLoadBalance        : True

CertificateThumbprints : {F549AFAA29EBF61E8709F2316B3981AD503AF387}

GatewayAuthType       : DomainAndRSA

GatewayEdition        : Enterprise

ReceiverForWebSites   : {Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.ReceiverForWebSite}



GatewayMode           : CVPN

CallbackUrl           : https://emeagateway.example.com:445

GslbAddressUri        : https://gslb.example.com/

AddressUri            : https://emeagateway.example.com/

Address               : https://emeagateway.example.com:445

GslbAddress           : https://gslb.example.com:443

VipAddress            : 10.0.0.2

Stas                  : {STA298854503, STA909374257}

StaLoadBalance        : True

CertificateThumbprints : {F549AFAA29EBF61E8709F2316B3981AD503AF387}

GatewayAuthType       :SmartCard
```

```
GatewayEdition         : Enterprise

ReceiverForWebSites    : {Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.ReceiverForWebSite}
```

Import-STFNetScalerConfiguration ohne Angabe einer Rückruf-URL

Kopieren Sie die ZIP-Datei auf den Desktop des aktuell angemeldeten StoreFront-Administrators.Lesen Sie das NetScaler ZIP-Importpaket in den Speicher ein und suchen Sie die drei Gateways anhand ihrer Indexwerte.

command KOPIEREN

```
$ImportedGateways = Read-STFNetScalerConfiguration -path "$env:USERPROFILE\desktop\GatewayConfig.zip"
```

Importieren Sie drei neue Gateways in StoreFront mit dem Cmdlet "Import-STFNetScalerConfiguration" und geben Sie die erforderlichen Gateway-Indizes an.Der Parameter "-Confirm:$False" verhindert, dass Sie von der Powershell zum Zulassen jedes einzelnen zu importierenden Gateways aufgefordert werden.Entfernen Sie den Parameter, wenn Sie Gateways sorgfältig einzeln importieren möchten.

command KOPIEREN

```
Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 0 -Confirm:$False

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 1 -Confirm:$False

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 2 -Confirm:$False
```

Import-STFNetScalerConfiguration unter Angabe einer eigenen Rückruf-URL

Importieren Sie drei neue Gateways in StoreFront mit dem Cmdlet "Import-STFNetScalerConfiguration" und geben Sie mit dem Parameter "-callbackURL" eine Rückruf-URL Ihrer Wahl an.

command KOPIEREN

```
$ImportedGateways = Read-STFNetScalerConfiguration -path "$env:USERPROFILE\desktop\GatewayConfig.zip"

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 0 -CallbackUrl "https://emeagatewaycb.example.c

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 1 -CallbackUrl "https://emeagatewaycb.example.c

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 2 -CallbackUrl "https://emeagatewaycb.example.c
```

Import STFNetScalerConfiguration unter Außerkraftsetzung der in der Importdatei gespeicherten Authentifizierungsmethode und Angabe einer eigenen Rückruf-URL

- Importieren Sie drei neue Gateways in StoreFront mit dem Cmdlet "Import-STFNetScalerConfiguration" und geben Sie mit dem Parameter "-callbackURL" eine Rückruf-URL Ihrer Wahl an.

Befehl KOPIEREN

```
$ImportedGateways = Read-STFNetScalerConfiguration -path "$env:USERPROFILE\desktop\GatewayConfig.zip"

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 0 -LogonType "SmartCard" -CallbackUrl "https://e

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 1 -LogonType "SmartCard" -CallbackUrl "https://e

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 2 -LogonType "SmartCard" -CallbackUrl "https://e
```

Konfigurieren von NetScaler Gateway-Verbindungseinstellungen

Jun 04, 2018

Anhand der folgenden Anleitungen können Sie die Details von NetScaler Gateway-Bereitstellungen aktualisieren, über die Benutzer auf Stores zugreifen. Weitere Informationen über die Konfiguration von NetScaler Gateway für StoreFront finden Sie unter Using WebFront to Integrate with StoreFront.

Wenn Sie ihre NetScaler Gateway-Bereitstellungen ändern, müssen Benutzer, die durch diese Bereitstellungen auf Stores zugreifen, Citrix Receiver mit den geänderten Verbindungsinformationen aktualisieren. Bei der Konfiguration einer Citrix Receiver für Web-Site für einen Store können Benutzer eine aktualisierte Citrix Receiver-Provisioningdatei von der Site beziehen. Andernfalls können Sie eine Provisioningdatei für den Store exportieren und diese Datei für die Benutzer verfügbar machen.

Wichtig: Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Wenn Sie die Änderungen vorgenommen haben, übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden.

Ändern der allgemeinen NetScaler Gateway-Einstellungen

Mit Allgemeine Einstellungen ändern bearbeiten Sie die Namen der NetScaler Gateway-Bereitstellungen, die Benutzern angezeigt werden, und aktualisieren die StoreFront-Konfiguration, wenn sich die URL des virtuellen Servers oder des Anmeldepunkts und der Bereitstellungsmodus der NetScaler Gateway-Infrastruktur ändert.

1. Klicken Sie auf der Windows-Startseite oder auf der Apps-Seite auf die Kachel Citrix StoreFront.
2. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten Stores aus und klicken Sie auf NetScaler Gateways verwalten.
3. Geben Sie einen Namen für die NetScaler Gateway-Bereitstellung an, mit dem die Benutzer sie leicht identifizieren können.
   Benutzern wird der Anzeigename angezeigt, den Sie in Citrix Receiver angegeben haben. Nehmen Sie deshalb relevante Informationen in den Namen auf, damit Benutzer leichter entscheiden können, ob sie die Bereitstellung verwenden möchten. Beispielsweise können Sie den geographischen Standort in die Anzeigenamen der NetScaler Gateway-Bereitstellungen einfügen, damit Benutzer problemlos das beste Gateway für ihren Standort identifizieren können.
4. Geben Sie die URL des virtuellen Servers oder Benutzeranmeldepunkts (für Access Gateway 5.0) für die Bereitstellung an. Geben Sie die Produktversion Ihrer Bereitstellung an.
   Der vollqualifizierte Domänenname (FQDN) für die StoreFront-Bereitstellung muss eindeutig sein und darf nicht dem vollqualifizierten Domänennamen des virtuellen NetScaler Gateway-Servers entsprechen. Das Verwenden des selben vollqualifizierten Domänennamens für StoreFront und den virtuellen NetScaler Gateway-Server wird nicht unterstützt.
5. Wenn in der Bereitstellung Access Gateway 5.0 ausgeführt wird, fahren Sie mit Schritt 7 fort. Andernfalls und geben Sie ggf. die Subnetz-IP-Adresse des NetScaler Gateway-Geräts an.
   Die Subnetzadresse ist die IP-Adresse, durch die NetScaler Gateway für die Kommunikation mit Servern im internen Netzwerk das Benutzergerät darstellt. Dies kann es sich auch die zugeordnete IP-Adresse des NetScaler Gateway-Geräts sein. Wenn angegeben, verwendet StoreFront die Subnetz-IP-Adresse, um zu überprüfen, ob eingehende Anfragen von einem vertrauenswürdigen Gerät stammen.

6. Wenn Sie ein Gerät mit NetScaler Gateway hinzufügen, wählen Sie aus der Liste Anmeldetyp die Authentifizierungsmethode aus, die Sie auf dem Gerät für Benutzer von Citrix Receiver konfiguriert haben.
   Die von Ihnen angegebenen Informationen über die Konfiguration des NetScaler Gateway-Geräts wird der Provisioningdatei für den Store hinzugefügt. Dies ermöglicht, dass Citrix Receiver die entsprechende Verbindungsanforderung schickt, wenn das Gerät zum ersten Mal kontaktiert wird.

   - Wenn Benutzer die Domänenanmeldeinformationen für Microsoft Active Directory eingeben müssen, wählen Sie Domäne.
   - WählenSie Sicherheitstoken, wenn Benutzer einen Tokencode von einem Sicherheitstoken eingeben müssen.
   - WählenSie Domäne und Sicherheitstoken aus, wenn Benutzer ihre Domänenanmeldeinformationen und einen Tokencode von einem Sicherheitstoken eingeben müssen.
   - Wählen Sie SMS-Authentifizierung, wenn Benutzer ein in einer Textnachricht gesendetes Einmalkennwort eingeben müssen.
   - Wenn Benutzer eine Smartcard vorlegen und eine PIN eingeben müssen, wählen Sie Smartcard.

   Wenn Sie die Smartcardauthentifizierung mit einer sekundären Authentifizierungsmethode konfigurieren, auf die Benutzer zurückgreifen können, wenn es Probleme mit den Smartcards gibt, wählen Sie die sekundäre Authentifizierungsmethode aus der Liste Smartcard-Fallback.

7. Wenn Ihre Bereitstellung NetScaler Gateway oder ein einzelnes Access Gateway 5.0-Gerät hat, geben Sie die URL für den NetScaler Gateway-Authentifizierungsdienst in das Feld Rückruf-URL ein. StoreFront fügt automatisch den Standardteil der URL an.
   Geben Sie die intern zugängliche URL des Geräts ein. StoreFront kontaktiert den NetScaler Gateway-Authentifizierungsdienst, um zu überprüfen, ob von NetScaler Gateway empfangene Anforderungen auch tatsächlich von diesem Gerät ausgehen.

Verwalten von Access Gateway 5.0-Geräten

Mit Geräte verwalten können Sie die IP-Adressen oder FQDNs der Geräte im Access Gateway 5.0-Cluster StoreFront hinzufügen, sie bearbeiten oder entfernen.

Aktivieren der Authentifizierung ohne Benutzereingriff durch Access Controller

Mit Authentifizierung ohne Benutzereingriff aktivieren können Sie URLs für den Authentifizierungsdienst, der auf den Access Controller-Servern für das Access Gateway 5.0-Cluster ausgeführt wird, hinzufügen, bearbeiten oder entfernen. Geben Sie aus Gründen der Fehlertoleranz URLs für mehrere Server ein und führen Sie die Server dabei in der Reihenfolge ihrer Priorität auf, um die Failoversequenz festzulegen. StoreFront authentifiziert Remotebenutzer über den Authentifizierungsdienst, damit sie ihre Anmeldeinformationen nicht neu eingeben müssen, wenn sie auf Stores zugreifen.

Verwalten von Secure Ticket Authorities

Mit Secure Ticket Authority können Sie die Liste der Secure Ticket Authorities (STAs), aus der StoreFront Sitzungstickets für Benutzer abruft, aktualisieren und Sitzungszuverlässigkeit konfigurieren. Die STA wird auf XenDesktop- und XenApp-Servern gehostet und gibt Sitzungstickets als Reaktion auf Verbindungsanforderungen aus. Auf diesen Sitzungstickets basiert die Authentifizierung und Autorisierung für den Zugriff auf XenDesktop- und XenApp-Ressourcen.

1. Klicken Sie auf der Windows-Startseite oder auf der Apps-Seite auf die Kachel Citrix StoreFront.
2. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten Stores und im Ergebnisbereich eine NetScaler Gateway-Bereitstellung aus. Klicken Sie im Bereich Aktionen auf Netscaler Gateways verwalten.
3. Klicken Sie auf Hinzufügen, um die URL eines Servers, auf dem die STA ausgeführt wird, einzugeben. Geben zur Aktivierung der Fehlertoleranz die URLs mehrerer Secure Ticket Authority-Server an und führen Sie die Server dabei in der

Reihenfolge ihrer Priorität auf, um die Failoversequenz festzulegen. Wenn Sie eine URL ändern möchten, wählen Sie den Eintrag in der Liste Secure Ticket Authority-URLs und klicken Sie auf Bearbeiten. Wählen Sie eine URL in der Liste und klicken Sie auf Entfernen, damit StoreFront zukünftig keine Sitzungstickets von dieser STA bezieht.

4. Aktivieren Sie das Kontrollkästchen Sitzungszuverlässigkeit aktivieren, wenn XenDesktop und XenApp getrennte Sitzungen aufrechterhalten sollen, während Citrix Receiver eine automatische Wiederverbindung versucht. Aktivieren Sie das Kontrollkästchen Tickets von zwei Secure Ticket Authoritys anfordern (falls verfügbar), wenn Sie mehrere STAs konfiguriert haben und sicherstellen möchten, dass Sitzungszuverlässigkeit immer gegeben ist.
   Wenn das Kontrollkästchen Tickets von zwei Secure Ticket Authoritys anfordern (falls verfügbar) aktiviert ist, ruft StoreFront Tickets von zwei verschiedenen Secure Ticket Authoritys ab, damit Benutzersitzungen nicht unterbrochen werden, wenn eine Secure Ticket Authority während der Sitzung ausfällt. Wenn StoreFront aus irgendeinem Grund keine Verbindung zu zwei Secure Ticket Authoritys herstellen kann, wird automatisch nur eine Secure Ticket Authority verwendet.

Entfernen von NetScaler Gateway-Bereitstellungen

Verwenden Sie im Bereich **Aktionen** die Aufgabe Entfernen für **NetScaler Gateways verwalten**, um eine NetScaler Gateway-Bereitstellung aus StoreFront zu löschen. Nach dem Entfernen eines NetScaler Gateway-Geräts können Benutzer nicht mehr über diese Bereitstellung auf Stores zugreifen.

Lastausgleich mit NetScaler

Nov 27, 2017

Dieser Artikel enthält Informationen zur Verwendung von NetScaler für den Lastausgleich zweier oder mehr StoreFront-Server.

Konfigurieren einer StoreFront-Servergruppe und des NetScaler-Lastausgleichs

Erstellen eines Serverzertifikats für den NetScaler Load Balancer- und die StoreFront-Server

Erstellen eines virtuellen Lastausgleichsservers für die Abonnementsynchronisierung zwischen Servergruppen

Konfigurieren der StoreFront-Servergruppe für den Lastausgleich

Citrix Service Monitor

NetScaler Gateway und virtuelle Lastausgleichsserver auf demselben NetScaler Gateway-Gerät

Loopback-Optionen beim Lastausgleich für eine StoreFront-Servergruppe mit NetScaler

Konfigurieren einer StoreFront-Servergruppe und des Lastausgleichs für NetScaler

Planen der StoreFront-Bereitstellung mit Lastausgleich

Dieser Artikel enthält Informationen zum Bereitstellen einer StoreFront-Servergruppe mit mindestens zwei StoreFront-Servern in einer aktiven Konfiguration mit Lastausgleich.DerArtikel enthält Angaben zum Konfigurieren eines NetScaler-Geräts für den Lastausgleich für von Citrix Receiver bzw. Citrix Receiver für Web eingehende Anforderungen über alle StoreFront-Knoten in der Servergruppe hinweg und zum Konfigurieren des neuen StoreFront-Monitors für die Verwendung mit einem NetScaler-Load Balancer oder dem Load Balancer eines Drittanbieters.

Beispiele für eine Lastausgleichskonfiguration finden Sie unten unter "Szenario 1" und "Szenario 2".

Getestet in der folgenden Umgebung

- Vier Windows Server 2012 R2 StoreFront 3.0-Knoten in einer einzelnen Servergruppe
- Ein für Least-Connection-Lastausgleich und Cookie-Persistenz konfigurierter NetScaler 10.5-Load Balancer.
- Ein Windows 8.1-Testclient mit Fiddler 4.0 und Citrix Receiver für Windows 4.3.

Zertifikatanforderungen für den Lastausgleich bei Verwendung von HTTPS

Lesen Sie den Abschnitt Planen des Einsatzes von Gateway- und Serverzertifikaten.

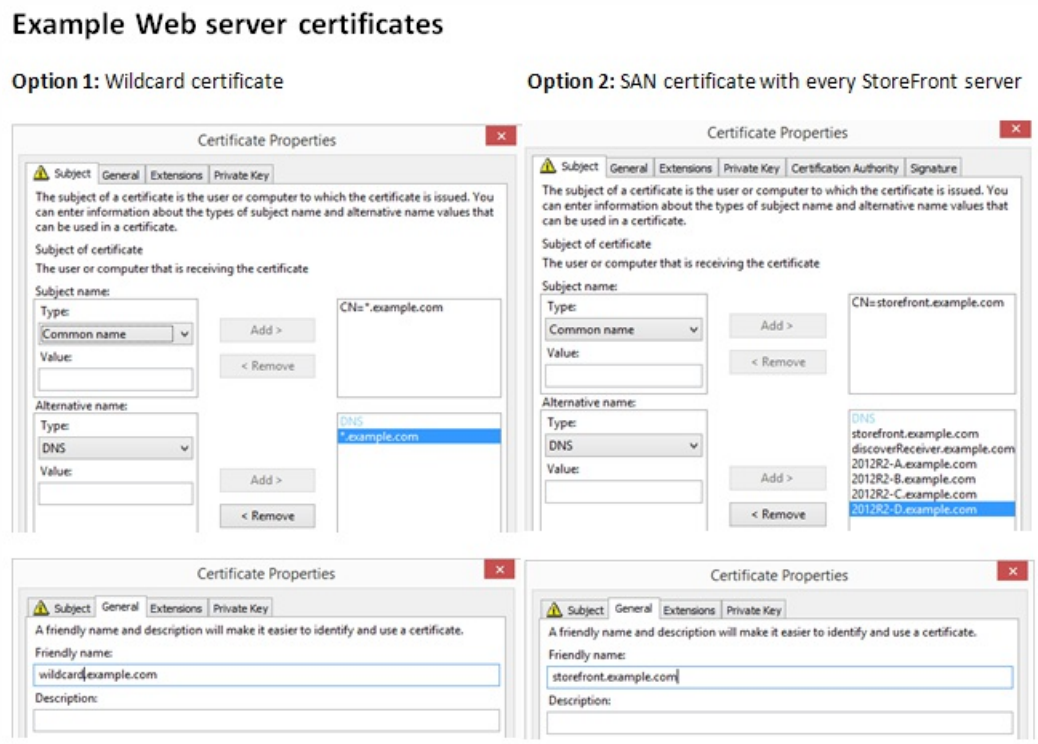
Ziehen Sie die folgenden Optionen in Betracht, bevor Sie ein Zertifikat von einer kommerziellen Zertifizierungsstelle erwerben oder eines von Ihrer Unternehmens-ZS ausstellen lassen.

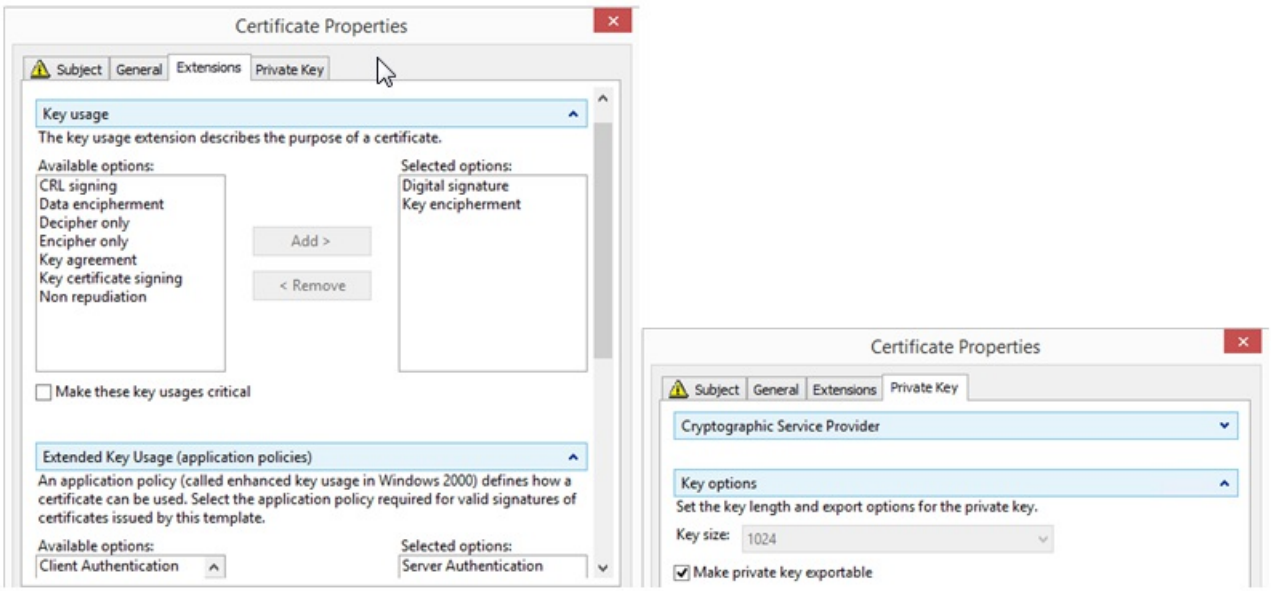
- **Option 1:** Verwendung eines *.beispiel.com-Platzhalterzertifikats auf dem virtuellen NetScaler-Lastausgleichsserver und den Knoten der StoreFront-Servergruppe.Dies vereinfacht die Konfiguration und ermöglicht das künftige Hinzufügen weiterer StoreFront-Server, ohne dass das Zertifikat ersetzt werden muss.
- **Option 2**: Verwendung eines Zertifikats mit alternativen Antragstellernamen (SAN) auf dem virtuellen NetScaler-Lastausgleichsserver und auf den Knoten der StoreFront-Servergruppe.Zusätzliche SANs in dem Zertifikat, die allen vollqualifizierten Domänennamen der StoreFront-Server entsprechen, sind zwar optional, jedoch empfehlenswert, da sie

eine größere Flexibilität bei der StoreFront-Bereitstellung bieten.Schließen Sie einen SAN für die E-Mail-basierte Ermittlung ein (discoverReceiver.example.com).

Weitere Informationen über die Konfiguration der E-Mail-basierten Ermittlung finden Sie unter http://blogs.citrix.com/2013/04/01/configuring-email-based-account-discovery-for-citrix-receiver/.

Hinweis: Wenn der private Schlüssel des Zertifikats nicht exportiert werden kann: Verwenden Sie zwei Zertifikate, eines auf dem virtuellen NetScaler-Lastausgleichsserver und eines auf den Knoten der StoreFront-Servergruppe. Beide Zertifikate müssen alternative Antragstellernamen enthalten.





Erstellen eines SSL-Zertifikats für den NetScaler Load Balancer und alle StoreFront-Server

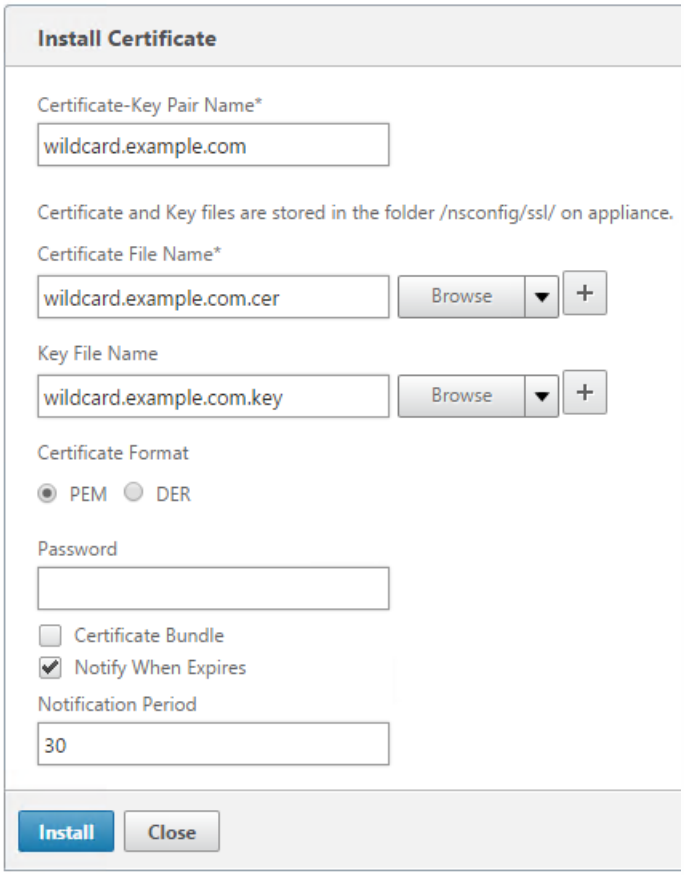
Importieren eines Zertifikats einer Windows-Zertifizierungsstelle in ein NetScaler-Gerät mit OpenSSL

- WinSCP ist ein nützliches kostenloses Drittanbietertool zum Verschieben von Dateien von einem Windows-Computer in ein NetScaler-Dateisystem.Kopieren Sie Zertifikate für den Import in den Ordner **/nsconfig/ssl/** im NetScaler-Dateisystem.
- Sie können auch mit den OpenSSL-Tools in NetScaler Gateway das Zertifikat und den Schlüssel aus einer **PKCS12/PFX**-Datei extrahieren, um eine CER- und eine KEY X.509-Datei separat im PEM-Format zu erstellen, die von NetScaler verwendet werden können.

1. Kopieren Sie die PFX-Datei in den Ordner **/nsconfig/ssl** auf dem NetScaler-Gerät oder in VPX.
2. Öffnen Sie die NetScaler-Befehlszeilenschnittstelle (CLI).
3. Geben Sie **Shell** ein, um die NetScaler-Befehlszeilenschnittstelle zu beenden und zur FreeBSD-Shell zu wechseln.
4. Wechseln Sie durch Eingabe von **cd /nsconfig/ssl** das Verzeichnis.
5. Führen Sie **openssl pkcs12 -in .pfx -nokeys -out .cer** aus und geben Sie bei entsprechender Aufforderung das PFX-Kennwort ein.
6. Führen Sie **openssl pkcs12 -in .pfx -nocerts -out .key** aus, geben Sie bei entsprechender Aufforderung das PFX-Kennwort ein und legen Sie die PEM- Passphrase für den privaten Schlüssel zum Schutz der KEY-Datei fest.
7. Führen Sie **ls –al** aus, um zu prüfen, ob die CER- und die KEY-Datei in **/nsconfig/ssl/** erstellt wurden.
8. Geben Sie zum Beenden und Rückkehren zur NetScaler Befehlszeilenschnittstelle **Exit** ein.

Konfigurieren des Serverzertifikats in NetScaler nach dem Import

1. Melden Sie sich bei der NetScaler-Verwaltungskonsole an.
2. Wählen Sie "Traffic Management > SSL > SSL Certificates" und klicken Sie auf "Install".
3. Geben Sie im Fenster Install Certificate den Namen des Zertifikats und des privaten Schlüsselpaars ein.
   - Wählen Sie die CER-Zertifikatdatei im NetScaler-Dateisystem unter /nsconfig/ssl/ aus.
   - Wählen Sie die KEY-Datei mit dem privaten Schlüssel am gleichen Speicherort aus.



Erstellen von DNS-Datensätzen für den Load Balancer der StoreFront-Servergruppe

Erstellen Sie einen DNS Alias- und einen PTR-Datensatz für den ausgewählten freigegebenen FQDN.Clients im Netzwerk verwenden diesen FQDN für den Zugriff auf die StoreFront-Servergruppe unter Verwendung des NetScaler-Load Balancers.

Beispiel: **storefront.example.com** wird in die virtuelle IP-Adresse (VIP) des Lastausgleichsservers aufgelöst.

Szenario 1: Eine durchgängige sichere HTPPS 443-Verbindung zwischen Client und NetScaler-Load Balancer und zwischen Load Balancer und mindestens zwei StoreFront 3.0-Servern.

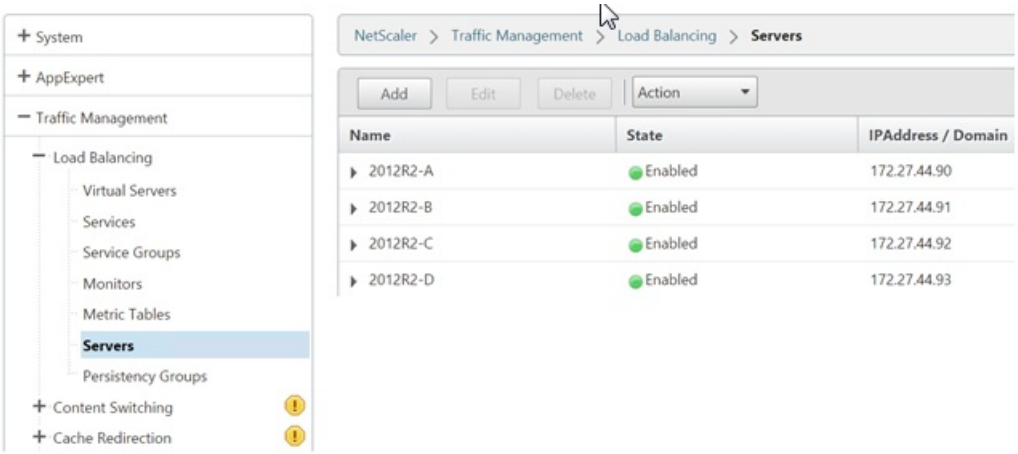
Bei diesem Szenario wird ein modifizierter StoreFront-Monitor unter Einsatz von Port 443 verwendet.

Hinzufügen einzelner StoreFront-Serverknoten zum NetScaler-Load Balancer

1. Melden Sie sich bei der NetScaler-Verwaltungskonsole an.
2. Wählen Sie **Traffic Management > Load Balancing > Servers > Add** aus und fügen Sie die vier StoreFront-Knoten für den Lastausgleich hinzu.

   Beispiel = 4 x 2012R2 StoreFront-Knoten mit den Namen 2012R2-A bis -D.

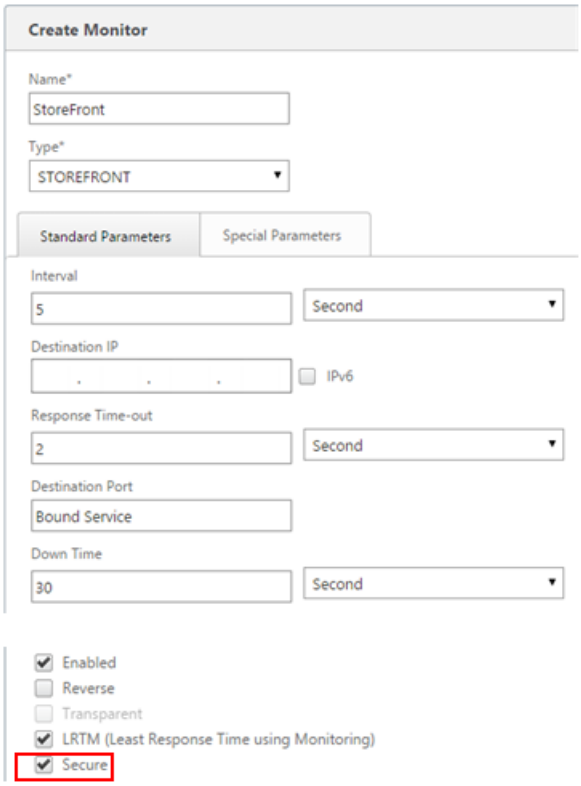
3. Verwenden Sie die IP-basierte Serverkonfiguration und geben Sie die Server-IP-Adresse für jeden StoreFront-Knoten ein.



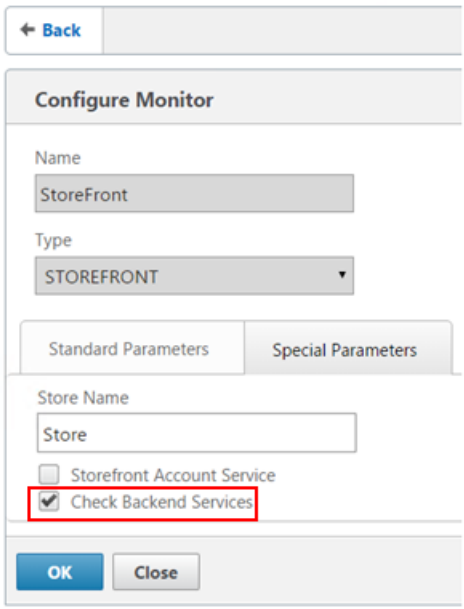
Definieren eines StoreFront-Monitors zur Prüfung des Status aller StoreFront-Knoten in der Servergruppe

1. Melden Sie sich bei der NetScaler-Verwaltungskonsole an.
2. Wählen Sie **Traffic Management > Load Balancing > Monitors > Add** aus und fügen Sie einen neuen Monitor unter dem Namen "StoreFront" unter Akzeptieren aller Standardeinstellungen hinzu.
3. Wählen Sie im Dropdownmenü **Type** die Option **StoreFront** aus.
4. Falls Sie HTTPS für die Verbindung zwischen dem virtuellen Lastausgleichsserver und StoreFront verwenden, aktivieren Sie das Kontrollkästchen **Secure**, falls nicht, lassen Sie es deaktiviert.
5. Geben Sie den Namen des Stores auf der Registerkarte "Parameters" ein.
6. Aktivieren Sie das Kontrollkästchen **Check Backend Services** auf der Registerkarte "Parameters".Damit wird die Überwachung von auf dem StoreFront-Server ausgeführten Diensten aktiviert.StoreFront-Dienste werden durch Sondieren eines Windows-Diensts auf dem StoreFront-Server überwacht, der den Status aller ausgeführten StoreFront-Dienste zurückgibt.

Standard Parameters Tab



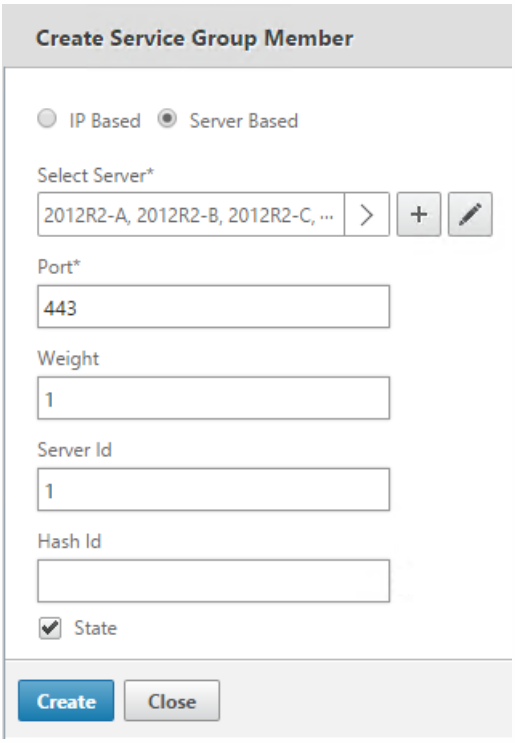
Special Parameters Tab



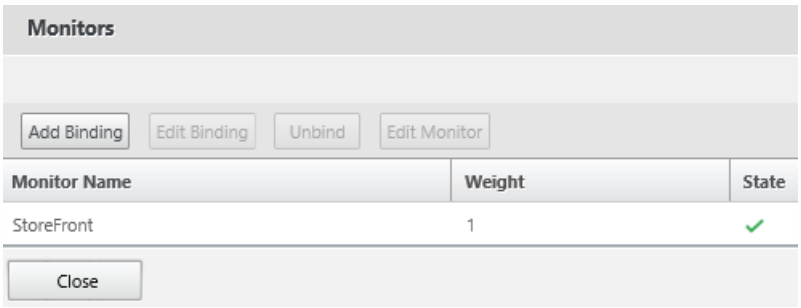
Erstellen einer HTTPS 443-Dienstgruppe für alle StoreFront-Server

1. Wählen Sie in der Dienstgruppe die Option Members auf der rechten Seite aus und fügen Sie alle StoreFront-Serverknoten, die Sie zuvor im Bereich "Servers" definiert haben, hinzu.

2. Legen Sie den SSL-Port fest und geben Sie für jeden Knoten beim Hinzufügen eine eindeutige Server-ID an.

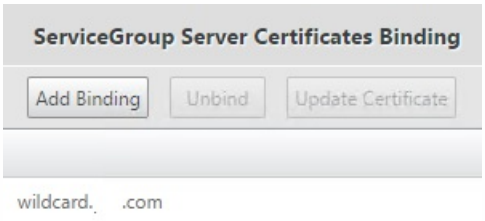


3. Wählen Sie auf der Registerkarte "Monitors" den zuvor erstellten StoreFront-Monitor aus.



4. Binden Sie auf der Registerkarte "Certificates" das zuvor importierte Serverzertifikat.

5. Binden Sie das Zertifizierungsstellenzertifikat, das zum Signieren des zuvor importierten Serverzertifikats verwendet wurde, sowie jegliche Zertifizierungsstellen, die Teil der PKI-Vertrauenskette sind.

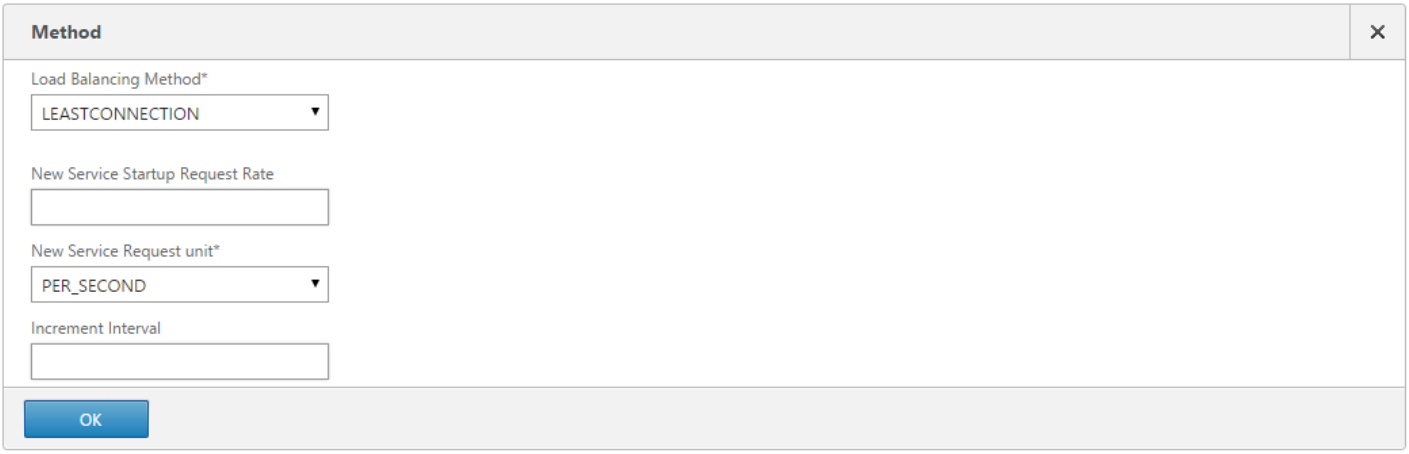


Erstellen eines virtuellen Lastausgleichservers für den Benutzerdatenverkehr

1. Melden Sie sich bei der NetScaler-Verwaltungskonsole an.

2. Wählen Sie **Traffic Management > Load Balancing > Virtual Servers > Add** zum Erstellen eines neuen virtuellen Servers aus.

3. Wählen Sie die Lastausgleichsmethode für den virtuellen Server aus.Für den Lastausgleich in StoreFront wird in der Regel **round robin** oder **least connection** verwendet.



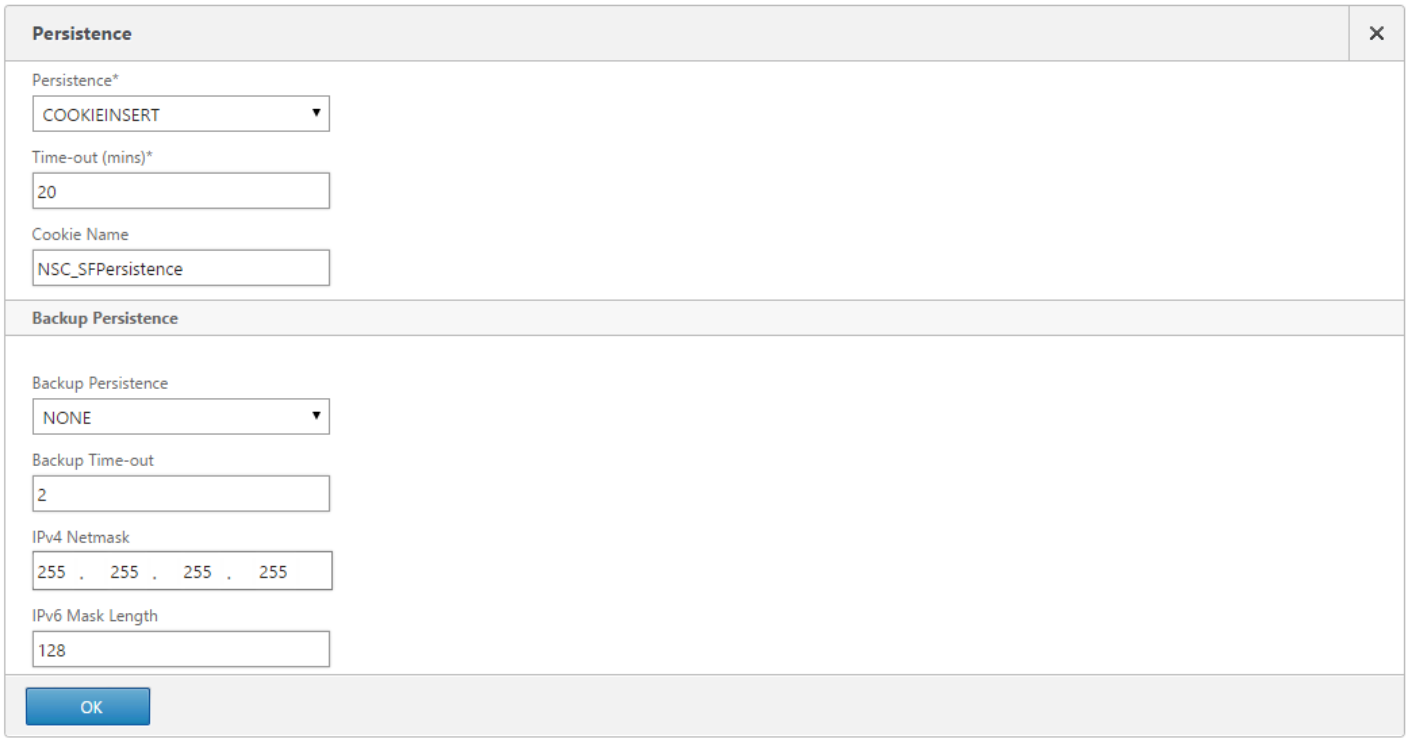
4. Binden Sie diezuvor erstellte Dienstgruppe an den virtuellen Lastausgleichsserver.

5. Binden Sie das Serverzertifikat und das ZS-Zertifikat, das Sie zuvor an die Dienstgruppe gebunden haben, an den virtuellen Lastausgleichsserver.

6. Wählen Sie im Menü für den virtuellen Lastausgleichsserver rechts **Persistence** aus und legen Sie als Persistenzmethode **CookieInsert** fest.

7. Benennen Sie das Cookie. Beispiel: **NSC_SFPersistence**, damit eine einfache Identifizierung in Fiddler-Ablaufverfolgungen beim Debuggen möglich ist.

8. Legen Sie für "Backup persistence" **None** fest.



Szenario 2: HTTPS-Beendigung – HTTPS 443-Kommunikation zwischen Client und NetScaler-Load Balancer und HTTP 80-Verbindungen zwischen Load Balancer und den StoreFront 3.0-Servern dahinter.

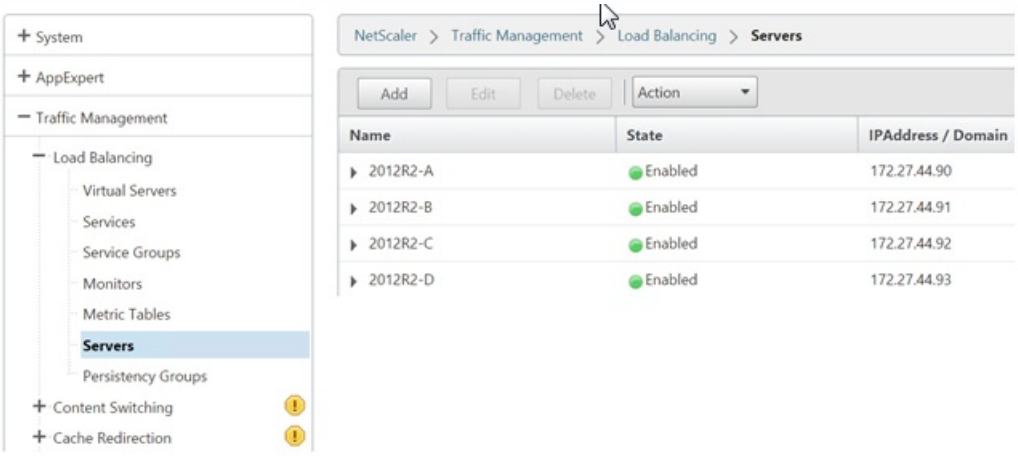
Bei diesem Szenario wird der Standard-StoreFront-Monitor unter Einsatz von Port 8000 verwendet.

Hinzufügen einzelner StoreFront-Server zum NetScaler-Load Balancer

1. Melden Sie sich bei der NetScaler-Verwaltungskonsole an.
2. Wählen Sie **Traffic Management > Load Balancing > Servers > Add** aus und fügen Sie die vier StoreFront-Server für den Lastausgleich hinzu.

   Beispiel = 4 x 2012R2 StoreFront-Server mit den Namen 2012R2-A bis -D.

3. Verwenden Sie die IP-basierte Serverkonfiguration und geben Sie die Server-IP-Adresse für jeden StoreFront-Server ein.



Definieren eines HTTP 8000-StoreFront-Monitors zur Überprüfung des Status aller StoreFront-Server in der Servergruppe

1. Melden Sie sich bei der NetScaler-Verwaltungskonsole an.
2. Wählen Sie **Traffic Management > Monitors > Add** aus und fügen Sie einen neuen Monitor unter dem Namen "StoreFront" hinzu.
3. Geben Sie einen Namen für den neuen Monitor ein und akzeptieren Sie alle Standardeinstellungen.
4. Wählen Sie im Dropdownmenü **Type** die Option **StoreFront** aus.
5. Geben Sie den Namen des Stores auf der Registerkarte "Parameters" ein.
6. Geben Sie unter "Destination Port" als Zielport **8000** ein; dies entspricht der Standardmonitorinstanz, die auf jedem StoreFront-Server erstellt wird.
7. Aktivieren Sie das Kontrollkästchen **Check Backend Services** auf der Registerkarte "Parameters".Damit wird die Überwachung von auf dem StoreFront-Server ausgeführten Diensten aktiviert.StoreFront-Dienste werden durch Sondieren eines Windows-Diensts auf dem StoreFront-Server überwacht, der den Status aller ausgeführten StoreFront-Dienste zurückgibt.

Erstellen einer HTTP 80-Dienstgruppe für alle StoreFront-Server

1. Wählen Sie in der Dienstgruppe die Option "Members" auf der rechten Seite aus und fügen Sie alle StoreFront-Serverknoten, die Sie zuvor im Bereich "Servers" definiert haben, hinzu.
2. Legen Sie für den HTTP-Port 80 fest und geben Sie für jeden Server beim Hinzufügen eine eindeutige Server-ID an.
3. Wählen Sie auf der Registerkarte "Monitors" den zuvor erstellten StoreFront-Monitor aus.

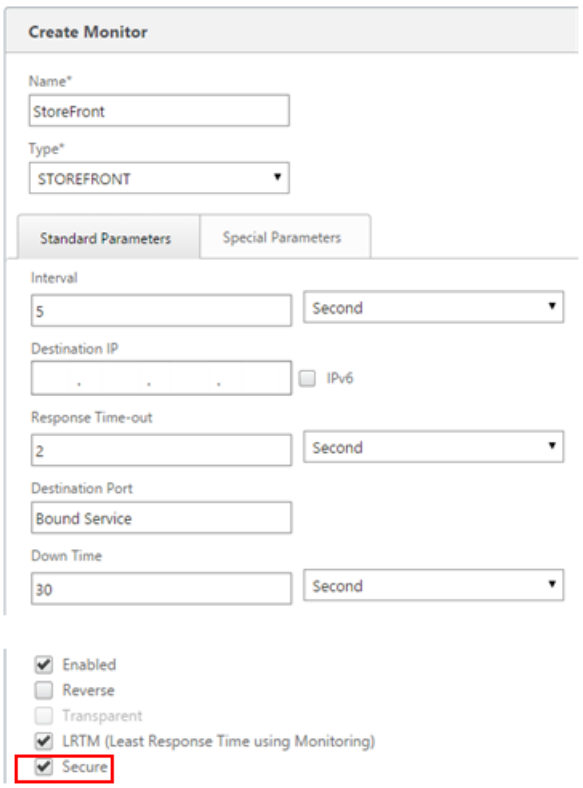
Erstellen eines virtuellen Lastausgleichservers für den Benutzerdatenverkehr mit HTTPS-Beendigung

1. Wählen Sie **Traffic Management > Load Balancing > Virtual Servers > Add** zum Erstellen eines neuen virtuellen Servers aus.
2. Wählen Sie die Lastausgleichsmethode für den virtuellen Server aus.Für den Lastausgleich in StoreFront wird in der Regel **round robin** oder **least connection** verwendet.
3. Binden Sie diezuvor erstellte Dienstgruppe an den virtuellen Lastausgleichsserver.
4. Binden Sie das Serverzertifikat und das ZS-Zertifikat, das Sie zuvor an die Dienstgruppe gebunden haben, an den virtuellen Lastausgleichsserver.

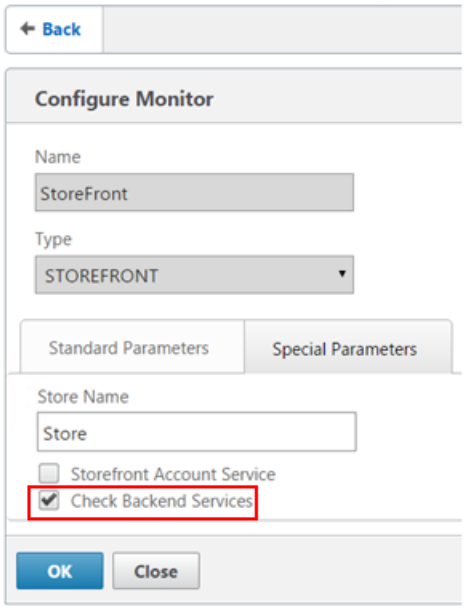
   Hinweis: Wenn der Client kein HTTP-Cookie speichern darf, enthalten nachfolgende Anforderungen kein HTTP-Cookie und **Persistence** wird nicht verwendet.

5. Wählen Sie im Menü für den virtuellen Lastausgleichsserver **Persistence** aus und legen Sie als Persistenzmethode **CookieInsert** fest.
6. Benennen Sie das Cookie. Beispiel: **NSC_SFPersistence**, damit eine einfache Identifizierung in Fiddler-Ablaufverfolgungen beim Debuggen möglich ist.
7. Legen Sie für "Backup persistence" **None** fest.

Standard Parameters Tab



Special Parameters Tab



Erstellen eines virtuellen Lastausgleichsservers für die Abonnementsynchronisierung zwischen Servergruppen

Beim Erstellen eines virtuellen Lastenausgleichsservers sind folgende Optionen in Erwägung zu ziehen:

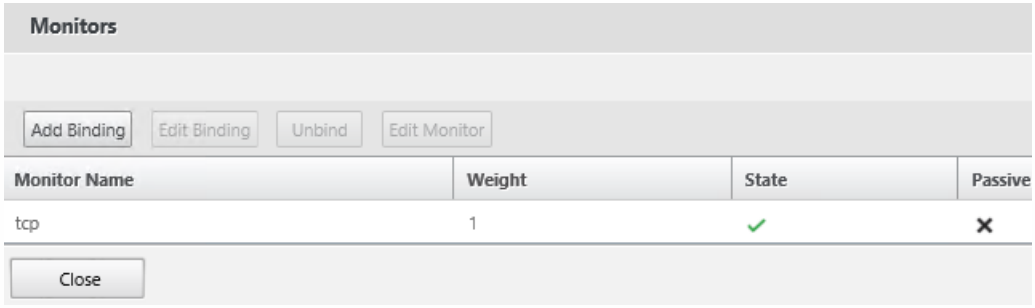
- **Option 1:** Erstellen eines einzelnen virtuellen Servers, um nur für den Benutzerdatenverkehr einen Lastausgleich vorzunehmen.Wenn Sie nur ICA-Starts veröffentlichter Apps und Desktops durchführen, ist nichts weiter erforderlich. (Obligatorisch und in der Regel das einzige Erfordernis.)
- **Option 2:** Erstellen zweier virtueller Lastausgleichsserver, einen für den Benutzerdatenverkehr beim Ausführen von ICA-Starts veröffentlichter Apps und Desktops und einen zweiten für die Synchronisierung von Abonnementdaten. (Nur erforderlich, wenn Abonnementdaten zwischen mindestens zwei StoreFront-Servergruppen mit Lastausgleich in einer großen Bereitstellung mit mehreren Standorten übertragen werden.)

Wenn eine Bereitstellung zwei oder mehr StoreFront-Servergruppen an verschiedenen geografischen Standorten umfasst, können Sie die Replikation von Abonnementdaten zwischen diesen Standorten über regelmäßige Pull-Aktionen nach Zeitplan durchführen. Für die StoreFront-Abonnementreplikation wird TCP-Port 808 verwendet, die Verwendung eines vorhandenen virtuellen Lastausgleichsservers an HTTP-Port 80 oder HTTPS-Port 443 schlägt daher fehl. Zur Bereitstellung hoher Dienstverfügbarkeit erstellen Sie einen zweiten virtuellen Server auf jedem NetScaler in der Bereitstellung zum Durchführen eines Lastausgleichs an TCP-Port 808 für jede der StoreFront-Servergruppen. Legen Sie beim Konfigurieren des Replikationszeitplans für die Servergruppe eine Adresse fest, die der virtuellen IP-Adresse des virtuellen Servers für die Abonnementsynchronisierung entspricht. Die Adresse der Servergruppe muss der FQDN des Load Balancers für die Servergruppe an diesem Standort sein.

Konfigurieren einer Dienstgruppe für die Synchronisierung von Abonnements

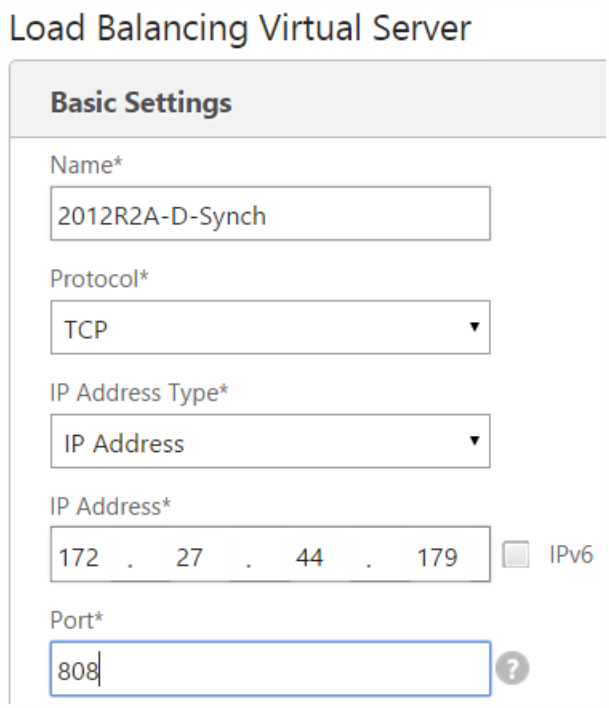
1. Melden Sie sich bei der NetScaler-Verwaltungskonsole an.

2. Wählen Sie **Traffic Management > Service Groups > Add** aus und fügen Sie eine neue Dienstgruppe hinzu.
3. Ändern Sie das Protokoll in **TCP**.
4. Wählen Sie in der Dienstgruppe die Option **Members** auf der rechten Seite aus und fügen Sie alle StoreFront-Serverknoten, die Sie zuvor im Bereich "Servers" definiert haben, hinzu.
5. Wählen Sie auf der Registerkarte **Monitors** den TCP-Monitor aus.



Erstellen eines virtuellen Lastausgleichsservers für die Abonnementsynchronisierung zwischen Servergruppen

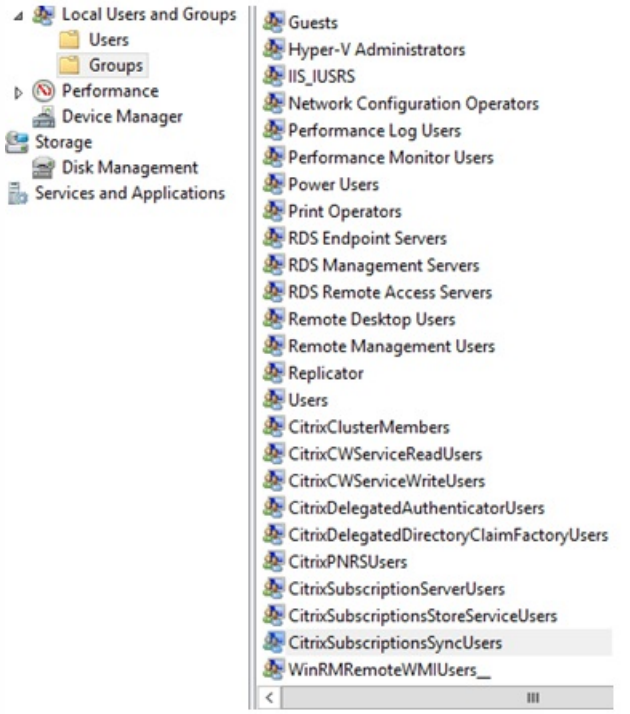
1. Melden Sie sich bei der NetScaler-Verwaltungskonsole an.
2. Wählen Sie **Traffic Management > Service Groups > Add** aus und fügen Sie eine neue Dienstgruppe hinzu.
3. Legen Sie als Lastausgleichsmethode **round robin** fest.
4. Ändern Sie das Protokoll in **TCP**.
5. Geben Sie als Portnummer **808** (**nicht** 443) ein.



Mitgliedschaft in CitrixSubscriptionsSyncUsers

Damit **StoreFront-Server A** an **Standort A** Abonnementdaten von **Server B** an einem anderen Standort anfordern und abrufen kann, muss Server A Mitglied der lokalen Sicherheitsgruppe **CitrixSubscriptionsSyncUsers** auf Server B sein. Die lokale Gruppe **CitrixSubscriptionsSyncUsers** enthält eine Zugriffssteuerungsliste aller remoten StoreFront-Server, die Abonnementdaten von einem bestimmten Server abrufen dürfen.Bei einer bidirektionalen Abonnementsynchronisierung

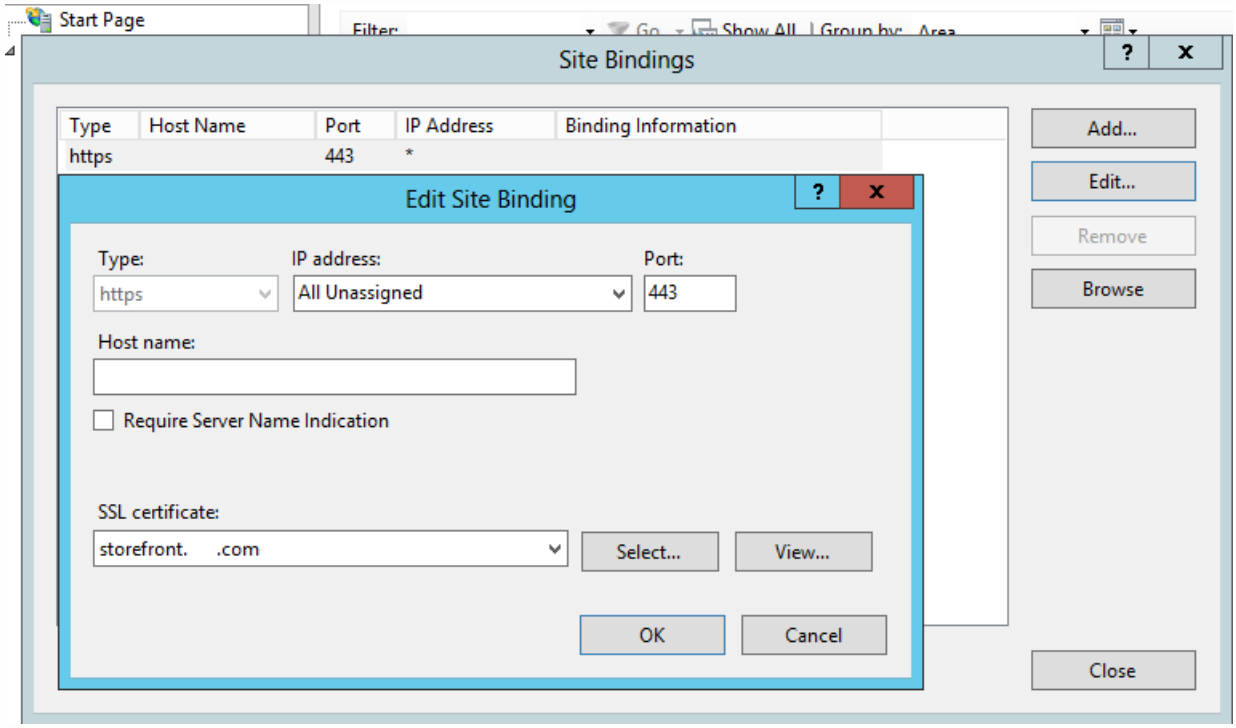
muss zudem Server B Mitglied der Sicherheitsgruppe **CitrixSubscriptionsSyncUsers** auf Server A sein, damit er von dort Abonnementdaten abrufen kann.



Konfigurieren der StoreFront-Servergruppe für den Lastausgleich

1. Importieren Sie auf allen StoreFront-Knoten in der Servergruppe das Zertifikat und den privaten Schlüssel, das bzw. den Sie auf dem virtuellen NetScaler-Lastausgleichsserver bereitgestellt haben.

2. Erstellen Sie eine HTTPS-Bindung in IIS auf allen StoreFront-Knoten und binden Sie das zuvor importierte Zertifikat.



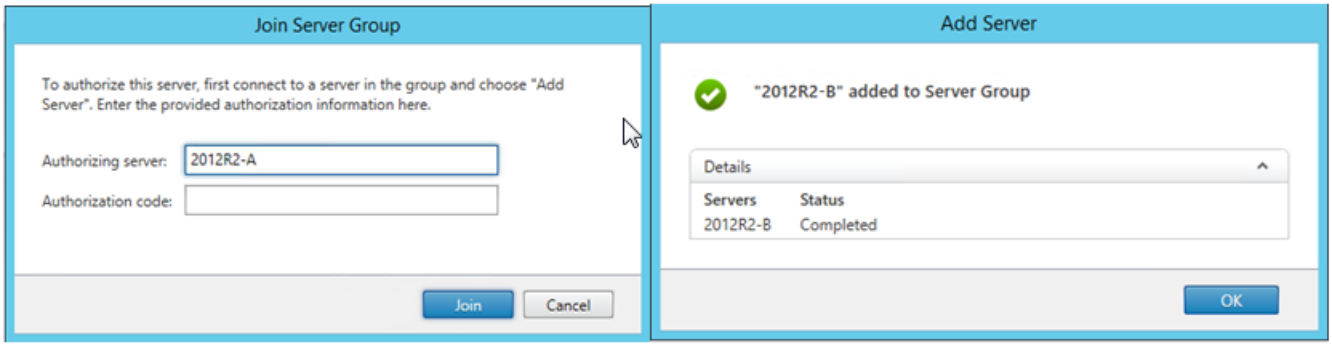
3. Installieren Sie StoreFront auf jedem Knoten in der Servergruppe.

4. Legen Sie bei der Installation von StoreFront die Host-Basis-URL auf dem primären Knoten als freigegebenen FQDN zur Verwendung durch alle Mitglieder der Servergruppe fest.Sie müssen ein Zertifikat verwenden, das den FQDN mit Lastausgleich als allgemeinen Namen (CN) oder als alternativen Antragstellernamen (Subject Alternative Name, SAN) enthält.

Informationen hierzu finden Sie unter Erstellen eines SSL-Zertifikats für den NetScaler Load Balancer- und den StoreFront-Server.

5. Fügen Sie im Rahmen der Erstkonfiguration von StoreFront die einzelnen Knoten nacheinander unter Verwendung des primären Knotens der Servergruppe hinzu.

6. Wählen Sie für beitretende Server **Server Group > Add Server > Copy the Authorization Code** aus.



7. Verteilen Sie die Konfiguration vom primären Knoten auf alle anderen Knoten in der Servergruppe.

8. Testen Sie die Servergruppe mit Lastausgleich mit einem Client, der den freigegebenen FQDN des Load Balancers kontaktieren und auflösen kann.

Citrix Service Monitor

Zur externen Überwachungdes Ausführungsstatus von Windows-Diensten, die für den einwandfreien Betrieb von StoreFront erforderlich sind, verwenden Sie den Windows-Dienst **Citrix Service Monitor**.Dieser Dienst ist von keinem anderen Dienst abhängig und kann andere wichtige StoreFront-Dienste überwachen und Fehler melden.Mit dem Dienst kann die relative Integrität einer StoreFront-Serverbereitstellung extern von anderen Citrix Komponenten, wie NetScaler, ermittelt werden.Die XML-Antwort des StoreFront-Diensts kann von einer Drittanbieter-Software zur Überwachung der Integrität wichtiger StoreFront-Dienste genutzt werden.

Wenn StoreFront bereitgestellt wird, wird ein Standardmonitor erstellt, der HTTP und Port 8000 verwendet.

Hinweis: In einer StoreFront-Bereitstellung ist nur eine Instanz eines Monitors zulässig.

Für Änderungen am vorhandenen Standardmonitor, z. B. zum Ändern des Protokolls und Ports auf HTTPS 443, verwenden Sie die drei PowerShell-Cmdlets zum Anzeigen bzw. Konfigurieren der Dienst-URL des StoreFront-Monitors.

Ersetzen des Standarddienstmonitors durch einen Monitor, der HTTPS und Port 443 verwendet

1. Öffnen Sie PowerShell Integrated Scripting Environment (ISE) auf dem primären StoreFront-Server und führen Sie folgende Befehle aus, um den Standardmonitor auf HTTPS 443 zu ändern.

```
$ServiceUrl = "https://localhost:443/StorefrontMonitor"
```

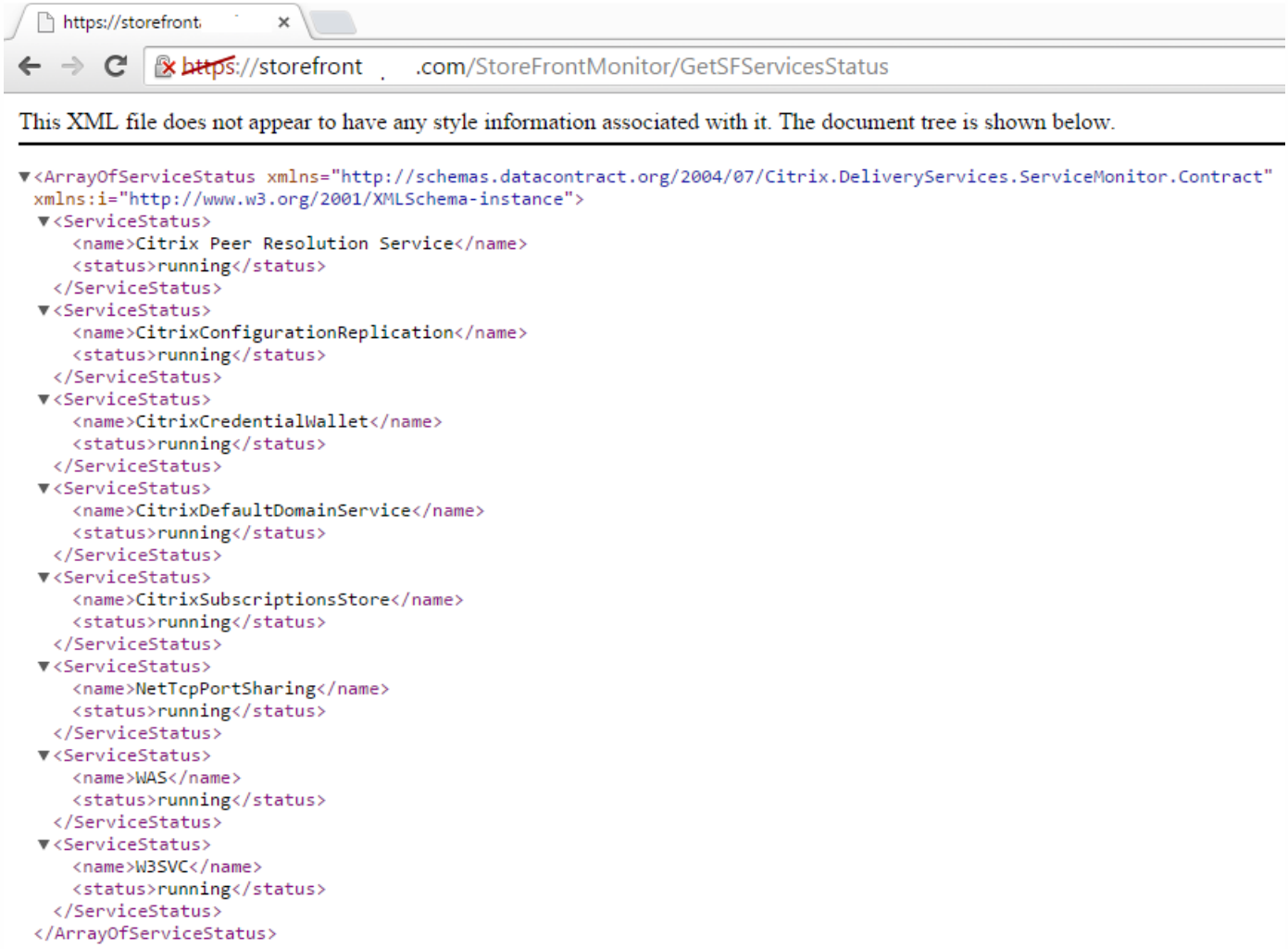
Set-STFServiceMonitor -ServiceUrl $ServiceUrl

Get-STFServiceMonitor

2. Nach Abschluss verteilen Sie die Änderungen auf alle anderen Server in der StoreFront-Servergruppe.

3. Für einen kurzen Test des neuen Monitors geben Sie die folgende URL im Browser auf dem StoreFront-Server oder auf einem anderen Computer mit Netzwerkzugriff auf den StoreFront-Server ein.Der Browser müsste eine XML-Zusammenfassung des Status jedes StoreFront-Diensts zurückgeben.

https://:443/StoreFrontMonitor/GetSFServicesStatus



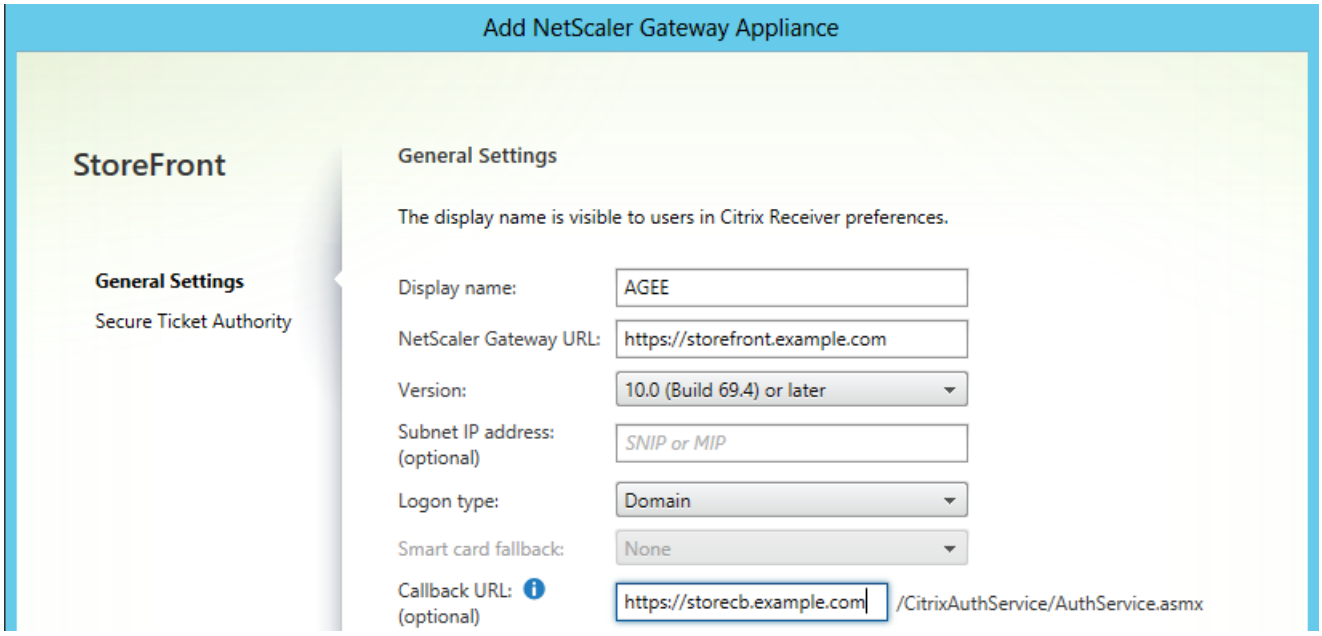
NetScaler Gateway und virtuelle Lastausgleichsserver auf demselben NetScaler Gateway-Gerät

Wenn Sie den virtuellen NetScaler Gateway-Server und den virtuellen Lastausgleichsserver auf demselben NetScaler-Gerät konfiguriert haben, treten beim Zugriff interner Domänenbenutzer auf die Host-Basis-URL von StoreFront mit Lastausgleich möglicherweise Probleme auf, wenn der Zugriff direkt und nicht über den virtuellen NetScaler Gateway-Server erfolgt.

In diesem Szenario geht StoreFront davon aus, dass der Endbenutzer sich bereits bei NetScaler Gateway authentifiziert hat, da StoreFront die Quell-IP-Adresse des Benutzers mit der Subnetz-IP-Adresse (SNIP) von NetScaler Gateway korreliert. Dadurch wird ein Versuch von StoreFront ausgelöst, den Benutzer unter Verwendung des AGBasic-Protokolls ohne Benutzereingriff bei NetScaler Gateway zu authentifizieren, anstatt den Benutzer zur Anmeldung mit seinen

Domänenanmeldeinformationen aufzufordern.Um dieses Problem zu vermeiden, verzichten Sie auf die Angabe einer SNIP-Adresse wie unten dargestellt, sodass die Authentifizierung mit Benutzernamen und Kennwort anstelle von AGBasic verwendet wird.

Konfigurieren von NetScaler Gateway in der StoreFront-Servergruppe



Loopback-Optionen beim Lastausgleich für eine StoreFront-Servergruppe mit NetScaler

Bei früheren Versionen von StoreFront (z. B. 2.6) wurde von Citrix empfohlen, die Hostdatei auf jedem StoreFront-Server manuell zu ändern, um den FQDN des Load Balancers der Loopbackadresse oder IP-Adresse auf dem spezifischen StoreFront-Server zuzuordnen.Dadurch wird sichergestellt, dass Receiver für Webin einer Bereitstellung mit Lastausgleich immer mit den StoreFront-Diensten auf dem gleichen Server kommuniziert.Dies ist erforderlich, da bei der expliziten Anmeldung zwischen Receiver für Web und dem Authentifizierungsdienst eine HTTP-Sitzung erstellt wird und Receiver für Web mit StoreFront-Diensten unter Verwendung des Basis-FQDN kommuniziert.Wenn der Basis-FQDN durch einen Load Balancer aufgelöst wird, könnte dieser Daten an einen anderen StoreFront-Server in der Gruppe senden, was zu einem Fehlschlagen der Authentifizierung führen würde.Es erfolgt keine Umgehung des Load Balancers, außer wenn Receiver für Web versucht, eine Verbindung mit dem Storedienst herzustellen, der auf dem gleichen Server wie Receiver für Web selbst residiert.

Sie können Loopback-Optionen mit PowerShell festlegen.Durch die Verwendung von Loopback wird die Erstellung von Hostdateieinträgen auf jedem StoreFront-Server in der Servergruppe überflüssig.

Beispiel einer web.config-Datei für Receiver für Web:

Beispiel eines PowerShell-Befehls:

& "c:\program files\Citrix\receiver storefront\scripts\ImportModules.ps1"

Set-DSLoopback -SiteId 1 -VirtualPath "/Citrix/StoreWeb" -Loopback "OnUsingHttp" -LoopbackPortUsingHttp 81

Der Parameter **-Loopback** kann einen von drei Werten haben.

Wert	Kontext

On: Ändert den Host der URL in 127.0.0.1.Schema und Port (falls angegeben) werden nicht geändert.	Kann nicht verwendet werden, wenn Load Balancer mit SSL-Terminierung verwendet wird.
OnUsingHttp: Ändert den Host in 127.0.0.1 und das Schema in HTTP und ändert den Port in den für l**oopbackPortUsingHttp** konfigurierten Wert.	Verwenden Sie dies nur, wenn Sie einen Load Balancer mit SSL-Terminierung haben.Die Kommunikation zwischen Load Balancer und StoreFront-Servern erfolgt über HTTP.Sie können den HTTP-Port explizit mit dem Attribut "-loopbackPortUsingHttp" konfigurieren.
Off: Die URL in der Anforderung wird nicht geändert.	Für die Problembehandlung verwenden.Tools wie Fiddler können den Datenverkehr zwischen Receiver für Web-Sites und StoreFront-Diensten nicht erfassen, wenn das Loopback auf "On" gesetzt ist.

Konfigurieren zweier URLs für dasselbe NetScaler Gateway

Nov 27, 2017

In StoreFront können Sie über "NetScaler Gateways verwalten" > "Hinzufügen" oder "Bearbeiten" in der StoreFront-Verwaltungskonsole eine einzelne NetScaler Gateway-URL hinzufügen. Es ist auch möglich, eine öffentliche NetScaler Gateway-URL und eine GSLB-URL (Global Server Load Balancing) über "NetScaler Gateways verwalten > importiert-aus-Datei" hinzuzufügen.

In diesem Artikel wird erläutert, wie Sie mit PowerShell-Cmdlets und dem StoreFront-PowerShell-SDK unter Verwendung des optionalen Parameters "-gslburl" das Attribut "GslbLocation" eines Gateways festlegen. Dieses Feature vereinfacht die NetScaler Gateway-Verwaltung in StoreFront in folgenden Anwendungsfällen:

1. **GSLB und mehrere NetScaler Gateways**: Verwenden von GSLB und mehrerer NetScaler Gateways für den Lastausgleich bei Remoteverbindungen mit veröffentlichten Ressourcen an mehreren Orten innerhalb einer großen, globalen Citrix Bereitstellung.
2. **Ein NetScaler Gateway mit öffentlicher oder privater URL**: Verwenden desselben NetScaler Gateways für den externen Zugriff über eine öffentliche URL und für den internen Zugriff über eine private URL.

Es handelt sich um ein erweitertes Feature. Wenn Sie GSLB noch nicht gut kennen, konsultieren Sie die Informationslinks am Ende dieses Artikels.

Das Feature bietet die folgenden Vorteile:

- Unterstützung zweier URLs für dasselbe Gateway-Objekt.
- Die Benutzer können beim Zugriff auf NetScaler Gateway zwischen zwei URLs wechseln, ohne dass der Administrator das StoreFront-Gateway-Objekt auf die gewünschte Gateway-URL umkonfigurieren muss.
- Weniger Zeitaufwand für Einrichtung und Tests der StoreFront-Gatewaykonfiguration bei Verwendung mehrerer GSLB-Gateways.
- Verwendung desselben NetScaler Gateway-Objekts in StoreFront innerhalb der DMZ für den externen und internen Zugriff.
- Unterstützung für beide URLs für das optimale Gateway-Routing. Weitere Informationen zum optimalen Gateway-Routing finden Sie unter Einrichten hoch verfügbarer Stores mit mehreren Sites.

Überlegungen zur Bereitstellung bei Verwendung zweier Gateway-URLs

> ### Important
>
> Bevor Sie eine zweite Gateway-URL mit dem Parameter "-gslburl" konfigurieren, empfiehlt Citrix zu prüfen, welche Serverzertifikate installiert sind und wie die DNS-Auflösung in Ihrem Unternehmen erfolgt. Alle URLs, die Sie in der NetScaler- und StoreFront-Bereitstellung verwenden möchten, müssen in den Serverzertifikaten aufgelistet sein. Weitere Informationen über Serverzertifikate, finden Sie unter Planen des Einsatzes von Gateway- und Serverzertifikaten.

DNS

- **Split-DNS**: Große Unternehmen verwenden häufig Split DNS. Bei Split DNS werden verschiedene Namespaces und DNS-

Server für die öffentliche und die private DNS-Auflösung verwendet. Vergewissern Sie sich, dass Ihre vorhandene DNS-Infrastruktur dies unterstützt.

- **Einzelne URL für den externen und internen Zugriff auf veröffentlichte Ressourcen**: Überlegen Sie, ob Sie für den Zugriff auf veröffentlichte Ressourcen von außerhalb und innerhalb des Firmennetzwerks dieselbe URL verwenden möchten oder ob zwei URLs (z. B. muster.com und muster.net) akzeptabel sind.

Serverzertifikat

Dieser Abschnitt enthält Beispiele für Serverzertifikatbereitstellungen bei Verwendung zweier Gateway-URLs.

- **Beispiel eines Serverzertifikats für eine StoreFront-Bereitstellung mit Lastausgleich**

  Ein privat signiertes Serverzertifikat mit Platzhaltern muss den FQDN "*.storefront.example.net" enthalten.

  Oder

  Ein privat signiertes SAN-Serverzertifikat muss alle für den Lastausgleich bei den drei StoreFront-Servern erforderlichen FQDNs enthalten.

  loadbalancer.storefront.example.net

  server1.storefront.example.net

  server2.storefront.example.net

  server3.storefront.example.net

  Legen Sie die Host-Basis-URL der StoreFront-Servergruppe auf den gemeinsamen FQDN fest, der in die IP-Adresse des Load Balancers aufgelöst wird.

  loadbalancer.storefront.example.net

- **Beispiel eines Serverzertifikats für eine Gruppe von XenApp- und XenDesktop 7.x-Delivery Controller**

  Ein privat signiertes Serverzertifikat mit Platzhaltern muss den FQDN "*.xendesktop.example.net" enthalten.

  Oder

  Ein privat signiertes SAN-Serverzertifikat muss alle, für eine XenDesktop-Site mit vier Controllern erforderlichen Server-FQDNs enthalten.

  XD1A. xendesktop.example.net

  XD1B. xendesktop.example.net

  XD2A. xendesktop.example.net

  XD2B. xendesktop.example.net

- **Beispiel eines Serverzertifikats für ein NetScaler Gateway, auf das extern und intern über Split DNS zugegriffen wird**

  Ein öffentlich signiertes SAN-Serverzertifikat für den externen und internen Zugriff muss den internen und den externen FQDN enthalten.

gateway.example.com

gateway.example.net

- **Beispiel eines Serverzertifikats für alle GSLB-Gateways, auf die extern zugegriffen wird**

  Ein öffentlich signiertes SAN-Serverzertifikat für den externen Zugriff über GSLB muss folgende FQDNs enthalten:

  gslbdomain.example.com

  emeagateway.example.com

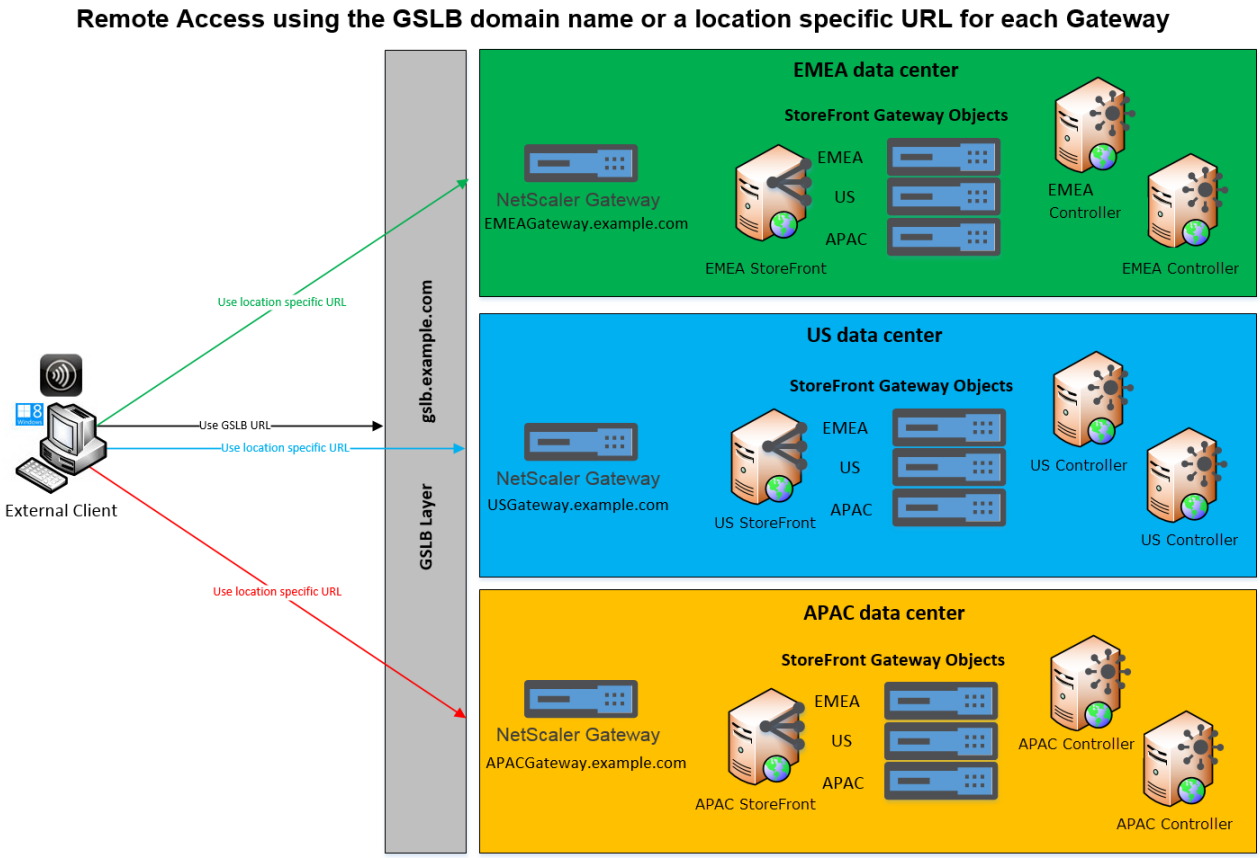
  usgateway.example.com

  apacgateway.example.com

  Dadurch können Benutzer über GSLB auf das am nächsten gelegene Gateway zugreifen oder ein anderes Gateway an dem Ort unter Auswahl seines FQDNs wählen.

Anwendungsfall 1: GSLB und mehrere NetScaler Gateways

Der Administrator verwendet GSLB und mehrere NetScaler Gateways für den Lastausgleich bei Remoteverbindungen mit veröffentlichten Ressourcen an mehreren Orten innerhalb einer großen, globalen Citrix Bereitstellung.



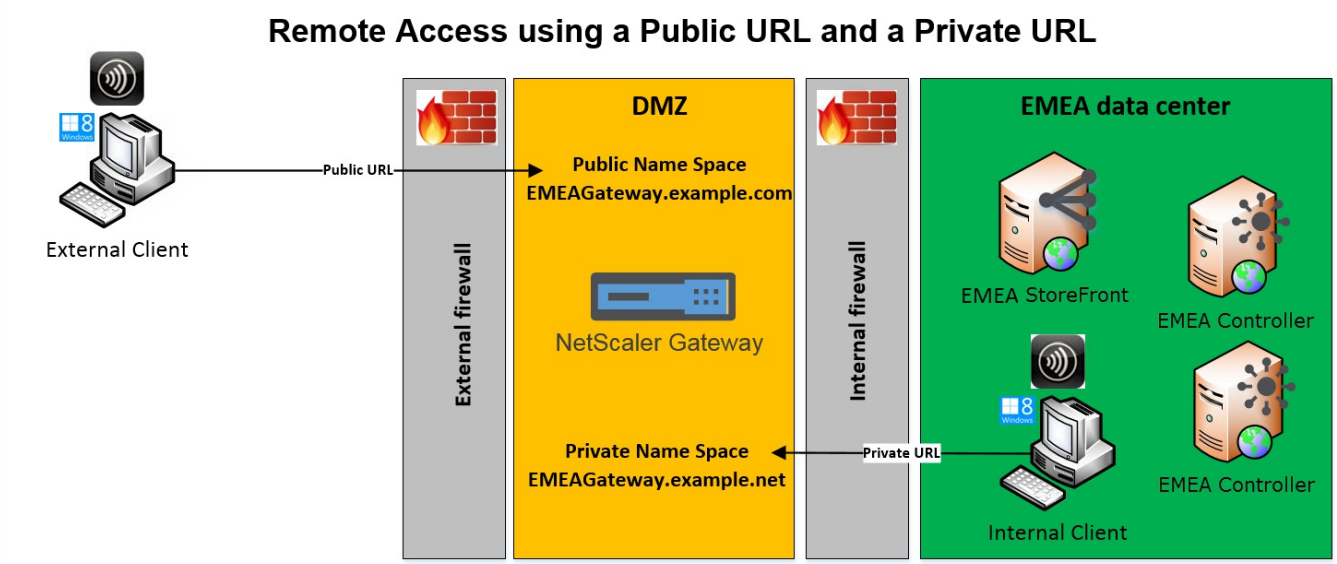
In diesem Beispiel:

- Jeder Standort bzw. jedes Datencenter enthält mindestens ein Gateway, mindestens einen StoreFront-Server und mindestens einen XenApp- und XenDesktop-Controller für veröffentlichte Ressourcen.

- Jeder für die GSLB Netscaler konfigurierte GSLB-Dienst in der globalen Bereitstellung repräsentiert einen virtuellen Gateway-VPN-Server. Alle StoreFront-Server in der Bereitstellung müssen so konfiguriert werden, dass sie alle virtuellen NetScaler Gateway-Server der GSLB-Schicht enthalten.
- Die GSLB-NetScaler Gateways werden im Aktiv/Aktiv-Modus verwendet, können aber auch ein Failover im Fall einer Störung bei der Netzwerkverbindung, bei DNS, dem Gateway, dem StoreFront-Server oder einem XenApp- und XenDesktop-Controller an einem Standort bieten. Die Benutzer werden automatisch an ein anderes Gateway weitergeleitet, wenn ein GSLB-Dienst ausfällt.
- Externe Clients werden bei Remoteverbindungen basierend auf dem konfigurierten GSLB-Lastausgleichsalgorithmus (z. B. Roundtripzeit oder statische Nähe) an das nächstgelegene Gateway weitergeleitet.
- Die eindeutige URL für jedes Gateway gestattet Benutzern die manuelle Auswahl des Datencenters zum Starten von Ressourcen.
- GSLB kann umgangen werden, wenn GSLB oder eine DNS-Delegierung nicht wie erwartet funktioniert. Die Benutzer können über die ortsspezifische URL weiterhin auf Remoteressourcen in beliebigen Datenzentren zugreifen, bis alle GSLB-Probleme behoben sind.

Anwendungsfall 2: ein NetScaler Gateway mit öffentlicher oder privater URL

Der Administrator verwendet dasselbe NetScaler Gateway für den externen Zugriff über eine öffentliche URL und für den internen Zugriff über eine private URL.



In diesem Beispiel:

- Der Administrator möchte, dass der gesamte Zugriff auf veröffentlichte Ressourcen und HDX-Startverkehr über ein NetScaler Gateway läuft, selbst wenn der Client intern ist.
- Das NetScaler Gateway ist in einer DMZ.
- Es gibt zwei Netzwerkrouten zum NetScaler Gateway über zwei Firewalls, jeweils eine auf jeder Seite der DMZ.
- Der öffentliche, externe Namespace unterscheidet sich von dem internen Namespace.

PowerShell-Cmdlet-Beispiele

Verwenden Sie die PowerShell-Cmdlets **Add-STFRoamingGateway** und **Set-STFRoamingGateway** mit dem Parameter "-gslburl" zum Festlegen des Attributs **GslbLocation** für das StoreFront-Gateway-Objekt. Beispiel:

Befehl KOPIEREN

```
Add-STFRoamingGateway -Name "EMEAGateway" -GatewayUrl "https://emeagateway.example.com" -GSLBurl "https://gslb.example.com

Set-STFRoamingGateway -Name "EMEAGateway" -GatewayUrl "https://emeagateway.example.com" -GSLBurl "https://gslb.example.com

Get-STFRoamingGateway -Name "EMEAGateway" (returns just the EMEA gateway object)

Or

Get-STFRoamingGateway (returns all gateway object configured in StoreFront)
```

Für Anwendungsfall 1 können Sie GSLBurl vom "EMEAGateway" entfernen, indem Sie **GslbLocation** auf NULL setzen. Der folgende PowerShell-Befehlt ändert das im Arbeitsspeicher gespeicherte Gatewayobjekt $EMEAGateway. **Set-STFRoamingGateway** kann dann $EMEAGateway übergeben werden, um die StoreFront-Konfiguration zu aktualisieren und GSLBurl zu entfernen.

Befehl KOPIEREN

```
$EMEAGateway = Get-STFRoamingGateway

$EMEAGateway.GslbLocation = $Null

Set-STFRoamingGateway -Gateway $EMEAGateway
```

Im Anwendungsfall 1 werden durch **Get-STFRoamingGateway** die folgenden Gateways zurückgegeben:

command KOPIEREN

```
Name: EMEAGateway

Location: https://emeagateway.example.com/ (Unique URL for the EMEA Gateway)

GslbLocation: https://gslb.example.com/ (GSLB URL for all three gateways)



Name: USGateway

Location: https://USgateway.example.com/ (Unique URL for the US Gateway)

GslbLocation: https://gslb.example.com/ (GSLB URL for all three gateways)



Name: APACGateway

Location: https://APACgateway.example.com/ (Unique URL for the APAC Gateway)

GslbLocation:  https://gslb.example.com/ (GSLB URL for all three gateways)
```

Im Anwendungsfall 2 werden durch **Get-STFRoamingGateway** die folgenden Gateways zurückgegeben:

command KOPIEREN

```
Name: EMEAGateway

Location: https://emeagateway.example.com/ (Public URL for the Gateway)

GslbLocation: https://emeagateway.example.net/ (Private URL for the Gateway)
```

Im Anwendungsfall 1 wird durch **Get STFStoreRegisteredOptimalLaunchGateway** "Optimal Gateway Routing" zurückgegeben:

command KOPIEREN

```
$StoreObject = Get-STFStoreService -SiteId 1 -VirtualPath "/Citrix/<YourStore>"

Get-STFStoreRegisteredOptimalLaunchGateway -StoreService $StoreObject



Hostnames:      {emeagateway.example.com, gslb.example.com}

Hostnames:      {usgateway.example.com, gslb.example.com}

Hostnames:      {apacgateway.example.com, gslb.example.com}
```

Die GSLB- oder interne URL für jedes Gateway wird in der Datei web.config des Roamingdiensts gespeichert

In der StoreFront-Verwaltungskonsole wird die GSLB-URL oder die interne URL aller Gateways nicht angezeigt. Der konfigurierte GSLBLocation-Pfad für alle GSLB-Gateways ist jedoch in der web.config-Datei des Roamingdiensts in C:\inetpub\wwwroot\Citrix\Roaming\web.config auf dem StoreFront-Server enthalten.

Anwendungsfall 1: Gateways in der web.config-Datei des Roamingdiensts

Anwendungsfall 2: Gateways in der web.config-Datei des Roamingdiensts

Konfigurieren von NetScaler und StoreFront für die delegierte Formularauthentifizierung (DFA)

Nov 27, 2017

Extensible Authentication bietet einen einzelnen Anpassungspunkt zur Erweiterung der formularbasierten Authentifizierung von NetScaler und StoreFront. Zum Erstellen einer Authentifizierungslösung mit dem Extensible Authentication-SDK müssen Sie die delegierte Formularauthentifizierung (DFA) zwischen NetScaler und StoreFront konfigurieren. Das Protokoll der delegierten Formularauthentifizierung ermöglicht die Erstellung und Verarbeitung von Authentifizierungsformularen, einschließlich Validierung der Anmeldeinformationen, zur Delegierung an eine andere Komponente. Beispiel: NetScaler delegiert seine Authentifizierung an StoreFront und StoreFront interagiert dann mit einem Drittanbieter-Authentifizierungsserver oder -dienst.

Installationsempfehlungen

- Zum Schützen der Kommunikation zwischen NetScaler und StoreFront verwenden Sie HTTPS anstelle von HTTP.
- Bei Clusterbereitstellungen stellen Sie sicher, dass auf allen Knoten das gleiche Serverzertifikat installiert und in der IIS HTTPS-Bindung konfiguriert ist, bevor Sie mit der Konfiguration beginnen.
- Stellen Sie sicher, dass in NetScaler der Aussteller des StoreFront-Serverzertifikats als vertrauenswürdige Zertifizierungsstelle eingerichtet ist, wenn in StoreFront HTTPS konfiguriert ist.

Überlegungen zur StoreFront-Clusterinstallation

- Installieren Sie das Authentifizierungs-Plug-In eines Drittanbieters auf allen Knoten bevor Sie diese gruppieren.
- Konfigurieren Sie alle Einstellungen für die delegierte Formularauthentifizierung auf einem Knoten und verteilen Sie die Änderungen auf die anderen. Weitere Informationen finden Sie unter "Aktivieren der delegierten Formularauthentifizierung".

Aktivieren der delegierten Formularauthentifizierung

Da es in StoreFront keine GUI-Option zur Einrichtung des vorinstallierten Schlüssels für Citrix gibt, installieren die delegierte Formularauthentifizierung mit der PowerShell-Konsole.

1. Installieren Sie die delegierte Formularauthentifizierung. Sie wird nicht standardmäßig installiert und muss mit der PowerShell-Konsole installiert werden.

```
PS C:\Users\administrator.PTD.000> cd 'C:\Program Files\Citrix\Receiver StoreFront\Scripts'
PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> & .\ImportModules.ps1
Adding snapins
Importing modules
Loading 'C:\Program Files\Citrix\Receiver StoreFront\\Admin\Citrix.DeliveryServices.ConfigurationProvider.dll'
Loading 'C:\Program Files\Citrix\Receiver StoreFront\\Admin\Citrix.DeliveryServices.ConfigurationProvider.dll'

PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> Install-DSDFAServer
Id                    : bf694fbc-ae0a-4d56-8749-c945559e897a
ClassType             : e1eb3668-9c1c-4ad8-bbae-c08b2682c1bc
FrameworkController   : Citrix.DeliveryServices.Framework.FileBased.FrameworkController
ParentInstance        : 8dd182c7-f970-466c-ad4c-27a5980f716c
RootInstance          : 5d0cdc75-1dee-4df7-8069-7375d79634b3
TenantId              : 860e9401-39c8-4f2c-928d-34251102b840
Data                  : {}
ReadOnlyData          : {[Name, DelegatedFormsServer], [Cmdlet, Add-DSWebFeature], [Snapin, Citrix.DeliverySer
                        vices.Web.Commands], [Tenant, 860e9401-39c8-4f2c-928d-34251102b840]}
ParameterData         : {[FeatureClassId, e1eb3668-9c1c-4ad8-bbae-c08b2682c1bc], [ParentInstanceId, 8dd182c7-f
                        970-466c-ad4c-27a5980f716c], [TenantId, 860e9401-39c8-4f2c-928d-34251102b840]}
AdditionalInstanceDependencies : {b1e48ef0-b9e5-4697-af9b-0910062aa2a3}
```

```
IsDeployed          : True
FeatureClass        : Citrix.DeliveryServices.Framework.Feature.FeatureClass
```

2. Fügen Sie Citrix Trusted Client hinzu. Konfigurieren Sie den gemeinsamen geheimen Schlüssel (Passphrase) zwischen StoreFront und NetScaler. Passphrase und Client-ID müssen mit den in NetScaler konfigurierten identisch sein.
   ```
   PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> Add-DSCitrixPSKTrustedClient -clientId netscaler.fqdn.com -passphrase secret
   ```
3. Richten Sie die Formularkonversationsfactory für die delegierte Formularauthentifizierung für die Leitung des gesamten Datenverkehrs an das benutzerdefinierte Formular ein. Suchen Sie die Formularkonversationsfactory, indem Sie in C:\inetpub\wwwroot\Citrix\Authentication\web.config nach ConversationFactory suchen. Der Abschnitt kann wie folgendes Beispiel aussehen:

4. Legen Sie die Formularkonversationsfactory für die delegierte Formularauthentifizierung in PowerShell fest. In diesem Beispiel ist dies ExampleBridgeAuthentication.
   ```
   PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> Set-DSDFAProperty -ConversationFactory ExampleBridgeAuthentication
   ```

Bei den Argumenten in PowerShell wird nicht zwischen Groß- und Kleinschreibung unterschieden: -ConversationFactory ist identisch mit conversationfactory.

Deinstallieren von StoreFront

Bevor Sie StoreFront deinstallieren, deinstallieren Sie jegliche Authentifizierungs-Plug-Ins von Drittanbietern, da diese sich auf die Funktionalität von StoreFront auswirken.

Authentifizierung mit andere Domänen

Nov 27, 2017

Einige Organisationen nutzen Richtlinien, die es nicht gestatten, externen Entwicklern oder Auftragnehmern Zugriff auf veröffentlichte Ressourcen in einer Produktionsumgebung zu geben. In diesem Artikel wird erläutert, wie Sie Zugriff auf veröffentlichte Ressourcen in einer Testumgebung geben, indem Sie die Authentifizierung über NetScaler Gateway mit einer Domäne ermöglichen. Die Authentifizierung bei StoreFront und die Receiver für Web-Site kann dann über eine andere Domäne erfolgen. Die in diesem Artikel beschriebene Authentifizierung über NetScaler Gateway wird für Benutzer unterstützt, die sich über die Receiver für Web-Site anmelden. Diese Authentifizierungsmethode wird nicht für Citrix Receiver für native Desktops oder mobile Geräte unterstützt.

Einrichten einer Testumgebung

In diesem Beispiel werden die Produktionsdomäne "production.com" und die Testdomäne "development.com" verwendet.

Domäne "production.com"

Die Domäne "production.com" ist im Beispiel wie folgt eingerichtet:

- NetScaler Gateway mit konfigurierter LDAP-Authentifizierungsrichtlinie für "production.com".
- Die Authentifizierung über das Gateway erfolgt mit einem Konto vom Typ production\testuser1 plus Kennwort.

Domäne "development.com"

Die Domäne "development.com" ist im Beispiel wie folgt eingerichtet:

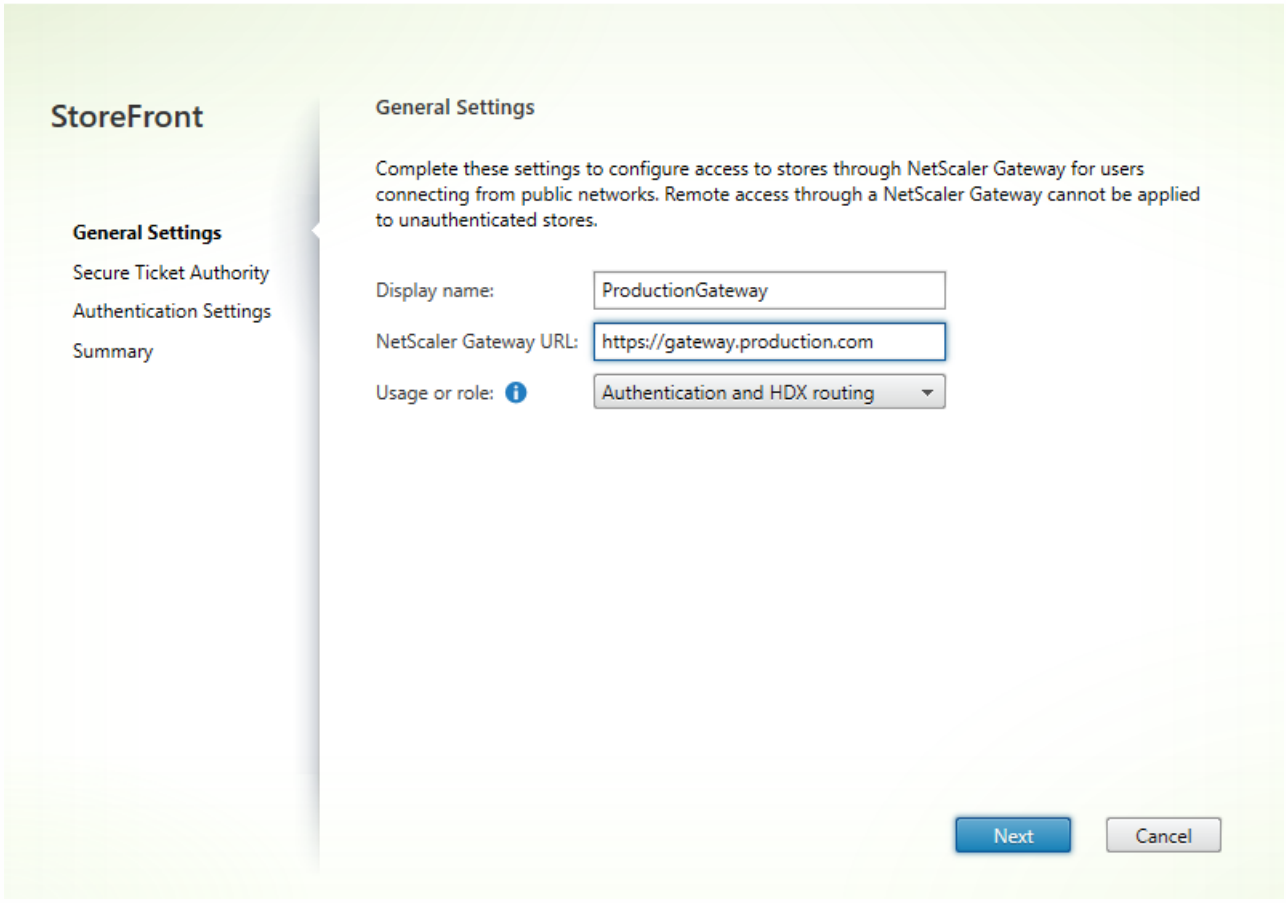
- StoreFront, XenApp und XenDesktop 7.0 oder höher und VDAs sind alle in der Domäne "development.com".
- Die Authentifizierung bei der Citrix Receiver für Web-Site erfolgt mit einem Konto vom Typ development\testuser1 plus Kennwort.
- Es besteht keine Vertrauensstellung zwischen den beiden Domänen.

Konfigurieren eines NetScaler Gateways für den Store

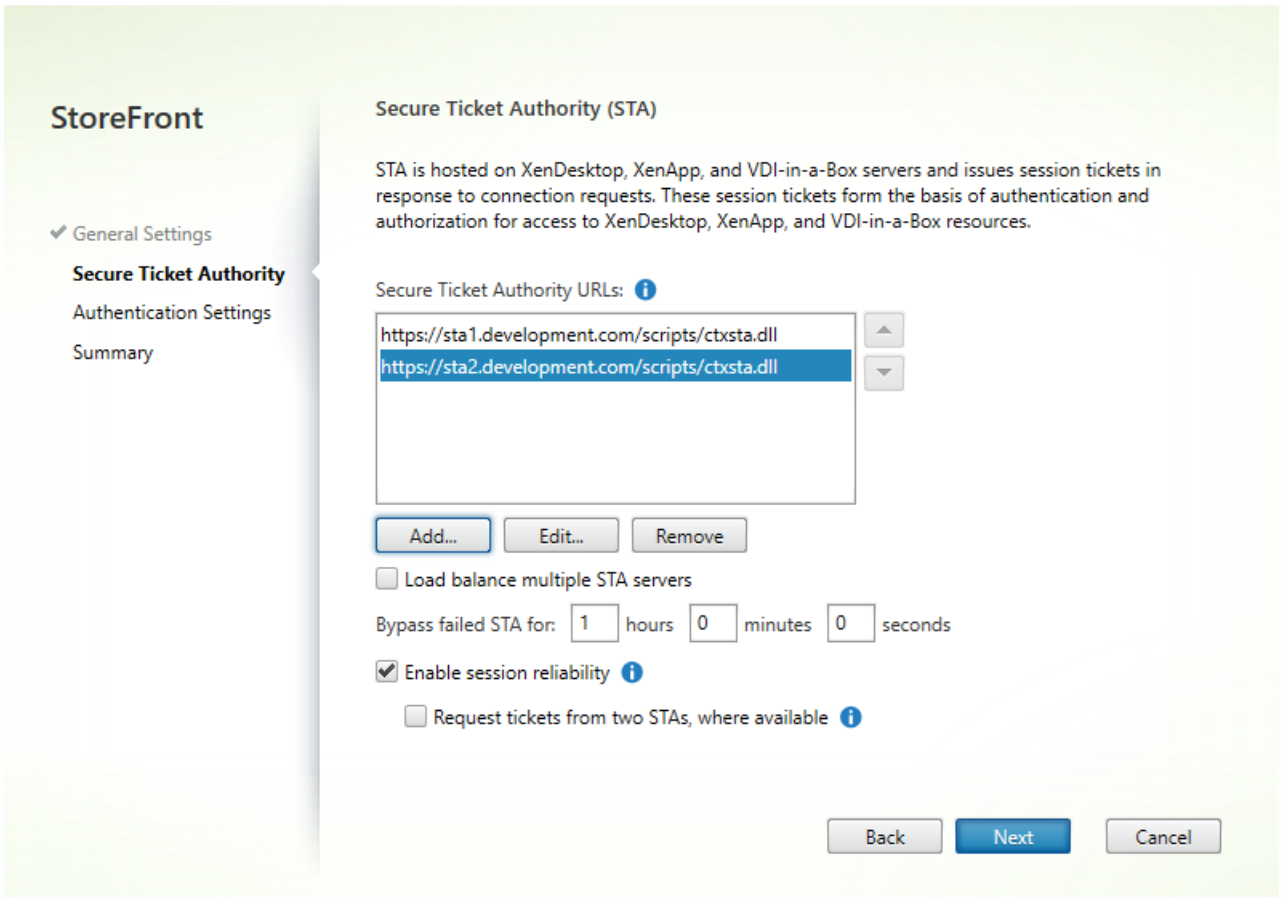
Konfigurieren eines NetScaler Gateways für den Store:

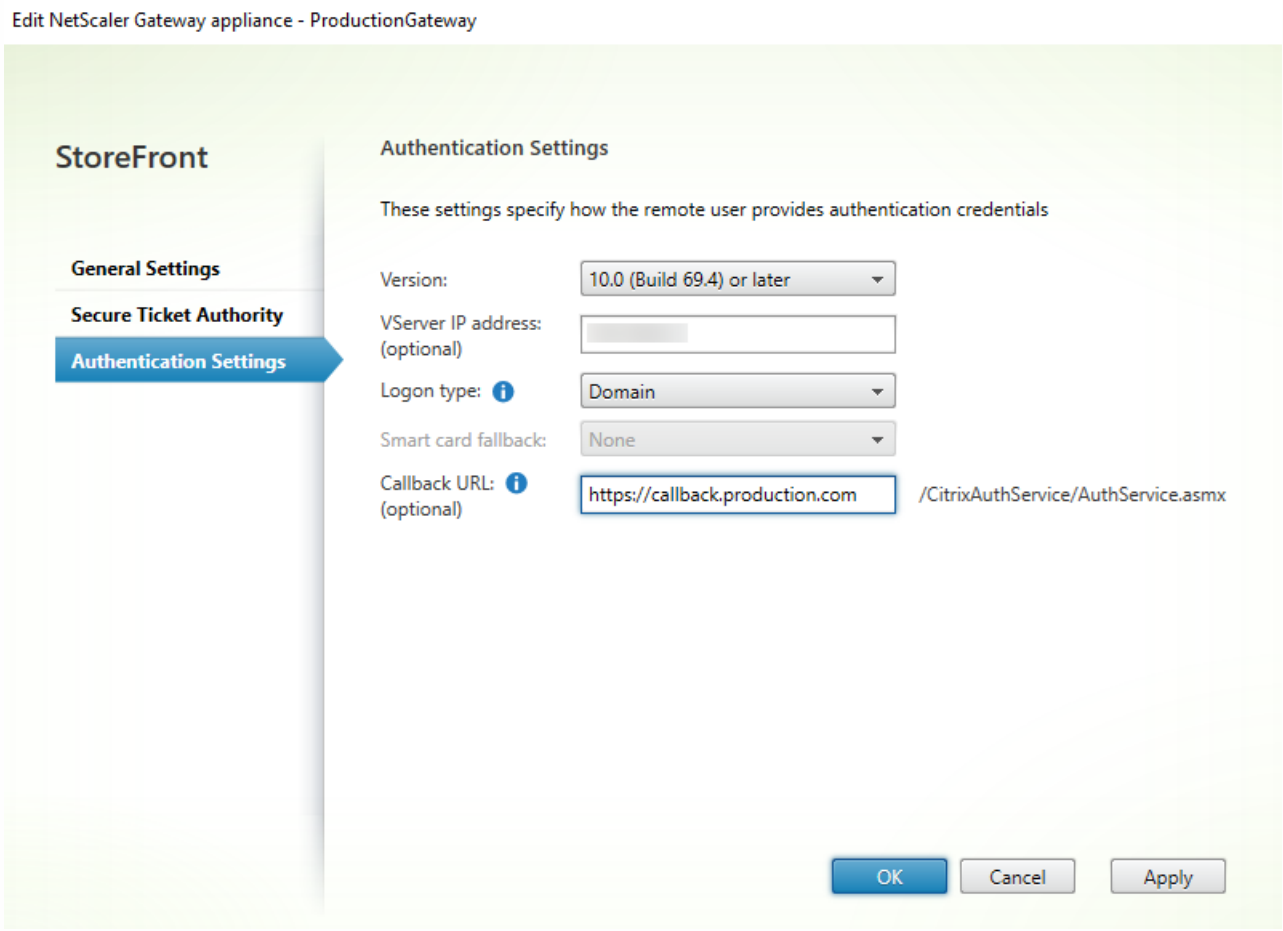
1. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole **Stores** aus und klicken Sie im Bereich **Aktionen** auf **NetScaler Gateways verwalten**.
2. Klicken Sie auf dem Bildschirm "NetScaler Gateways verwalten" auf die Schaltfläche **Hinzufügen**.
3. Legen Sie die Einstellungen für "Allgemeine Einstellungen", "Secure Ticket Authority" und "Authentifizierung" fest.

Add NetScaler Gateway Appliance



Add NetScaler Gateway Appliance



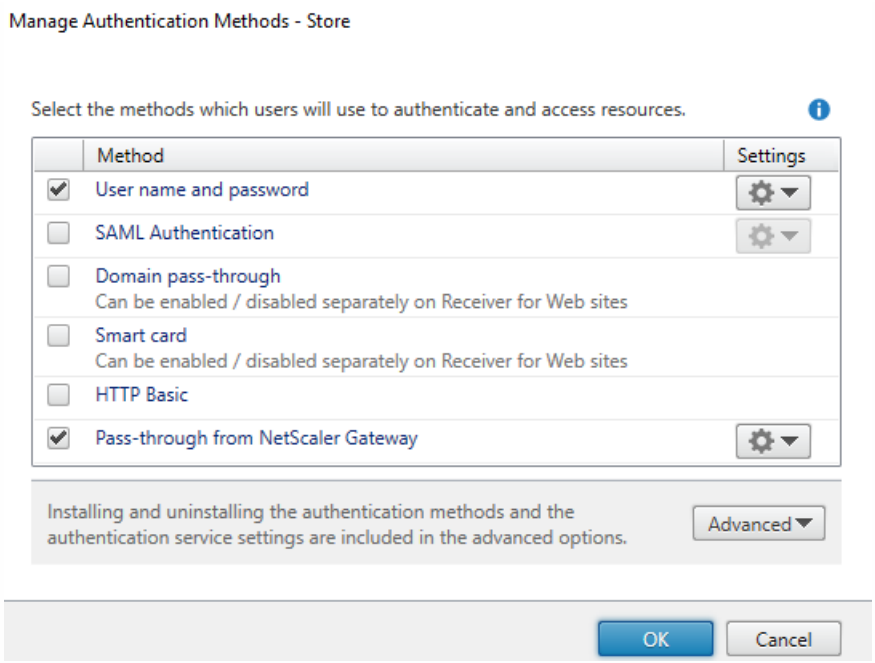


Hinweis

Bedingte DNS-Weiterleitungen müssen ggf. hinzugefügt werden, damit DNS-Server in beiden Domänen FQDNs in der anderen Domäne auflösen können. NetScaler muss die FQDNs des STA-Servers in der Domäne "development.com" auflösen können, indem es den DNS-Server von "production.com" verwendet. StoreFront muss außerdem die Rückruf-URL in der Domäne "production.com" auflösen können, indem es den DNS-Server von "development.com" verwendet. Als Alternative kann ein FQDN von "development.com" verwendet werden, der in die virtuelle IP-Adresse (VIP) des virtuellen NetScaler Gateway-Servers aufgelöst wird.

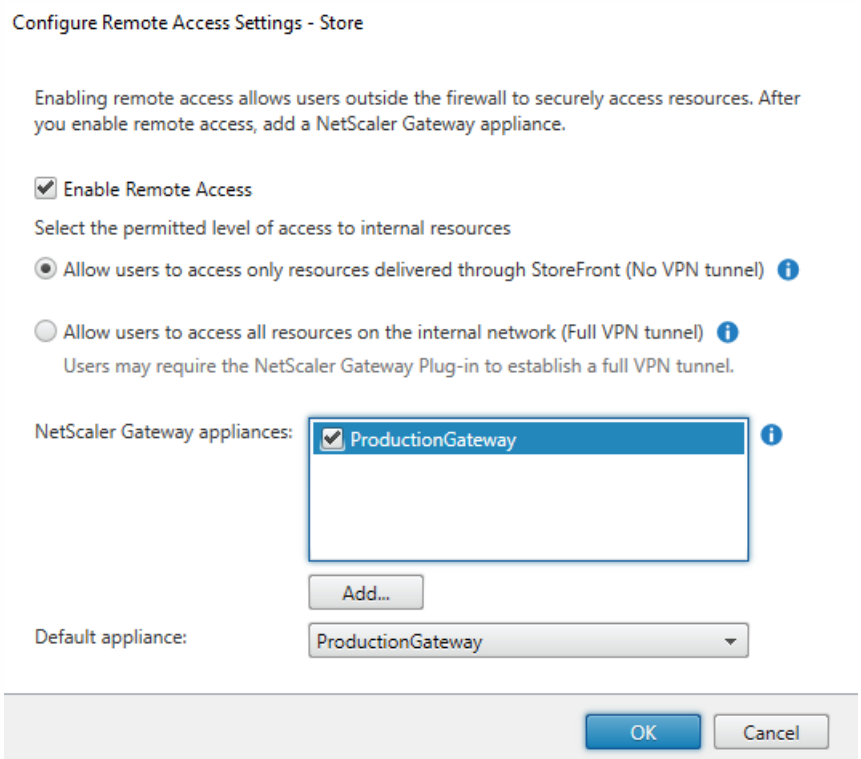
Aktivieren der Passthrough-Authentifizierung von NetScaler Gateway

1. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole **Stores** aus und klicken Sie im Bereich **Aktionen** auf **Authentifizierungsmethoden verwalten**.
2. Aktivieren Sie auf dem Bildschirm "Authentifizierungsmethoden verwalten" die Option **Passthrough-Authentifizierung von NetScaler Gateway**.
3. Klicken Sie auf **OK**.



Konfigurieren des Stores für einen Remotezugriff über Gateway

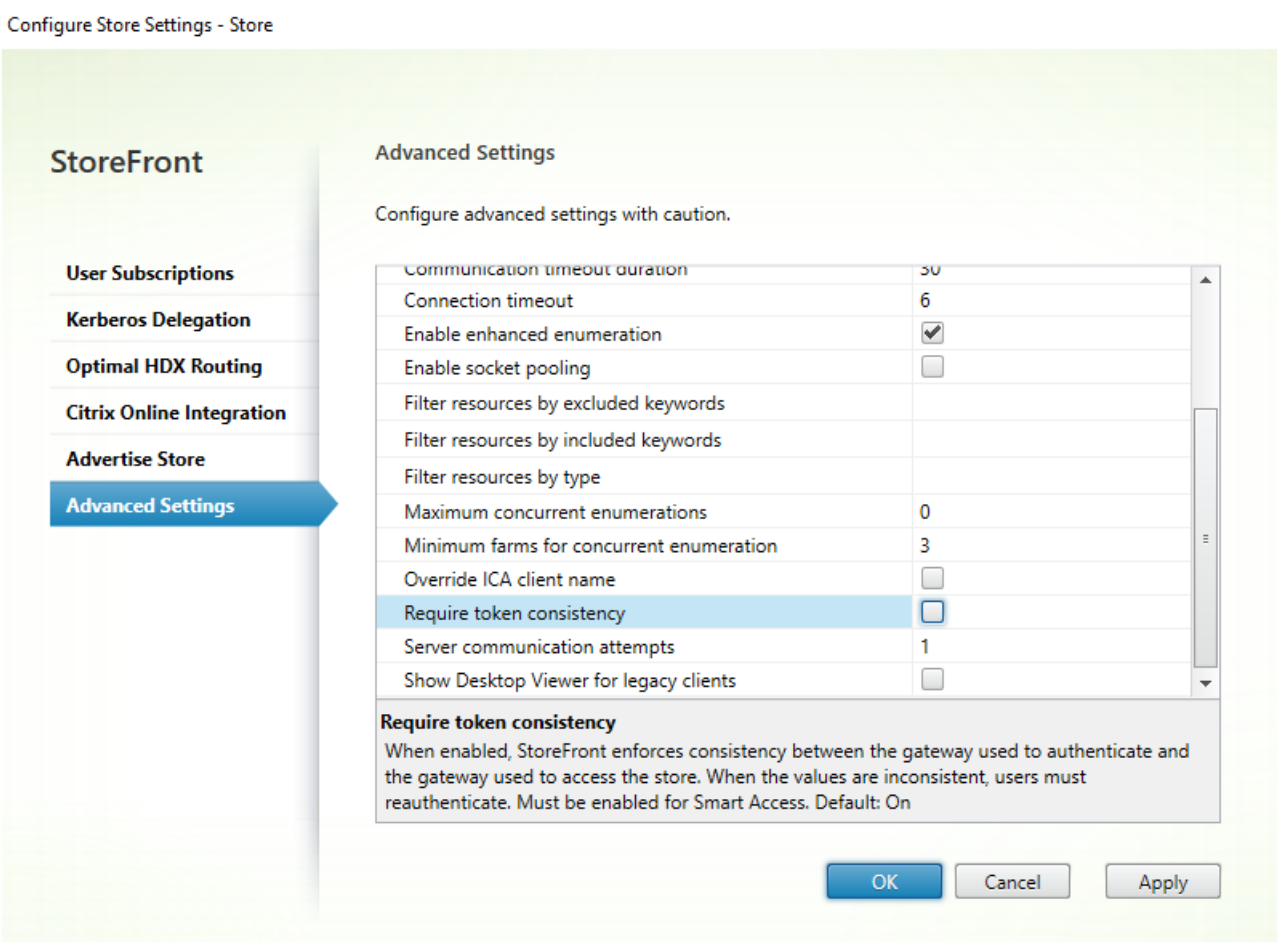
1. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores** und im Ergebnisbereich einen Store aus. Klicken Sie im Bereich **Aktionen** auf **Remotezugriffeinstellungen konfigurieren**.
2. Wählen Sie **Remotezugriff aktivieren**.
3. Stellen Sie sicher, dass Sie NetScaler Gateway beim Store registriert haben. Wenn NetScaler Gateway nicht registriert ist, können keine STA-Sitzungstickets erstellt werden.



Deaktivieren der Tokenkonsistenz

1. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores** und im Ergebnisbereich einen Store aus. Klicken Sie im Bereich **Aktionen** auf **Storeeinstellungen konfigurieren**.

2. Wählen Sie auf der Seite "Storeeinstellungen konfigurieren" die Option **Erweiterte Einstellungen** aus.
3. Deaktivieren Sie das Kontrollkästchen **Tokenkonsistenz erforderlich**. Weitere Informationen finden Sie unter Erweiterte Storeeinstellungen.
4. Klicken Sie auf **OK**.



Hinweis

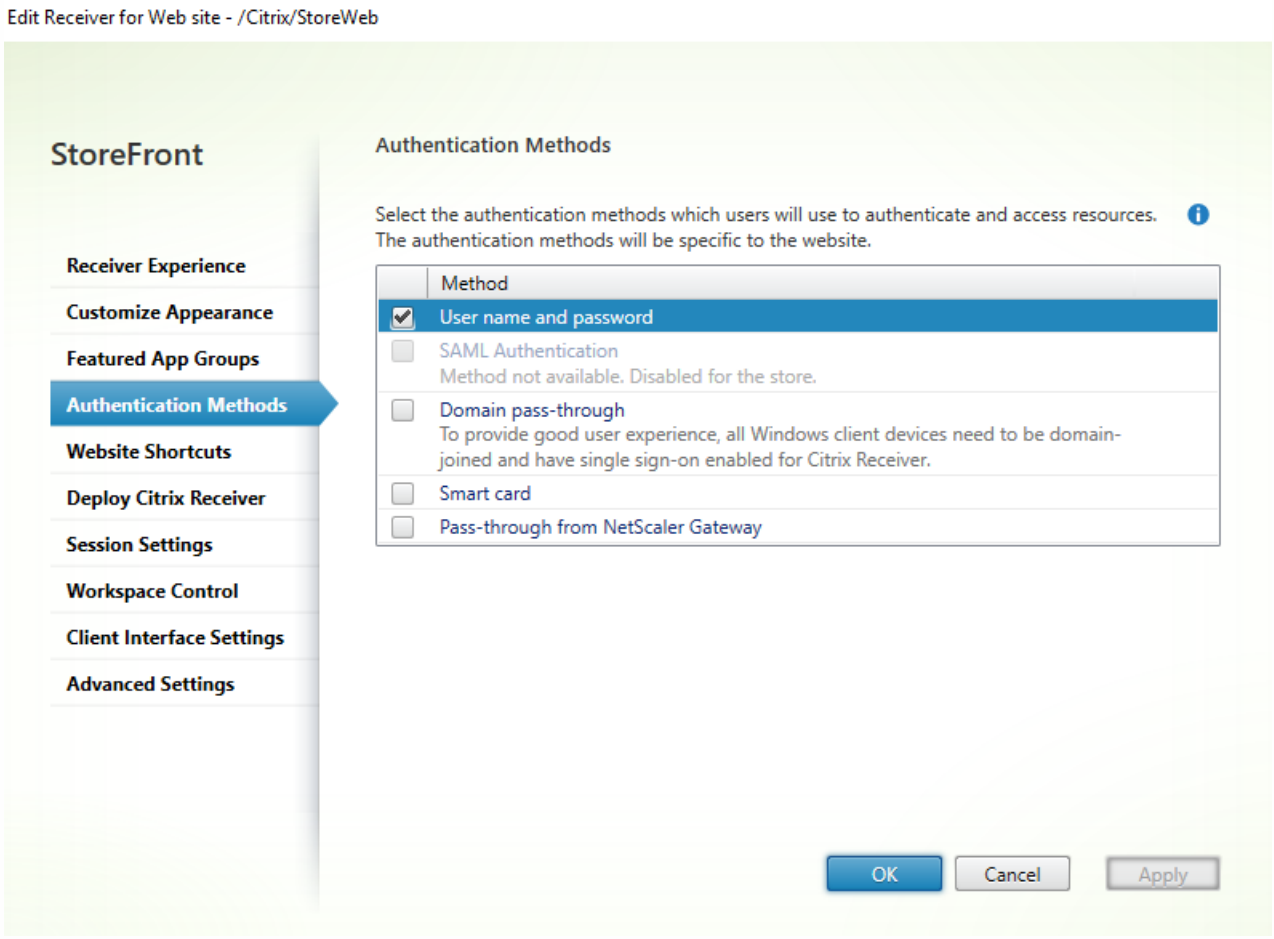
Die Einstellung "Tokenkonsistenz erforderlich" ist standardmäßig aktiviert. Wenn Sie diese Einstellung deaktivieren, funktionieren SmartAccess-Features für die NetScaler Endpunktanalyse (EPA) nicht mehr. Weitere Informationen zu SmartAccess finden Sie unter CTX138110.

Deaktivieren der Passthrough-Authentifizierung von NetScaler Gateway für die Receiver für Web-Site

Important

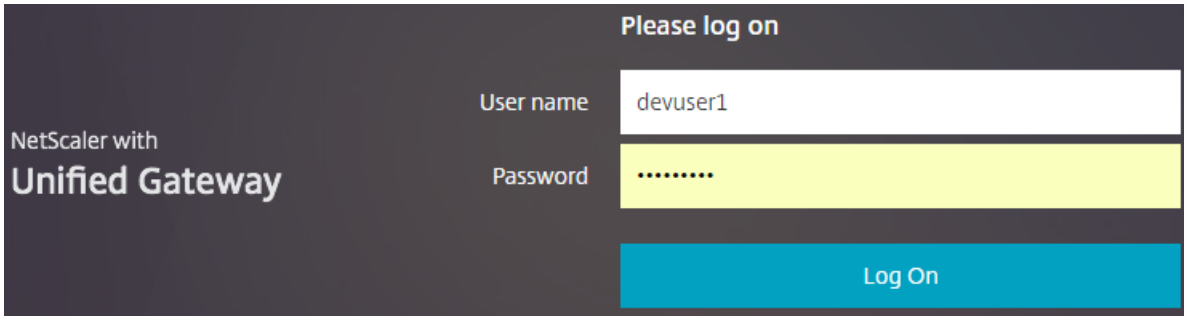
Durch Deaktivieren der Passthrough-Authentifizierung von NetScaler Gateway wird verhindert, dass Receiver für Web die falschen Anmeldeinformationen der Domäne "production.com" verwendet, die von NetScaler weitergegeben wurden. Bei deaktivierter Passthrough-Authentifizierung von NetScaler Gateway wird der Benutzer von Receiver für Web zur Eingabe der Anmeldeinformationen aufgefordert. Diese Anmeldeinformationen unterscheiden sich von den Anmeldeinformationen, die zur Anmeldung über Netscaler Gateway verwendet werden.

1. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores** aus.
2. Wählen Sie den **Store** aus, den Sie ändern möchten.
3. Klicken Sie im Bereich **Aktionen** auf **Receiver für Web-Sites verwalten**.
4. Deaktivieren Sie unter "Authentifizierungsmethoden" das Kontrollkästchen "Passthrough-Authentifizierung von NetScaler Gateway".
5. Klicken Sie auf **OK**.

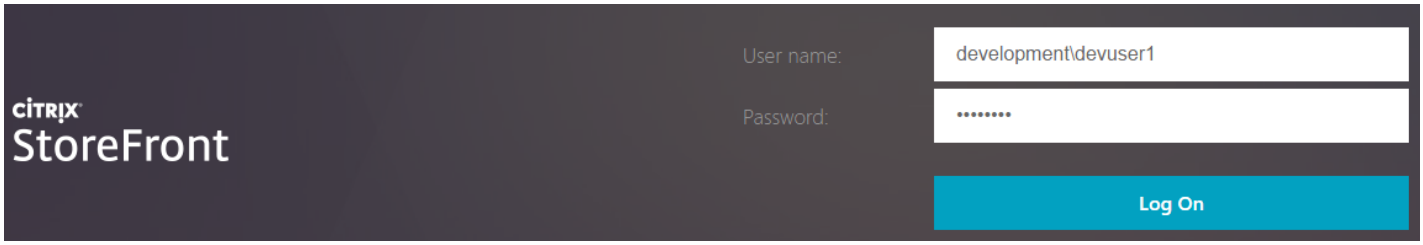


Anmeldung beim Gateway mit einem Benutzerkonto und Anmeldeinformationen von "production.com"

Melden Sie sich zum Test beim Gateway mit einem Benutzerkonto und Anmeldeinformationen von "production.com" an.



Nach der Anmeldung wird der Benutzer aufgefordert, die Anmeldeinformationen von "development.com" einzugeben.

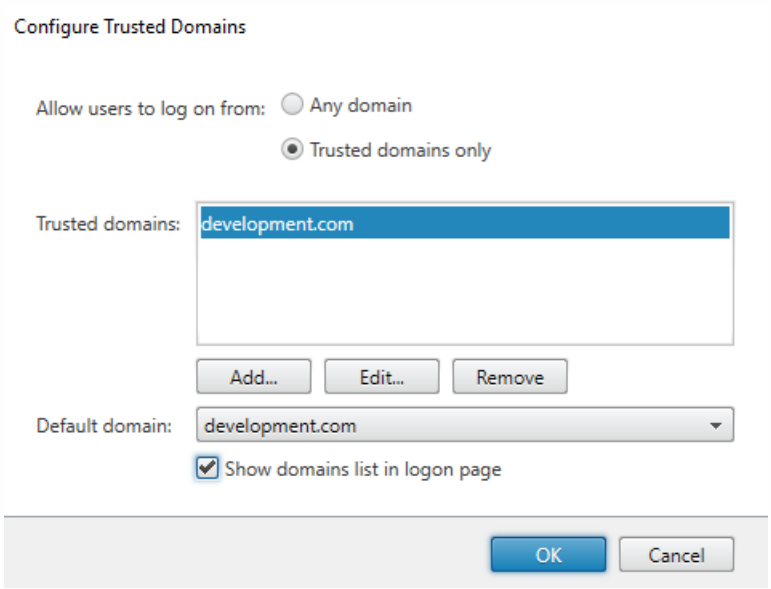


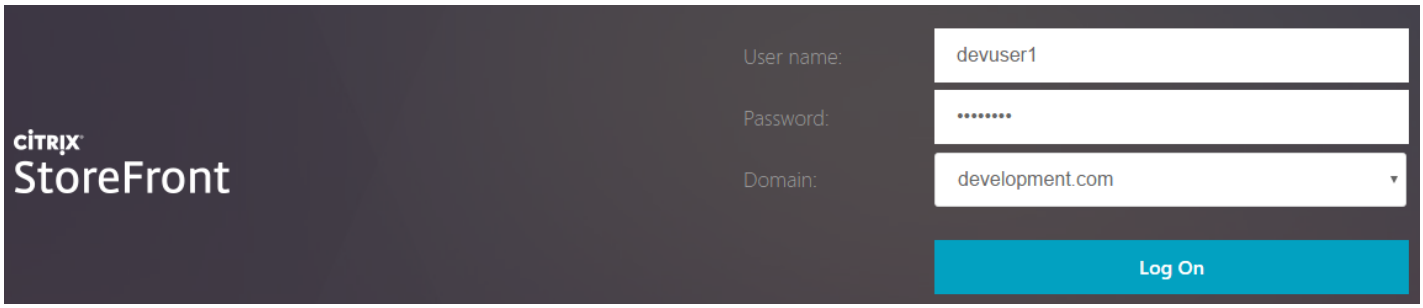
Hinzufügen einer Dropdownliste vertrauenswürdiger Domänen in StoreFront (optional)

Mit dieser optional verfügbaren Einstellung kann verhindert werden, dass Benutzer versehentlich die falsche Domäne zur Authentifizierung über NetScaler Gateway eingeben.

Wenn der Benutzername für beide Domänen gleich ist, ist die Eingabe der falschen Domäne wahrscheinlicher. Neue Benutzer können auch gewohnt sein, keine Domäne bei der Anmeldung über NetScaler Gateway anzugeben. Benutzer können dann vergessen, domäne\benutzername für die zweite Domäne einzugeben, wenn sie aufgefordert werden, sich bei der Receiver für Web-Site anzumelden.

1. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole **Stores** aus und klicken Sie im Bereich **Aktionen** auf **Authentifizierungsmethoden verwalten**.
2. Klicken Sie auf den Dropdownpfeil neben **Benutzername und Kennwort**.
3. Klicken Sie auf **Hinzufügen**, um "development.com" als vertrauenswürdige Domäne hinzuzufügen, und aktivieren Sie das Kontrollkästchen **Domänenliste auf Anmeldeseite anzeigen**.
4. Klicken Sie auf **OK**.



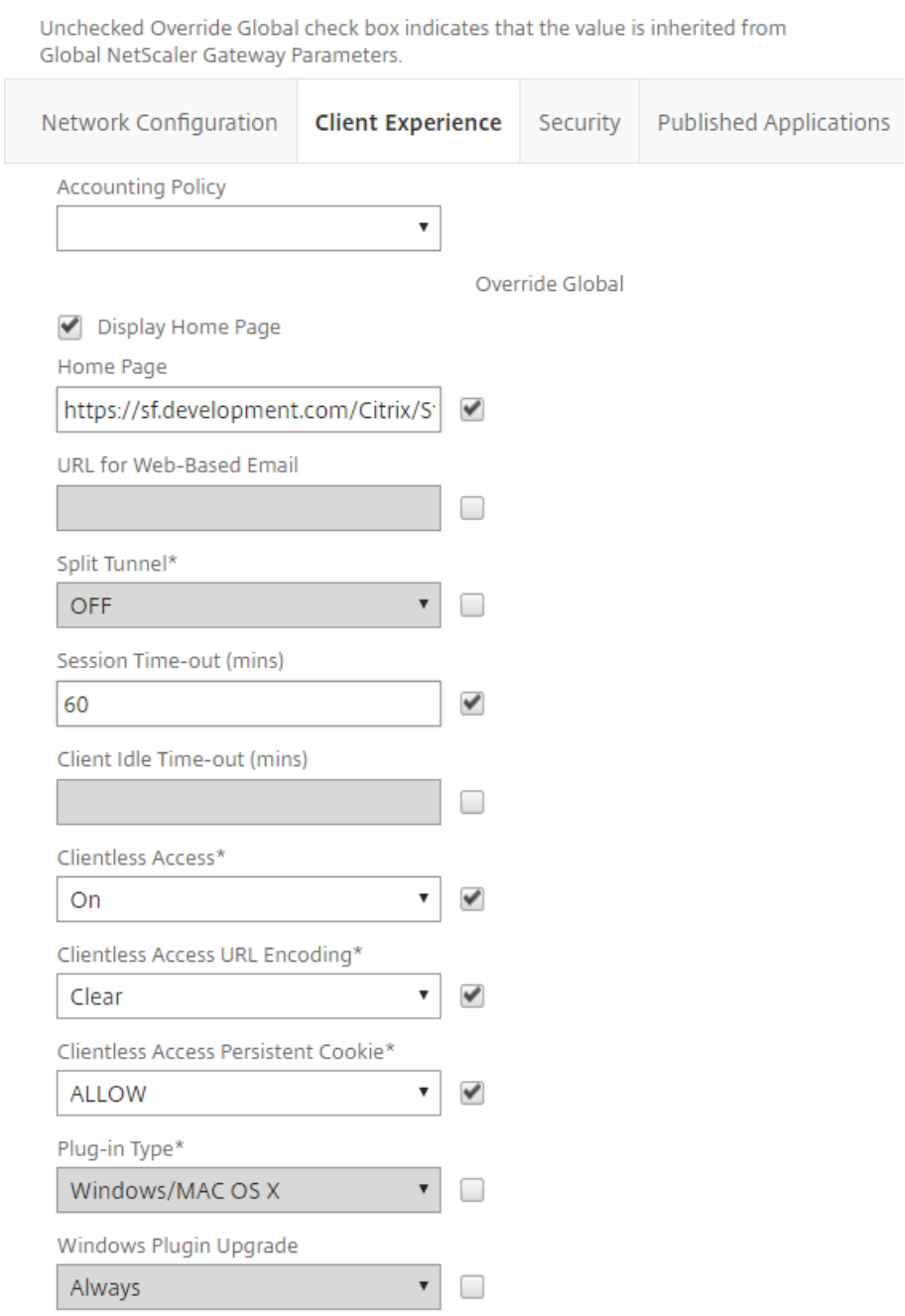


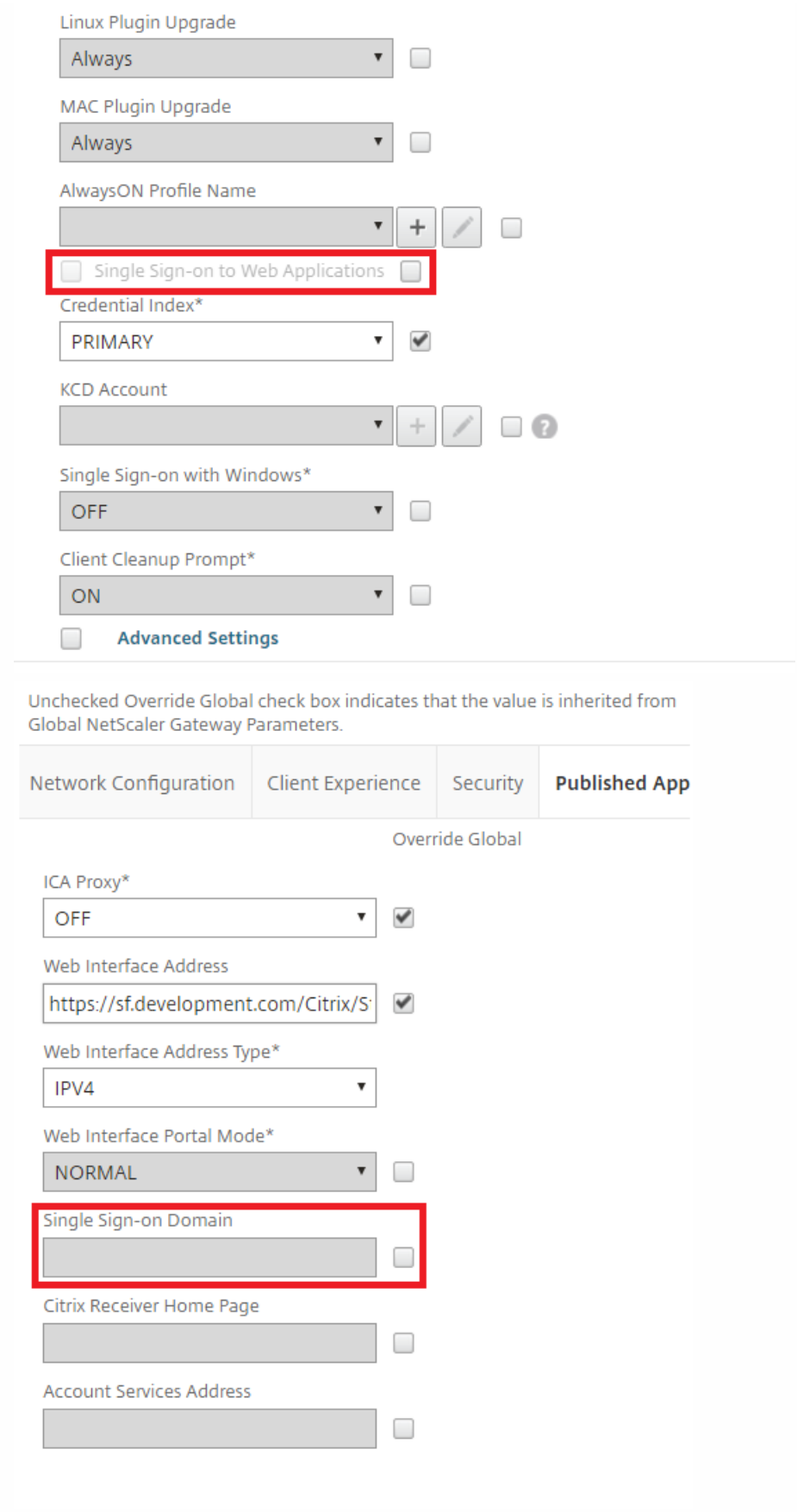
Hinweis

> Die Kennwortzwischenspeicherung im Browser wird für dieses Authentifizierungsszenario nicht empfohlen. Wenn Benutzer unterschiedliche Kennwörter für die beiden Domänenkonten verwenden, kann die Kennwortzwischenspeicherung zu Fehlern führen.

Aktionsrichtlinie für NetScaler-Sitzungen mit clientlosem VPN (CVPN)

- Bei aktiviertem Single Sign-On für Webanwendungen in der NetScaler-Sitzungsrichtlinie ignoriert Receiver für Web falsche Anmeldeinformationen, die von NetScaler gesendet wurden, da die Authentifizierungsmethode **Passthrough-Authentifizierung von NetScaler Gateway** auf der Receiver für Web-Site deaktiviert ist. Receiver für Web fordert Benutzer zur Eingabe der Anmeldeinformationen auf, unabhängig von der gewählten Einstellung für diese Option.
- Das Ausfüllen der Single Sign-On-Einträge auf den Registerkarten "Client Experience" und "Published Apps" in NetScaler ändert nicht das in diesem Artikel beschriebene Verhalten.





Konfigurieren von Beacons

Nov 27, 2017

Mit der Aufgabe Beacons verwalten können Sie URLs innerhalb und außerhalb des internen Netzwerks angeben, die als Beacons verwendet werden sollen. Citrix Receiver versucht eine Kontaktaufnahme mit den Beacons und ermittelt anhand der Antworten, ob Benutzer mit lokalen oder öffentlichen Netzwerken verbunden sind. Wenn ein Benutzer auf einen Desktop oder eine Anwendung zugreift, werden die Standortinformationen an den Server mit der Ressource weitergegeben, sodass die entsprechenden Verbindungsinformationen an Citrix Receiver zurückgegeben werden können. Dadurch wird sichergestellt, dass Benutzer nicht aufgefordert werden, sich neu anmelden, wenn sie auf einen Desktop oder eine Anwendung zugreifen.

Beispiel: Wenn der interne Beacon zugänglich ist, ist der Benutzer mit dem lokalen Netzwerk verbunden. Wenn Citrix Receiver den internen Beacon nicht kontaktieren kann und Antworten von beiden externen Beacons empfängt, hat der Benutzer eine Internetverbindung, ist jedoch außerhalb des Unternehmensnetzwerks. Daher muss der Benutzer eine Verbindung mit Desktops und Anwendungen über NetScaler Gateway herstellen. Wenn ein Benutzer auf einen Desktop oder eine Anwendung zugreift, wird der Server mit der Ressource benachrichtigt, um Details zum NetScaler Gateway-Gerät, über das die Verbindung geleitet werden muss, bereitzustellen. Dies bedeutet, dass der Benutzer sich beim Zugriff auf den Desktop oder die Anwendung nicht am Gerät anmelden muss.

Standardmäßig verwendet StoreFront die Server-URL oder die Lastausgleichs-URL der Bereitstellung als internen Beacon. Die URLs der Citrix Website und des virtuellen Servers oder Benutzeranmeldepunkts (Access Gateway 5.0) der zuerst hinzugefügten NetScaler Gateway-Bereitstellung werden standardmäßig als externe Beacons verwendet.

Wenn Sie Beacons ändern, müssen Sie sicherstellen, dass Benutzer Citrix Receiver mit den geänderten Beaconinformationen aktualisieren. Bei der Konfiguration einer Receiver fürWeb-Site für einen Store können Benutzer eine aktualisierte Citrix Receiver-Provisioningdatei von der Site beziehen. Andernfalls können Sie eine Provisioningdatei für den Store exportieren und diese Datei für die Benutzer verfügbar machen.

Wichtig: Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Wenn Sie die Änderungen vorgenommen haben, übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden.

1. Klicken Sie auf der Windows-Startseite oder auf der Apps-Seite auf die Kachel Citrix StoreFront.
2. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores** aus und klicken Sie im Bereich Aktionen auf Beacons verwalten.
3. Geben Sie die URL für die Verwendung als interner Beacon an.
   - Zum Verwenden der Server-URL oder der Lastausgleichs-URL der StoreFront-Bereitstellung, wählen Sie Dienst-URL verwenden.
   - Zum Verwenden einer anderen URL wählen Sie Beaconadresse angeben und geben Sie eine hoch verfügbare URL im internen Netzwerk an.
4. Klicken Sie auf Hinzufügen, um die URL eines externen Beacons hinzuzufügen. Zum Ändern eines Beacons wählen Sie die URL in der Liste Externe Beacons aus und klicken Sie auf Bearbeiten. Wählen Sie eine URL in der Liste aus und klicken Sie auf Entfernen, um die Verwendung der Adresse als Beacon zu beenden.
   Sie müssen mindestens zwei hoch verfügbare externe Beacons, die von öffentlichen Netzwerken aus aufgelöst werden können, angeben. Die Beacon-URLs müssen vollqualifizierte Domänennamen sein (http://example.com), verwenden Sie keine abgekürzten NetBIOS-Namen (http://example). So kann Citrix Receiver ermitteln, ob Benutzer hinter einer Internetpaywall sind, z. B. in einem Hotel oder Internetcafé. In solchen Fällen stellen alle externen Beacons eine

Verbindung mit demselben Proxy her.

Erweiterte Konfigurationen

Nov 27, 2017

Bei StoreFront können Sie erweiterte Optionen über PowerShell, Zertifikateigenschaften oder Konfigurationsdateien mit der StoreFront-Konsole konfigurieren.

Konfigurieren von Desktopgerätesites	Erstellen, Entfernen und Ändern von Desktopgerätesites.
Erstellen eines einzelnen vollqualifizierten Domänennamens (FQDN) für den internen und externen Zugriff auf einen Store	Ermöglicht den Zugriff auf Ressourcen aus dem Unternehmensnetzwerk und aus dem Internet durch ein NetScaler Gateway und vereinfacht die Benutzererfahrung durch Erstellen eines einzelnen FQDN für interne und externe Roamingclients.
Konfigurieren der Ressourcenfilterung	Filtern von Enumerationsressourcen nach Ressourcentyp und Schlüsselwörtern.

Konfigurieren von Desktopgerätesites

Nov 27, 2017

Die folgenden Anleitungen beschreiben, wie Sie Desktopgerätesites erstellen, löschen und ändern. Sie führen Windows PowerShell-Befehle aus, um Sites zu erstellen und zu entfernen. Sie ändern die Einstellungen für die Desktopgerätesite, indem Sie die Sitekonfigurationsdateien bearbeiten.

Wichtig: Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Wenn Sie die Änderungen vorgenommen haben, übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden.
Hinweis: Die StoreFront- und PowerShell-Konsolen können nicht gleichzeitig geöffnet sein. Schließen Sie immer zuerst die StoreFront-Verwaltungskonsole, bevor Sie die PowerShell-Konsole zum Verwalten der StoreFront-Konfiguration öffnen. Schließen Sie gleichermaßen immer alle Instanzen von PowerShell, bevor Sie die StoreFront-Konsole öffnen.

Erstellen oder Entfernen von Desktopgerätesites

Über jede Desktopgerätesite kann nur auf einen einzelnen Store zugegriffen werden. Sie können einen Store mit allen Ressourcen für Benutzer mit Desktopgeräten erstellen, die nicht in der Domäne sind. Alternativ, erstellen Sie separate Stores mit jeweils einer Desktopgerätesite und konfigurieren Sie die Desktopgeräte des Benutzers für die Verbindung mit der entsprechenden Site.

1. Starten Sie Windows PowerShell von einem Konto mit lokalen Administratorrechten und geben Sie an der Eingabeaufforderung den folgenden Befehl ein, damit die StoreFront-Module importiert werden.
   & "installationlocation\Scripts\ImportModules.ps1"
   installationlocation ist das Verzeichnis, in dem StoreFront installiert ist (in der Regel C:\Programme\Citrix Receiver StoreFront\).

2. Um eine neue Desktopgerätesite zu erstellen, geben Sie den folgenden Befehl ein.
   Install-DSDesktopAppliance -FriendlyName sitename -SiteId iisid
   -VirtualPath sitepath -UseHttps {$False | $True}
   -StoreUrl storeaddress [-EnableMultiDesktop {$False | $True}]
   [-EnableExplicit {$True | $False}] [-EnableSmartCard {$False | $True}]
   [-EnableEmbeddedSmartCardSSO {$False | $True}]
   sitename ist ein Name, mit dem Sie die Desktopgerätesite leichten identifizieren können. Geben Sie für iisid die numerische ID der Microsoft Internetinformationsdienste-Website (IIS) ein, von der StoreFront gehostet wird. Diese ID ist der IIS-Verwaltungskonsole zu entnehmen. Ersetzen Sie sitepath durch den relativen Pfad, unter dem die Site in IIS erstellt werden soll, z. B. /Citrix/DesktopAppliance. Beachten Sie, dass bei Desktopgerätesite-URLszwischen Groß- und Kleinschreibung unterschieden wird.

   Geben Sie an, ob StoreFront für HTTPS konfiguriert ist, indem Sie für -UseHttps den entsprechenden Wert einstellen.

   Verwenden Sie StoreUrl storeaddress, um die absolute URL für den Storedienst anzugeben, der von der Desktop Appliance Connector-Site verwendet wird. Dieser Wert wird für die Storezusammenfassung in der Verwaltungskonsole angezeigt.

   Standardmäßig wird automatisch der erste dem Benutzer verfügbare Desktop gestartet, wenn ein Benutzer sich an einer Desktopgerätesite anmeldet. Um die neue Desktopgerätesite so konfigurieren, dass Benutzer ggf. zwischen mehreren Desktops wählen können, setzen Sie -EnableMultiDesktop auf $True.

Die explizite Authentifizierung ist standardmäßig für neue Sites aktiviert. Sie können die explizite Authentifizierung deaktivieren, indem Sie das Argument -EnableExplicit auf $False setzen. Aktivieren Sie die Smartcardauthentifizierung, indem Sie -EnableSmartCard auf $True setzen. Um die Passthrough-Authentifizierung mit Smartcards zu aktivieren, müssen Sie -EnableSmartCard und -EnableEmbeddedSmartCardSSO auf $True setzen. Wenn Sie die explizite Authentifizierung und entweder Smartcard- oder Passthrough mit Smartcard aktivieren, werden Benutzer erst aufgefordert, sich mit einer Smartcard anzumelden, können aber auf die explizite Authentifizierung zurückgreifen, wenn es mit den Smartcards Probleme gibt.

Die optionalen Argumente konfigurieren Einstellungen, die auch nach dem Erstellen der Desktopgerätesite geändert werden können, indem Sie die Sitekonfigurationsdatei bearbeiten.

Beispiel:

Erstellen Sie eine Desktop Appliance Connector-Site im virtuellen Pfad /Citrix/DesktopAppliance1 auf der IIS-Standardwebsite.

```
Install-DSDesktopAppliance `

-FriendlyName DesktopAppliance1 `

-SiteId 1 `

-VirtualPath /Citrix/DesktopAppliance1 `

-UseHttps $false `

-StoreUrl https://serverName/Citrix/Store `

-EnableMultiDesktop $true `

-EnableExplicit $true `

-EnableSmartCard $true `

-EnableEmbeddedSmartCardSSO $false
```

3. Um eine vorhandene Desktopgerätesite zu entfernen, geben Sie den folgenden Befehl ein.
   `Remove-DSDesktopAppliance -SiteId iisid -VirtualPath sitepath`
   Dabei ist iisid die numerische ID der IIS-Site, die StoreFront hostet, und sitepath ist der relative Pfad der Desktopgerätesite in IIS, z. B. /Citrix/DesktopAppliance.

4. Um die Desktopgerätesites aufzulisten, die derzeit in der StoreFront-Bereitstellung verfügbar sind, geben Sie den folgenden Befehl ein.
   `Get-DSDesktopAppliancesSummary`

Konfigurieren der Benutzerauthentifizierung

Desktopgerätesites unterstützen explizite, Smartcard- oder Passthrough-Authentifizierung mit Smartcards. Die explizite Authentifizierung ist standardmäßig aktiviert. Wenn Sie die explizite Authentifizierung und entweder Smartcard oder Passthrough mit Smartcard aktivieren, werden Benutzer standardmäßig zunächst aufgefordert, sich mit einer Smartcard anzumelden. Wenn Benutzer Probleme mit ihren Smartcards haben, können sie die Anmeldeinformationen explizit eingeben. Wenn Sie IIS so konfigurieren, dass Clientzertifikate für HTTPS-Verbindungen zu allen StoreFront-URLs erforderlich sind,

können Benutzer nicht auf die explizite Authentifizierung zurückgreifen, wenn ihre Smartcards nicht verfügbar sind. Um die Authentifizierungsmethoden für eine Desktopgerätesite zu konfigurieren, bearbeiten Sie die Sitekonfigurationsdatei.

1. Öffnen Sie die Datei web.config für die Desktopgerätesite mit einem Texteditor. Die Datei ist normalerweise im Verzeichnis C:\inetpub\wwwroot\Citrix\storename\DesktopAppliance, wobei storename für denNamen steht, der beim Erstellen des Stores angegeben wurde.
2. Suchen Sie das folgende Element in der Datei.
3. Ändern Sie den Wert des Attributs enabled zu false , um die explizite Authentifizierung für die Site zu deaktivieren.
4. Suchen Sie das folgende Element in der Datei.

5. Setzen Sie den Wert des Attributs enabled auf true , um die Smartcardauthentifizierung zu aktivieren. Um die Passthrough-Authentifizierung mit Smartcard zu aktivieren, müssen Sie auch den Wert des Attributs useEmbeddedSmartcardSso auf true setzen. Verwenden Sie das Attribut embeddedSmartcardSsoPinTimeout, um festzulegen, wie lange (in Stunden, Minuten und Sekunden) der PIN-Eingabebildschirm angezeigt wird. Kommt es zu einem Timeout des PIN-Eingabebildschirms, wird Benutzern die Anmeldeseite angezeigt und sie müssen ihre Smartcard entfernen und neu einlegen, um wieder zum PIN-Eingabebildschirm zurückzukehren. Standardeinstellung für den Timeoutwert ist 20 Sekunden.

Ermöglichen der Auswahl zwischen mehreren Desktops für Benutzer

Standardmäßig wird beim Anmelden an einer Desktopgerätesite der erste (in alphabetischer Reihenfolge) Desktop automatisch gestartet, der für den Benutzer in dem Store zur Verfügung steht, für den die Site konfiguriert ist. Wenn Sie Benutzern Zugriff auf mehrere Desktops in einem Store bereitstellen, können Sie die Desktopgerätesite so konfigurieren, dass die verfügbaren Desktops angezeigt werden, damit Benutzer einen auswählen können. Bearbeiten Sie die Sitekonfigurationsdatei, um diese Einstellungen zu ändern.

1. Öffnen Sie die Datei web.config für die Desktopgerätesite mit einem Text-Editor. Die Datei ist normalerweise im Verzeichnis C:\inetpub\wwwroot\Citrix\storenameDesktopAppliance, wobei f storenameür den Namen steht, der beim Erstellen des Stores angegeben wurde.
2. Suchen Sie das folgende Element in der Datei.
3. Ändern Sie den Wert des Attributs showMultiDesktop zu true , damit Benutzer beim Anmelden an der Desktopgerätesite alle Desktops sehen und unter den verfügbaren Desktops im Store einen wählen können.

Erstellen eines einzelnen vollqualifizierten Domänennamens (FQDN) für den internen und externen Zugriff auf einen Store

Nov 27, 2017

Hinweis: Die folgenden Versionen sind erforderlich, damit Sie dieses Feature mit einem nativen Receiver für Desktop verwenden können.

- Windows Receiver 4.2
- MAC Receiver 11.9

Sie können Zugriff auf Ressourcen aus dem Unternehmensnetzwerk und aus dem Internet durch ein NetScaler Gateway ermöglichen und die Benutzererfahrung durch Erstellen eines einzelnen FQDN für interne und externen Roamingclients vereinfachen.

Ein einzelner FQDN ist nützlich für Benutzer, die eine systemeigene Receiver-Version verwenden. Sie müssen sich nur eine URL merken, unabhängig davon, ob sie mit einem internen oder öffentlichen Netzwerk verbunden sind.

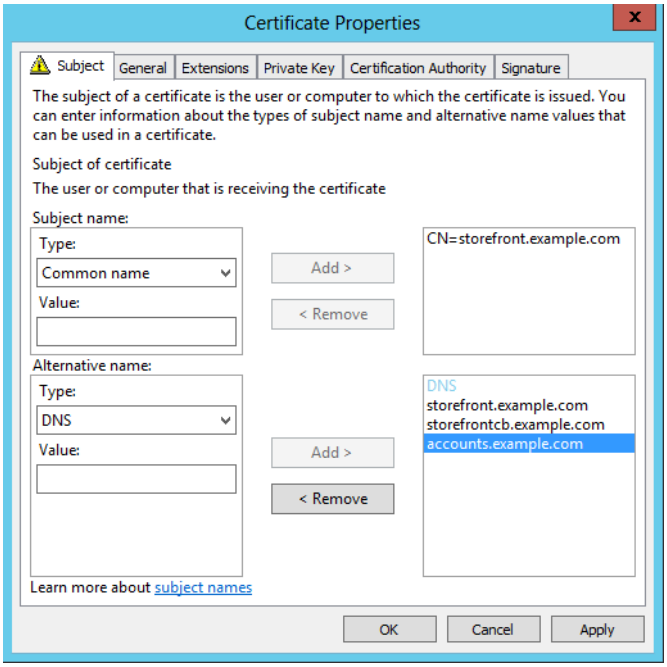
StoreFront-Beacons für systemeigene Receiver-Versionen

Citrix Receiver versucht eine Kontaktaufnahme mit den Beacons und ermittelt anhand der Antworten, ob Benutzer mit lokalen oder öffentlichen Netzwerken verbunden sind. Wenn ein Benutzer auf einen Desktop oder eine Anwendung zugreift, werden die Standortinformationen an den Server mit der Ressource weitergegeben, sodass die entsprechenden Verbindungsinformationen an Citrix Receiver zurückgegeben werden können. Dadurch wird sichergestellt, dass Benutzer nicht aufgefordert werden, sich neu anmelden, wenn sie auf einen Desktop oder eine Anwendung zugreifen. Weitere Informationen zur Konfiguration von Beacons finden Sie unter Konfigurieren von Beacons.

Konfigurieren des virtuellen NetScaler Gateway-Servers und SSL-Zertifikats

Der gemeinsame FQDN wird entweder in die IP des Routers für die externe Firewall aufgelöst oder in die IP eines virtuellen NetScaler Gateway-Servers in der DMZ, wenn Clients versuchen, auf Ressourcen von außerhalb des Unternehmensnetzwerks zuzugreifen. Stellen Sie sicher, dass die Felder Common Name und Subject Alternative Name des SSL-Zertifikats den freigegebenen FQDN für den externen Zugriff auf den Store enthalten. Bei Verwendung einer Drittanbieter-Stammzertifizierungsstelle (z. B. VeriSign) anstelle der unternehmenseigenen Zertifizierungsstelle zum Signieren des Gateway-Zertifikats vertrauen alle externen Clients automatisch dem an den virtuellen Gateway-Server gebundenen Zertifikat. Bei Verwendung einer Drittanbieter-Stammzertifizierungsstelle wie VeriSign müssen keine zusätzlichen Stammzertifizierungsstellen-Zertifikate auf externen Clients importiert werden.

Überlegen Sie beim Bereitstellen eines einzelnen Zertifikats mit dem Common Name des gemeinsamen FQDN für NetScaler Gateway und den StoreFront-Server, ob Sie Remotediscovery unterstützen möchten. Falls ja, muss das Zertifikat der Spezifikation für alternative Antragstellernamen entsprechen.



Beispiel für ein Zertifikat für den virtuellen NetScaler Gateway-Server: storefront.example.com

1. Stellen Sie sicher, dass der gemeinsame FQDN, die Callback-URL und die Kontenalias-URL im DNS-Feld des Zertifikats als alternativer Antragstellername (Subject Alternative Name, SAN) enthalten ist.
2. Stellen Sie sicher, dass der private Schlüssel exportierbar ist, sodass Zertifikat und Schlüssel in NetScaler Gateway importiert werden können.
3. Stellen Sie sicher, dass "Default Authorization" auf "Allow" festgelegt ist.
4. Signieren Sie das Zertifikat durch eine Drittanbieter-Zertifizierungsstelle wie etwa VeriSign oder eine Stammzertifizierungsstelle Ihres Unternehmens.

Beispiel-SANs für Servergruppen mit zwei Knoten:

storefront.example.com (erforderlich)

storefrontcb.example.com (erforderlich)

accounts.example.com (erforderlich)

storefrontserver1.example.com (optional)

storefrontserver2.example.com (optional)

Signieren Sie das SSL-Zertifikat des virtuellen NetScaler Gateway-Servers durch eine Zertifizierungsstelle.

Je nach Ihren Anforderungen haben Sie zwei Optionen zur Auswahl der Art des signierten Zertifikats.

- 1. Voneiner Drittanbieter-Zertifizierungsstelle signiertes Zertifikat: Wenn das an den virtuellen NetScaler Gateway-Server gebundene Zertifikat von einem vertrauenswürdigen Drittanbieter signiert wurde, muss auf externen Clients wahrscheinlich KEIN Stammzertifizierungsstellenzertifikat in den Speicher vertrauenswürdiger Stammzertifizierungsstellen kopiert werden. Auf Windows-Clients sind die Zertifikate der gängigen Stammzertifizierungsstellen vorinstalliert. Beispiele kommerzieller Drittanbieter-Zertifizierungsstellen, die verwendet werden können, sind DigiCert, Thawte und VeriSign. Auf mobile Geräte wie iPads, iPhones und Android-Tablets/-Telefone müssen Stammzertifizierungsstellenzertifikate jedoch möglicherweise kopiert werden, damit diese Geräte dem virtuellen

NetScaler Gateway-Server vertrauen.

- 2. Von einer Unternehmens-Stammzertifizierungsstelle signiertes Zertifikat: Wenn Sie diese Option wählen, muss das Zertifikat auf allen externen Clients in den Speicher vertrauenswürdiger Stammzertifizierungsstellen kopiert werden. Bei Verwendung mobiler Geräte mit systemeigener Receiver-Version (z. B. iPhones und iPads) erstellen Sie ein Sicherheitsprofil auf diesen Geräten.

Importieren des Stammzertifikats auf mobilen Geräten

- Auf iOS-Geräten können CER x.509-Zertifikatdateien als E-Mail-Anlagen importiert werden, da der Zugriff auf den lokalen Speicher solcher Geräte normalerweise nicht möglich ist.
- Android-Geräte erfordern das gleiche CER x.509-Format. Das Zertifikat kann aus dem lokalen Speicher des Geräts oder als E-Mail-Anlage importiert werden.

Externes DNS: storefront.example.com

Stellen Sie sicher, dass die DNS-Auflösung Ihres Internetdienstanbieters in die externe IP des Firewallrouters am äußeren Rand der DMZ bzw. in die virtuelle IP-Adresse des virtuellen NetScaler Gateway-Servers auflöst.

Split-View DNS

- Wenn Split-View DNS richtig konfiguriert ist, sendet die Quelladresse der DNS-Anfrage den Client zum richtigen DNS Alias-Datensatz.
- Wenn Clients zwischen öffentlichen Netzwerken und Unternehmensnetzwerken wechseln, sollte sich ihre IP ändern. Abhängig von dem Netzwerk, mit dem sie verbunden sind, sollten sie bei der Anfrage bei storefront.example.com den richtigen Alias-Datensatz erhalten.

Importieren von Zertifikaten von einer Windows-Zertifizierungsstelle in NetScaler Gateway

WinSCP ist ein nützliches und kostenloses Drittanbietertool zum Verschieben von Dateien von einer Windows-Maschine in ein NetScaler Gateway-Dateisystem. Kopieren Sie Zertifikate für den Import in den Ordner /nsconfig/ssl/ im NetScaler Gateway-Dateisystem. Siekönnen mit den OpenSSL-Tools in NetScaler Gateway das Zertifikat und den Schlüssel aus einer PKCS12/PFX-Datei extrahieren, um eine CER- und eine KEY X.509-Datei separat im PEM-Format zu erstellen, die von NetScaler Gateway verwendet werden können.

1. Kopieren Sie die PFX-Datei in den Ordner /nsconfig/ssl auf dem NetScaler Gateway-Gerät in VPX.
2. Öffnen Sie die NetScaler Gateway-Befehlszeilenschnittstelle.
3. Zum Wechseln in die FreeBSD-Shell geben Sie Shell ein, um die NetScaler Gateway-Befehlszeilenschnittstelle zu verlassen.
4. Geben Sie zum Wechseln des Verzeichnisses cd /nsconfig/ssl ein.
5. Führen Sie openssl pkcs12 -in <imported cert file>.pfx -nokeys -out <certfilename>.cer aus und geben Sie bei entsprechender Aufforderung das PFX-Kennwort ein.
6. Führen Sie openssl pkcs12 -in <imported cert file>.pfx -nocerts -out <keyfilename>key aus.
7. Geben Sie bei Aufforderung das PFX-Kennwort ein und legen Sie eine PEM- Passphrase für den privaten Schlüssel zum Schutz der KEY-Datei fest.
8. Umsicherzustellen, dass die CER- und die KEY-Datei erfolgreich erstellt wurden, führen Sie in /nsconfig/ssl/ den Befehl ls –al aus.
9. Geben Sie Exit ein, um zur NetScaler Gateway-Befehlszeilenschnittstelle zurückzukehren.

Native Gateway-Sitzungsrichtlinie für Receiver für Windows/Mac

REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver && REQ.HTTP.HEADER X-Citrix-Gateway EXISTS

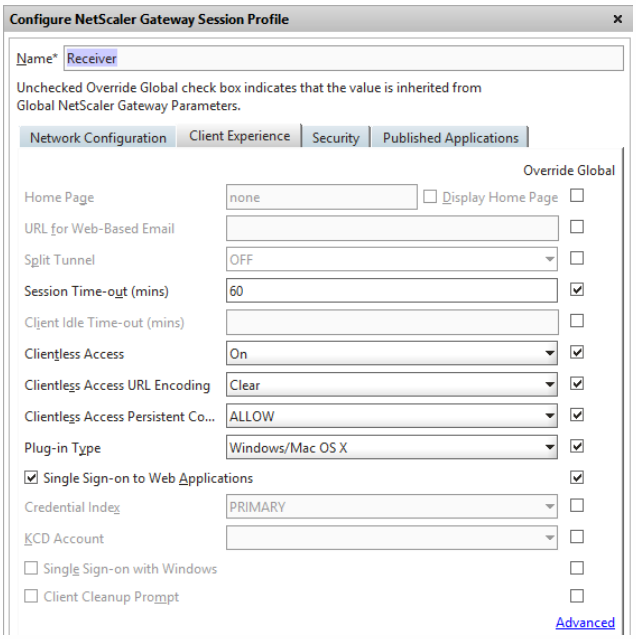
Sitzungsrichtlinie für Receiver für Web

REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver && REQ.HTTP.HEADER Referer EXISTS

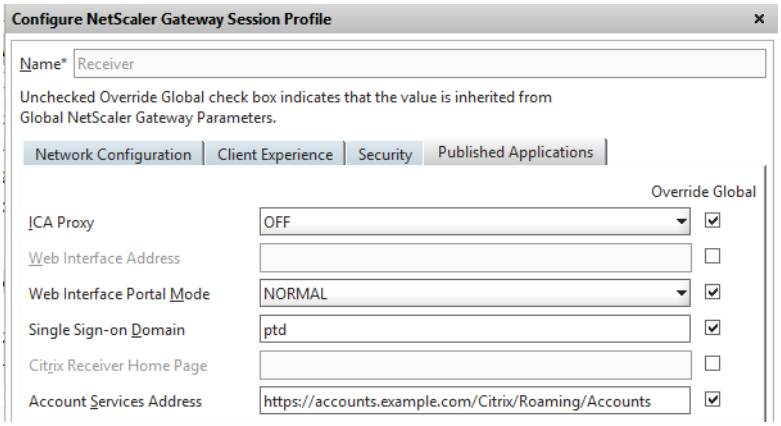
CVPN- und SmartAccess-Einstellungen

Wenn Sie SmartAccess verwenden, aktivieren Sie den SmartAccess-Modus auf der Eigenschaftenseite des virtuellen NetScaler Gateway-Servers. Für jeden gleichzeitigen Benutzer, der auf Remoteressourcen zugreift, ist eine universelle Lizenz erforderlich.

Receiver-Profil

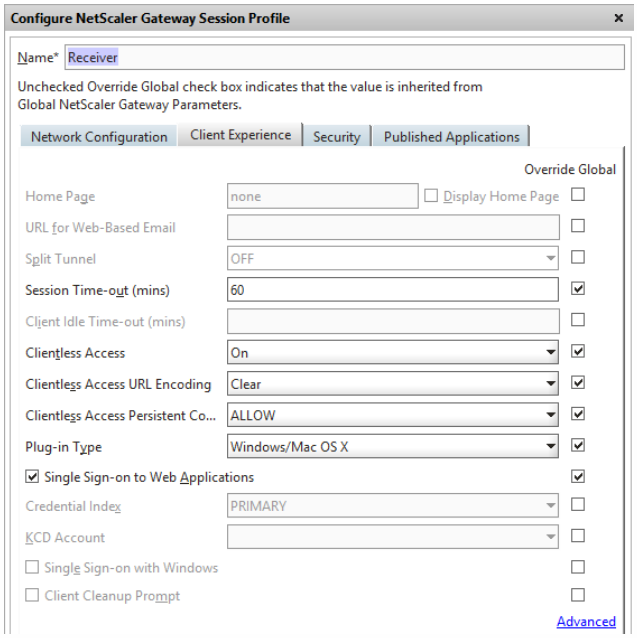


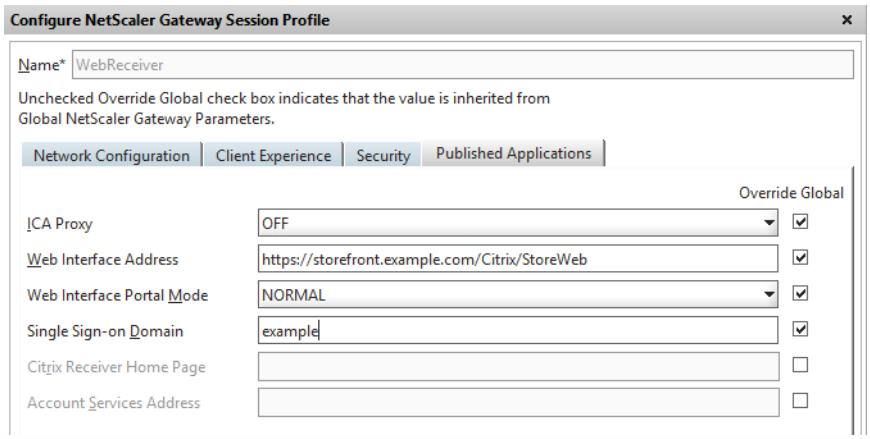
Konfigurieren Sie als Kontodienst-URL für das Sitzungsprofil https://accounts.example.com/Citrix/Roaming/Accounts und NICHT https://storefront.example.com/Citrix/Roaming/Accounts.



Fügen Sie diese URL zudem für <allowedAudiences> in den web.config-Dateien für Authentifizierung und Roaming auf dem StoreFront-Server hinzu. Weitere Informationen finden Sie unten im Abschnitt "Konfigurieren der Host-Basis-URL des StoreFront-Servers, des Gateways und des SSL-Zertifikats".

Receiver für Web-Profil

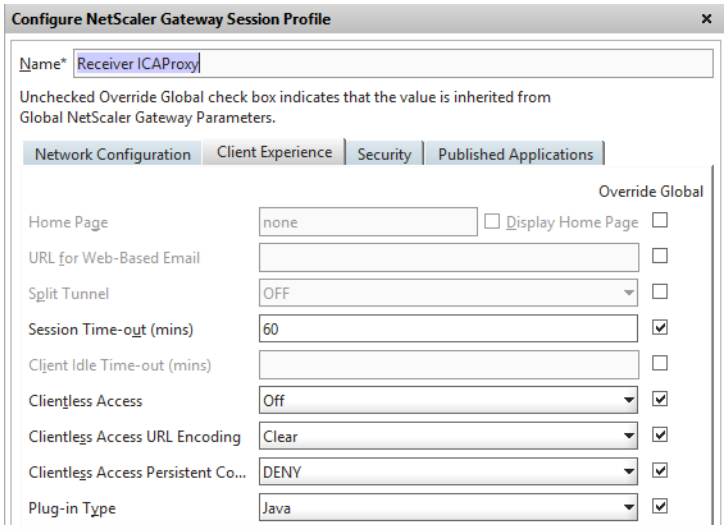


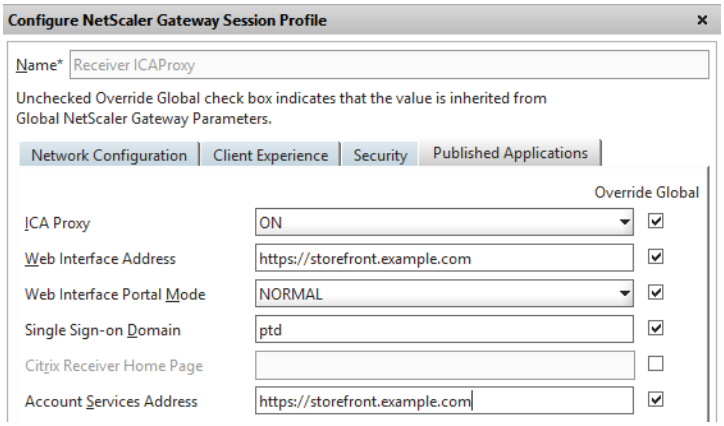


ICA-Proxy-Einstellung und Moduseinstellung "Basic"

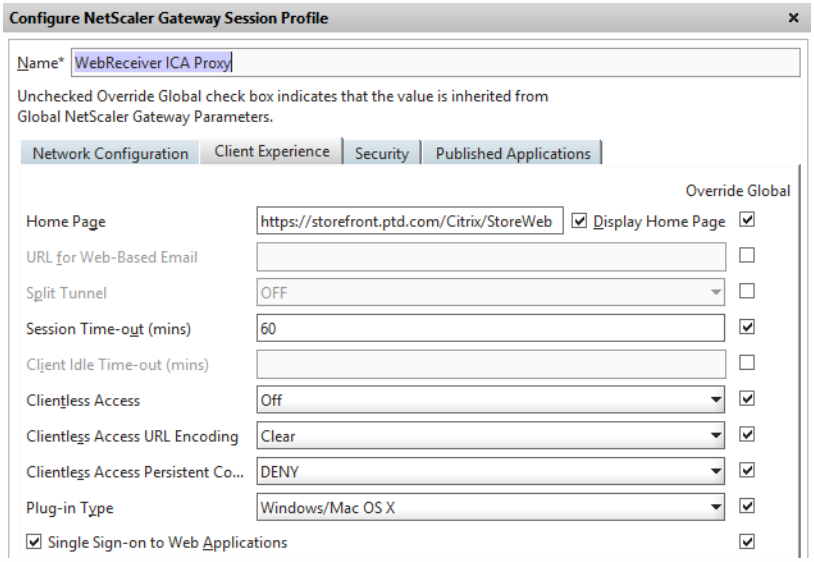
Wenn Sie den ICA-Proxy verwenden, aktivieren Sie den Modus "Basic" auf der Eigenschaftenseite des virtuellen NetScaler Gateway-Servers. Es ist nur eine NetScaler-Plattformlizenz erforderlich.

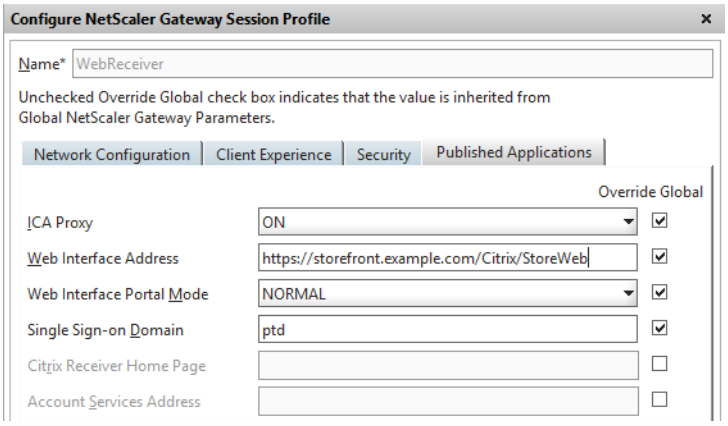
Receiver-Profil





Receiver für Web-Profil





Konfigurieren der Host-Basis-URL des StoreFront-Servers, des Gateways und des SSL-Zertifikats

Wenn ein StoreFront-Cluster oder eine einzelne StoreFront-IP zum Hosten des Stores erstellt wurde, muss der gemeinsame FQDN, der in den virtuellen NetScaler Gateway-Server aufgelöst wird, auch direkt in den StoreFront-Load Balancer aufgelöst werden.

Internes DNS: Erstellen Sie drei DNS Alias-Datensätze.

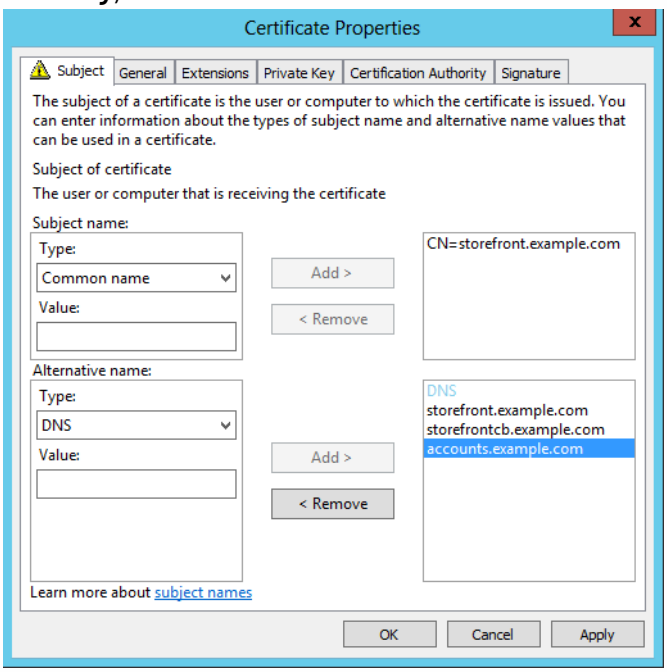
- storefront.example.com muss in den StoreFront-Load Balancer bzw. die IP des einzelnen StoreFront-Servers aufgelöst

werden.

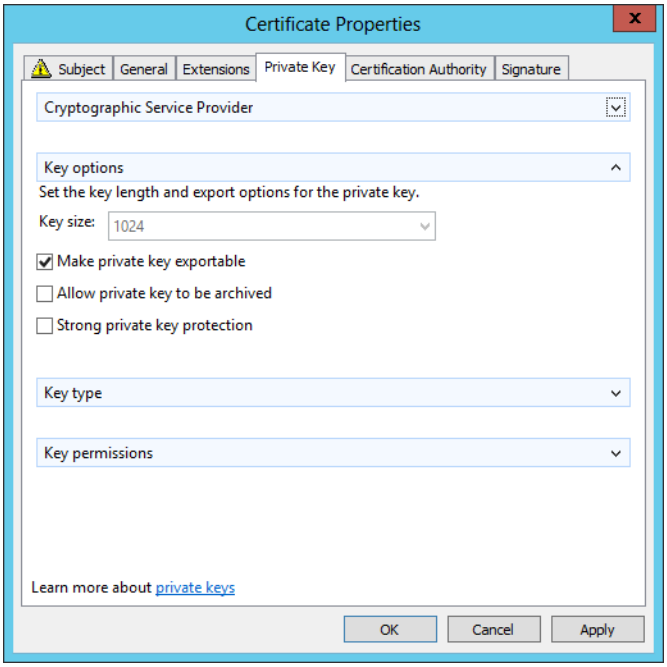
- storefrontcb.example.com muss in die virtuelle IP-Adresse des virtuellen Gatewayservers aufgelöst werden. Treffen Sie daher entsprechende Vorkehrungen, wenn zwischen DMZ und lokalem Unternehmensnetzwerk eine Firewall sitzt.
- accounts.example.com – erstellen Sie ein DNS-Alias für storefront.example.com. Dieses wird außerdem in die IP des Load Balancers für das StoreFront-Cluster bzw. die IP eines einzelnen StoreFront-Servers aufgelöst.

Beispielzertifikat für den StoreFront-Server: storefront.example.com

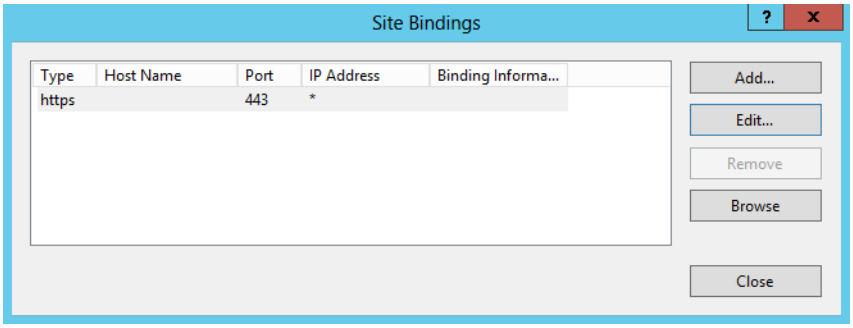
1. Erstellen Sie ein geeignetes Zertifikat für den StoreFront-Server bzw. die StoreFront-Servergruppe, bevor Sie StoreFront installieren.
2. Tragen Sie den gemeinsamen FQDN in die Felder "Common Name" und "DNS" ein. Dieser muss mit dem FQDN in dem zuvor erstellten, an den virtuellen NetScaler Gateway-Server gebundenen SSL-Zertifikat übereinstimmen oder verwenden Sie das gleiche an den virtuellen NetScaler Gateway-Server gebundene Zertifikat.
3. Fügen Sie dem Zertifikat das Kontenalias (accounts.example.com) als weiteren SAN hinzu. Das Kontenalias im SAN ist das zuvor im NetScaler Gateway-Sitzungsprofil (siehe **Sitzungsrichtlinie und -profil für systemeigenes Receiver-Gateway**) verwendete Alias.



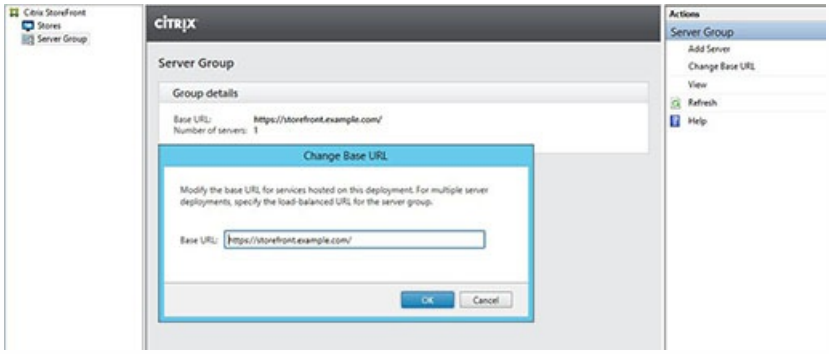
4. Stellen Sie sicher, dass der private Schlüssel exportierbar ist, damit das Zertifikat auf einen anderen Server oder auf StoreFront-Servergruppenknoten übertragen werden kann.



5. Signieren Sie das Zertifikat durch eine Drittanbieter-Zertifizierungsstelle (z. B. VeriSign), eine Stammzertifizierungsstelle Ihres Unternehmens oder eine Zwischenzertifizierungsstelle.
6. Exportieren Sie das Zertifikat im PFX-Format einschließlich des privaten Schlüssels.
7. Importieren Sie das Zertifikat und den privaten Schlüssel auf den StoreFront-Server. Wenn Sie ein Windows-NLB-StoreFront-Cluster bereitstellen, importieren Sie das Zertifikat auf jeden Knoten. Wenn Sie einen anderen Load Balancer verwenden, z. B. einen virtuellen NetScaler-LB-Server, importieren Sie das Zertifikat auf diesen.
8. Erstellen Sie auf dem StoreFront-Server eine HTTPS-Bindung in IIS und binden Sie das importierte SSL-Zertifikat an diese.



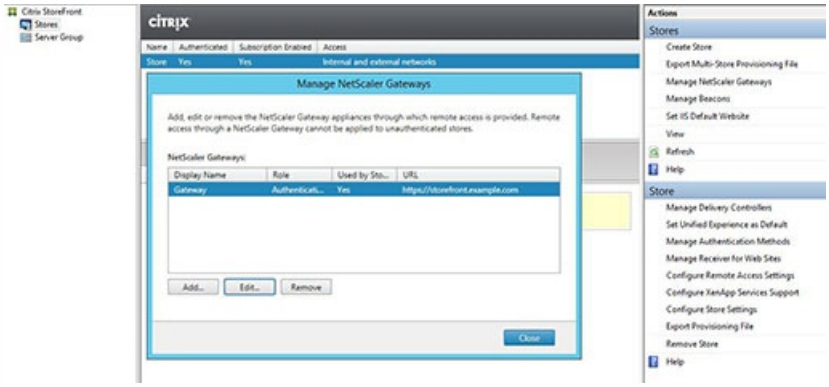
9. Konfigurieren Sie die Host-Basis-URL auf dem StoreFront-Server entsprechend dem bereits gewählten gemeinsamen FQDN.
   Hinweis: StoreFront wählt immer automatisch den letzten alternativen Antragstellernamen in der SAN-Liste in dem Zertifikat. Dies ist lediglich eine empfohlene Host-Basis-URL zur Unterstützung von StoreFront-Administratoren und i. d. R. korrekt. Sie können sie manuell auf einen beliebigen HTTPS://<FQDN> festlegen, vorausgesetzt, dieser ist im Zertifikat als SAN eingetragen. Beispiel: https://storefront.example.com



Konfigurieren des Gateways auf dem StoreFront-Server: storefront.example.com

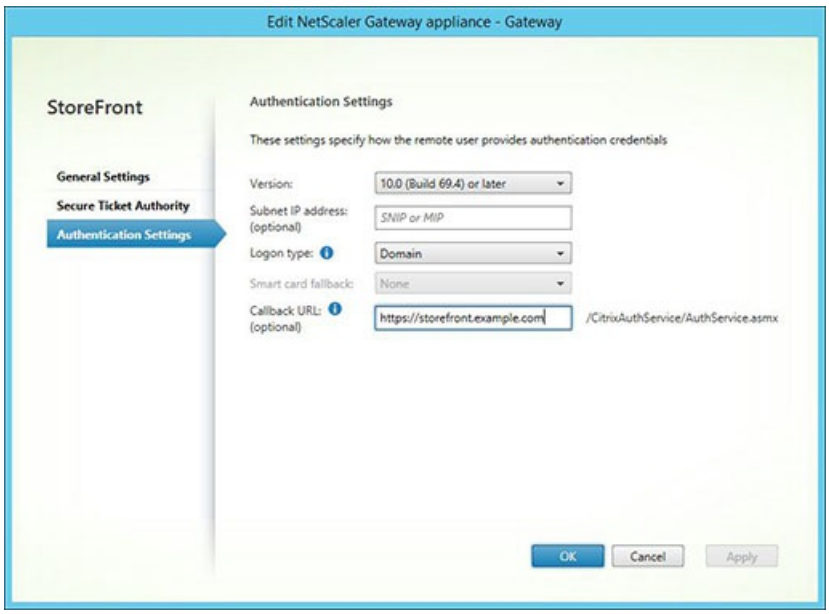
1. Klicken Sie im Knoten **Stores** im Bereich **Aktionen** auf **NetScaler Gateways verwalten**.

2. Wählen Sie das Gateway aus der Liste aus und klicken Sie auf **Weiter**.



3. Geben Sie auf der Seite **Allgemeine Einstellungen** den gemeinsamen FQDN in das Feld **NetScaler Gateway-URL** ein.

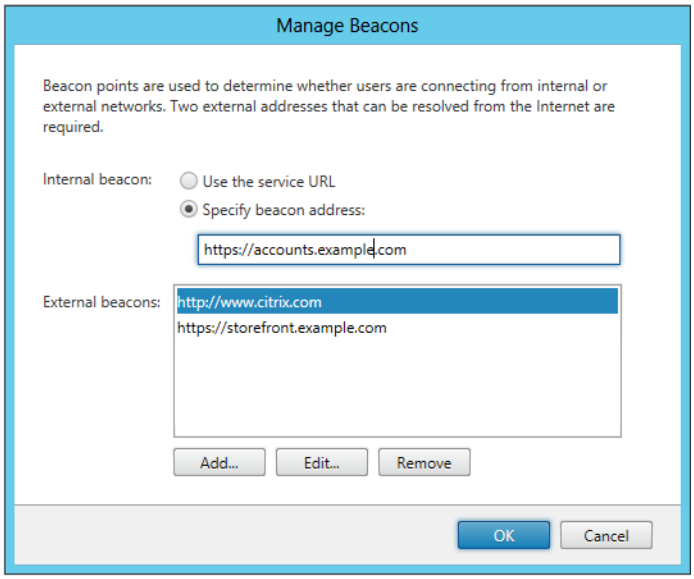
4. Wählen Sie die Registerkarte **Authentifizierungseinstellungen** und geben Sie den Callback-FQDN in das Feld **Callback-URL** ein.



5. Wählen Sie die Registerkarte **Secure Ticket Authority** und stellen Sie sicher, dass die Liste der Secure Ticket Authority-Server (STA-Server) der Liste der bereits im Knoten **Store** konfigurierten Delivery Controller entspricht.

6. Aktivieren Sie den Remotezugriff für den Store.

7. Legen Sie den internen Beacon manuell auf das Kontenalias (accounts.example.com) fest. Er darf nicht von außerhalb des Gateways auflösbar sein. Dieser FQDN muss sich von dem externen Beacon unterscheiden, der von der StoreFront-Host-Basis-URL und dem virtuellen NetScaler Gateway-Server (storefront.example.com) gemeinsam verwendet wird. Verwenden Sie NICHT den gemeinsam verwendeten FQDN, da hierdurch der interne und der externe Beacon identisch werden.



8. Wenn Sie die Discovery mit FQDNs unterstützen möchten, führen Sie die nachfolgenden Schritte aus. Wenndie Provisioningdateikonfiguration genügt oder Sie nur Receiver für Web verwenden, überspringen Sie die folgenden Schritte.

Fügen Sie in C:\inetpub\wwwroot\Citrix\Authentication\web.config einen zusätzlichen -Eintrag ein. Die web.config-Datei für die Authentifizierung hat zwei -Einträge. Nur der erste Authentication Token Producer-Eintrag in der Datei erfordert einen zusätzlichen -Eintrag.

9. Suchen Sie nach der Zeichenfolge "". Suchen Sie den unten gezeigten Eintrag, fügen Sie die **fett** dargestellte Zeile hinzu und speichern und schließen Sie die Datei web.config.

.....

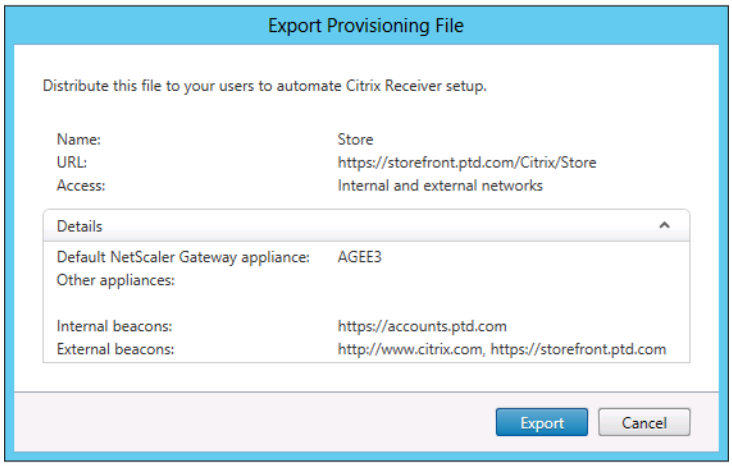
.....

9. **C:\inetpub\wwwroot\Citrix\Roaming\web.config**:Suchen Sie den unten gezeigten Eintrag, fügen Sie die **fett** dargestellte Zeile hinzu und speichern und schließen Sie die Datei web.config.

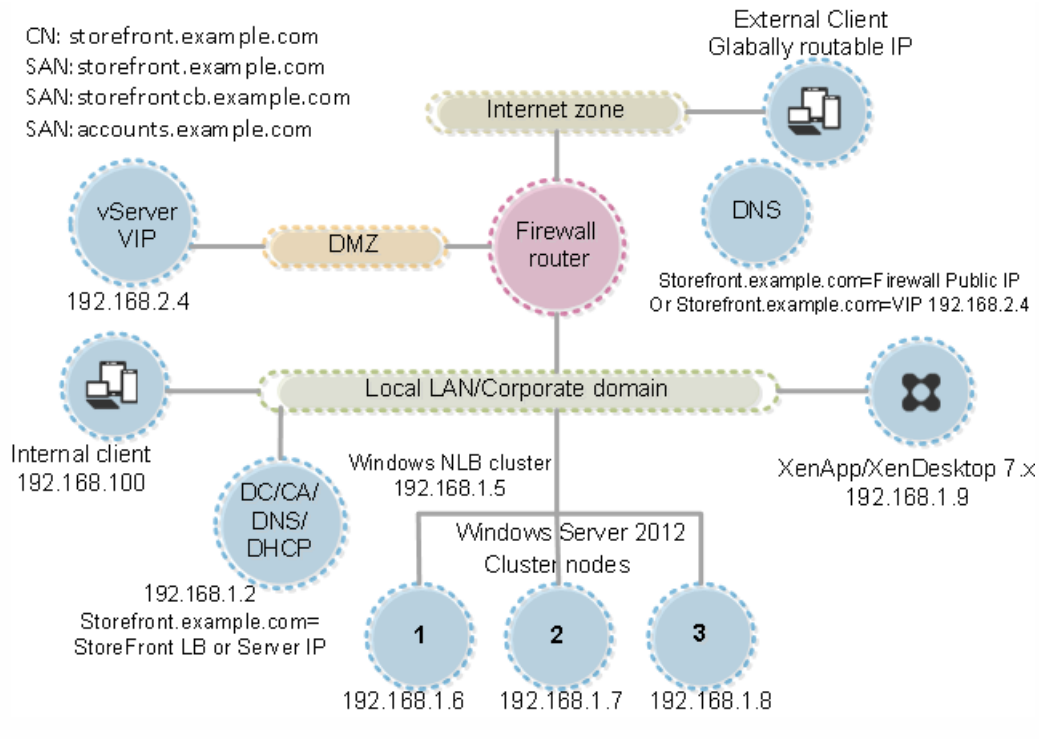
.....

.....

Alternativ können Sie die Receiver-eigene CR-Provisioningdatei für den Store exportieren. Dadurch wird die Erstverwendungs-Konfiguration in systemeigenen Receiver-Versionen überflüssig. Verteilen Sie diese Datei an alle Windows- und MAC-Receiver-Clients.



Wenn Receiver auf einem Client installiert wird, wird der CR-Dateityp erkannt und die Provisioningdatei durch einen Doppelklick automatisch importiert.



Konfigurieren der Ressourcenfilterung

Nov 27, 2017

In diesem Abschnitt wird erläutert, wie Enumerationsressourcen nach Ressourcentyp und Schlüsselwörtern gefiltert werden können. Sie können diese Art des Filternsmit fortgeschritteneren Anpassungen verwenden, die das Store Customization SDK bietet. Mit diesem SDK können Sie steuern, welche Apps und Desktops Benutzern angezeigt werden. Zudem können Sie Zugriffsbedingungen ändern und Startparameter anpassen. Weitere Informationen finden Sie in der Dokumentation zum Store Customization SDK.

Hinweis: Die StoreFront- und PowerShell-Konsolen können nicht gleichzeitig geöffnet sein. Schließen Sie immer zuerst die StoreFront-Verwaltungskonsole, bevor Sie die PowerShell-Konsole zum Verwalten der StoreFront-Konfiguration öffnen. Schließen Sie gleichermaßen immer alle Instanzen von PowerShell, bevor Sie die StoreFront-Konsole öffnen.

Konfigurieren von Filtern

Konfigurieren Sie Filter mit den PowerShell-Cmdlets, die im StoresModule definiert sind. Laden Sie die erforderlichen Module mit dem folgenden PowerShell-Befehl:

```
$dsInstallProp = Get-ItemProperty `
 -Path HKLM:\SOFTWARE\Citrix\DeliveryServicesManagement -Name InstallDir
$dsInstallDir = $dsInstallProp.InstallDir
& $dsInstallDir\..\Scripts\ImportModules.ps1
```

Filtern nach Typ

Mit diesem Filter filtern Sie die Ressourcenenumeration nach Ressourcentyp. Dieser einschließende Filter entfernt alle Ressourcen aus dem Ergebnis der Ressourcenenumeration, die nicht den angegebenen Typen entsprechen. Verwenden Sie die folgenden Cmdlets:

Set-DSResourceFilterType: Hiermit wird die Enumerationsfilterung basierend auf Ressourcentypen festgelegt.

Get-DSResourceFilterType: Hiermit wird die Liste der Ressourcentypen abgerufen, die StoreFront in der Enumeration zurückgeben kann.

Hinweis: Ressourcentypen werden vor Schlüsselwörtern angewendet.

Filtern nach Schlüsselwörtern

Dieser Filter dient zum Filtern von Ressourcen basierend auf Schlüsselwörtern, z. B. für Ressourcen, die von XenDesktop oder XenApp abgeleitet werden. Schlüsselwörter werden aus Markup im Beschreibungsfeld der entsprechenden Ressource generiert.

Der Filter funktioniert entweder einschließend oder ausschließend, aber nicht auf beide Arten. Der einschließende Filter lässt die Enumeration von Ressourcen zu, die den Schlüsselwörtern entsprechen, und entfernt nicht zutreffende Ressourcen aus der Enumeration. Der ausschließende Filter schließt Ressourcen, die den Schlüsselwörtern entsprechen, aus der Enumeration aus. Verwenden Sie die folgenden Cmdlets:

Set-DSResourceFilterKeyword: Hiermit wird die Enumerationsfilterung basierend auf Ressourcenschlüsseln festgelegt.

Get-DSResourceFilterKeyword: Hiermit wird eine Liste mit Filterschlüsselwörtern abgerufen.

Die folgenden Schlüsselwörter sind reserviert und dürfen nicht zum Filtern verwendet werden:

- Automatisch
- Erforderlich

Weitere Informationen zu Schlüsselwörtern finden Sie unter Optimieren der Benutzererfahrung und Konfigurieren der Anwendungsbereitstellung.

Beispiele

Mit diesem Befehl werden Workflowressourcen durch den Filter von der Enumeration ausgeschlossen:

```
Set-DSResourceFilterKeyword -SiteId 1 -VirtualPath "/Citrix/Store" -ExcludeKeywords @("WFS")
```

Mit diesem Beispiel werden als zulässigen Ressourcentypen ausschließlich Anwendungen festgelegt:

```
Set-DSResourceFilterType -SiteId 1 -VirtualPath "/Citrix/Store" -IncludeTypes @("Applications")
```

Konfigurieren mit Konfigurationsdateien

Nov 27, 2017

Sie können mit Konfigurationsdateien weitere Einstellungen für Citrix StoreFront und Citrix Receiver für Web konfigurieren, die nicht mit der Citrix StoreFront-Verwaltungskonsole festgelegt werden können.

Für Citrix StoreFront können Sie Folgendes konfigurieren:

- Aktivieren der ICA-Dateisignierung
- Deaktivieren der Dateitypzuordnung
- Anpassen des Citrix Receiver-Anmeldedialogfelds
- Deaktivieren der Zwischenspeicherung von Kennwörtern und Benutzernamen in Receiver für Windows

Für Citrix Receiver für Web können Sie Folgendes konfigurieren:

- Anzeige von Ressourcen für Benutzer
- Deaktivieren der Ordneransicht "Eigene Apps"

Konfigurieren von StoreFront mit Konfigurationsdateien

Nov 27, 2017

In diesem Artikel werden zusätzliche Konfigurationsaufgaben beschrieben, die nicht mit der Citrix StoreFront-Verwaltungskonsole ausgeführt werden können.

Aktivieren der ICA-Dateisignierung

StoreFront bietet die Option, ICA-Dateien digital zu signieren, damit die Versionen von Citrix Receiver, die dieses Feature unterstützen, prüfen können, ob eine Datei aus einer vertrauenswürdigen Quelle stammt. Wenn die Dateisignierung in StoreFront aktiviert ist, wird die beim Starten einer Anwendung durch einen Benutzer generierte ICA-Datei mit einem Zertifikat aus dem persönlichen Zertifikatspeicher des StoreFront-Servers signiert. ICA-Dateien können mit einem Hashalgorithmus signiert werden, der von dem auf dem StoreFront-Server ausgeführten Betriebssystem unterstützt wird. Die digitale Signatur wird von Clients, die dieses Feature nicht unterstützen oder nicht für die ICA-Dateisignierung konfiguriert sind, ignoriert. Wenn die Signierung fehlschlägt, wird die ICA-Datei ohne digitale Signatur generiert und an Citrix Receiver gesendet. Anhand der Konfiguration wird daraufhin bestimmt, ob die unsignierte Datei akzeptiert wird.

Damit die ICA-Dateisignierung im Zusammenhang mit StoreFront verwendet werden kann, müssen die Zertifikate den privaten Schlüssel enthalten und im zulässigen Gültigkeitszeitraum liegen. Wenn das Zertifikat eine Schlüsselnutzungserweiterung enthält, muss diese die Verwendung des Schlüssels für digitale Signaturen gestatten. Falls eine erweiterte Schlüsselnutzungserweiterung enthalten ist, muss dafür Codesignierung oder Serverauthentifizierung festgelegt worden sein.

Citrix empfiehlt bei ICA-Dateisignierung, ein Codesignierungs- oder SSL-Signierungszertifikat von einer öffentlichen Zertifizierungsstelle oder von der privaten Zertifizierungsstelle Ihrer Organisation zu verwenden. Wenn es Ihnen nicht möglich ist, ein geeignetes Zertifikat von einer Zertifizierungsstelle zu beziehen, können Sie entweder ein vorhandenes SSL-Zertifikat (z. B. ein Serverzertifikat) verwenden oder ein neues Zertifikat von der Stammzertifizierungsstelle erstellen und an die Benutzergeräte verteilen.

ICA-Dateisignierung ist in Stores standardmäßig deaktiviert. Zum Aktivieren der ICA-Dateisignierung bearbeiten Sie die Storekonfigurationsdatei und führen Windows PowerShell-Befehle aus. Weitere Informationen zum Aktivieren der ICA-Dateisignierung in Citrix Receiver finden Sie unter ICA-Dateisignierung: Schutz vor dem Starten von Anwendungen oder Desktops von nicht vertrauenswürdigen Servern.

Hinweis: Die StoreFront- und PowerShell-Konsolen können nicht gleichzeitig geöffnet sein. Schließen Sie immer zuerst die StoreFront-Verwaltungskonsole, bevor Sie die PowerShell-Konsole zum Verwalten der StoreFront-Konfiguration öffnen. Schließen Sie gleichermaßen immer alle Instanzen von PowerShell, bevor Sie die StoreFront-Konsole öffnen.
Wichtig: Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Wenn Sie die Änderungen vorgenommen haben, übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden.

1. Vergewissern Sie sich, dass das Zertifikat, mit dem Sie die ICA-Dateien signieren möchten, im Citrix Delivery Services-Zertifikatspeicher auf dem StoreFront-Server verfügbar ist und nicht im aktuellen Zertifikatspeicher des Benutzers.
2. Öffnen Sie die Datei web.config für den Store mit einem Text-Editor. Die Datei ist normalerweise im Verzeichnis C:\inetpub\wwwroot\Citrix\storename\, wobei "storename" für den Namen steht, der beim Erstellen des Stores angegeben wurde.
3. Suchen Sie den folgenden Abschnitt in der Datei.

   ...

4. Fügen Sie Details des Zertifikats, das für die Signierung verwendet werden soll, wie unten dargestellt hinzu.

   certificateid" thumb="certificatethumbprint" />

   ...

   certificateid ist ein Wert, anhand dessen Sie das Zertifikat in der Storekonfigurationsdatei identifizieren können, und certificatethumbprint ist die Übersicht (oder der Fingerabdruck) der vom Hashalgorithmus erzeugten Zertifikatdaten.

5. Suchen Sie das folgende Element in der Datei.

6. Ändern Sie den Wert des Attributs enabled in True, um die ICA-Dateisignierung für den Store zu aktivieren. Legen Sie als Wert des Attributs certificateId die ID fest, anhand derer Sie das Zertifikat identifizieren möchten, d. h. certificateid in Schritt 4.
7. Wenn Sie einen anderen Hashalgorithmus als SHA-1 verwenden möchten, legen Sie als Wert für das Attribut hashAgorithm nach Bedarf entweder sha256, sha384 oder sha512 fest.
8. Starten Sie von einem Konto mit lokalen Administratorrechten Windows PowerShell und geben Sie an der Eingabeaufforderung die folgenden Befehle ein, damit der Store auf den privaten Schlüssel zugreifen kann.
   Add-PSSnapin Citrix.DeliveryServices.Framework.Commands
   $certificate = Get-DSCertificate "certificatethumbprint"

   Add-DSCertificateKeyReadAccess -certificate $certificates[0] -accountName “IIS APPPOOL\Citrix Delivery Services Resources”
   Dabei ist certificatethumbprint das Digest der vom Hashalgorithmus generierten Zertifikatdaten.

Deaktivieren der Dateitypzuordnung

Standardmäßig ist die Dateitypzuordnung in Stores aktiviert, damit Inhalte nahtlos an die abonnierten Anwendungen der Benutzer umgeleitet werden, wenn sie lokale Dateien der entsprechenden Typen öffnen. Bearbeiten Sie die Storekonfigurationsdatei, um die Dateitypzuordnung zu deaktivieren.

Wichtig: Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Wenn Sie die Änderungen vorgenommen haben, übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden.

1. Öffnen Sie die Datei web.config für den Store mit einem Text-Editor. Die Datei ist normalerweise im Verzeichnis C:\inetpub\wwwroot\Citrix\storename\ wobei storename für den Namen steht, der beim Erstellen des Stores angegeben wurde.
2. Suchen Sie das folgende Element in der Datei.

3. Ändern Sie den Wert des Attributs enableFileTypeAssociation in off, um die Dateitypzuordnung für den Store zu deaktivieren.

Anpassen des Citrix Receiver-Anmeldedialogfelds

Wenn sich Citrix Receiver-Benutzer an einem Store anmelden, wird standardmäßig kein Titeltext im Anmeldedialogfeld angezeigt. Sie können den Standardtext "Melden Sie sich an" anzeigen oder eine eigene benutzerdefinierte Meldung. Bearbeiten Sie die Dateien für den Authentifizierungsdienst, um den Titeltext im Citrix Receiver-Anmeldedialogfeld anzuzeigen und anzupassen.

Wichtig: Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Wenn Sie die Änderungen vorgenommen haben, übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden.

1. Öffnen Sie die Datei UsernamePassword.tfrm für den Authentifizierungsdienst mit einem Text-Editor. Die Datei ist normalerweise im Verzeichnis C:\inetpub\wwwroot\Citrix\Authentication\App_Data\Templates\.
2. Suchen Sie die folgenden Zeilen in der Datei.
   @* @Heading("ExplicitAuth:AuthenticateHeadingText") *@
3. Kommentieren Sie die Anweisung aus, indem Sie die Zeichen @* zu Beginn und am Ende entfernen (siehe unten).
   @* @Heading("ExplicitAuth:AuthenticateHeadingText") *@
   Benutzern von Citrix Receiver wird der Titeltext "Melden Sie sich an" oder die entsprechende lokalisierte Version dieses Texts angezeigt, wenn sie sich an Stores anmelden, die diesen Authentifizierungsdienst verwenden.

4. Um den Titeltext zu ändern, öffnen Sie mit einem Text-Editor die Datei ExplicitAuth.resx für den Authentifizierungsdienst (normalerweise im Verzeichnis C:\inetpub\wwwroot\Citrix\Authentication\App_Data\resources\).
5. Suchen Sie die folgenden Elemente in der Datei. Bearbeiten Sie den vom -Element umschlossenen Text, um den Titeltext zu ändern, der Benutzern im Citrix Receiver-Anmeldedialogfeld angezeigt wird, wenn sie auf Stores zugreifen, die diesen Authentifizierungsdienst verwenden.

   My Company Name

   Um den Titeltext des Citrix Receiver-Anmeldedialogfelds für Benutzer mit einem anderen Gebietsschema zu ändern, bearbeiten Sie die lokalisierten Dateien ExplicitAuth.languagecode.resx, wobei languagecode die Gebietsschema-ID ist.

Deaktivieren der Zwischenspeicherung von Kennwörtern und Benutzernamen in Citrix Receiver für Windows

Standardmäßig speichert Citrix Receiver für Windows die Kennwörter von Benutzern, wenn sie sich bei StoreFront-Stores anmelden. Sie können verhindern, dass Citrix Receiver für Windows, jedoch nicht Citrix Receiver für Windows Enterprise, die Kennwörter von Benutzern zwischenspeichert, indem Sie die Dateien für den Authentifizierungsdienst ändern.

Wichtig: Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Wenn Sie die Änderungen vorgenommen haben, übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden.

1. Öffnen Sie die folgende Datei in einem Texteditor: inetpub\wwwroot\Citrix\Authentication\App_Data\Templates\UsernamePassword.tfrm file.
2. Suchen Sie die folgende Zeile in der Datei.
   @SaveCredential(id: @GetTextValue("saveCredentialsId"), labelKey: "ExplicitFormsCommon:SaveCredentialsLabel", initiallyChecked: ControlValue("SaveCredentials"))
3. Kommentieren Sie die Anweisung wie unten angegeben.
   @SaveCredential(id: @GetTextValue("saveCredentialsId"), labelKey: "ExplicitFormsCommon:SaveCredentialsLabel", initiallyChecked: ControlValue("SaveCredentials"))

Benutzer von Citrix Receiver für Windows müssen ihre Kennwörter jedes Mal eingeben, wenn sie sich bei einem Store mit diesem Authentifizierungsdienst anmelden. Diese Einstellung gilt nicht für Citrix Receiver für Windows Enterprise.

> **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.

Standardmäßig verwendete Citrix Receiver für Windows automatisch den zuletzt eingegebenen Benutzernamen. Um das automatische Eintragen des Benutzernamens in das entsprechende Feld zu unterdrücken, bearbeiten Sie die Registrierung auf dem Benutzergerät:

1. Erstellen Sie einen REG_SZ-Wert unter HKLM\SOFTWARE\Citrix\AuthManager\RememberUsername.
2. Geben Sie als Wert " false" an.

Konfigurieren von Citrix Receiver für Web-Sites mit Konfigurationsdateien

Nov 27, 2017

In diesem Artikel werden zusätzliche Konfigurationsaufgaben für Citrix Receiver für Web-Sites beschrieben, die nicht mit der Citrix StoreFront-Verwaltungskonsole ausgeführt werden können.

Konfigurieren der Anzeige von Ressourcen für Benutzer

Wennsowohl Desktops als auch Anwendungen über eine Citrix Receiver für Web-Site verfügbar sind, werden standardmäßig separate Ansichten für Desktops und Anwendungen angezeigt. Benutzern wird nach der Anmeldung an der Site zuerst die Desktopansicht angezeigt. Wenn nur ein einziger Desktop für einen Benutzer verfügbar ist (unabhängig davon, ob auch Anwendungen von einer Site zur Verfügung stehen) wird dieser Desktop automatisch gestartet, wenn sich der Benutzer anmeldet. Bearbeiten Sie die Sitekonfigurationsdatei, um diese Einstellungen zu ändern.

Wichtig: Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Wenn Sie die Änderungen vorgenommen haben, übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden.

1. Öffnen Sie die Datei web.config für die Citrix Receiver für Web-Site in einem Text-Editor. Die Datei ist normalerweise im Verzeichnis C:\inetpub\wwwroot\Citrix\storenameWeb, wobei storename der Name ist, der beim Erstellen des Stores angegeben wurde.
2. Suchen Sie das folgende Element in der Datei.

3. Ändern Sie den Wert der Attribute showDesktopsView und showAppsView in false, damit den Benutzern weder Desktops noch Anwendungen angezeigt werden, selbst wenn sie über die Site verfügbar sind. Wenn die Desktop- und die Anwendungsansicht aktiviert ist, legen Sie für das Attribut defaultView den Wert apps fest, damit die Anwendungsansicht zuerst angezeigt wird, wenn Benutzer sich an der Site anmelden.
4. Suchen Sie das folgende Element in der Datei.

5. Ändern Sie den Wert des Attributs autoLaunchDesktop in false, damit Citrix Receiver für Web-Sites nicht automatisch einen Desktop startet, wenn sich ein Benutzer bei der Site anmeldet und nur ein einziger Desktop für den Benutzer verfügbar ist.
   Wenn das Attribut autoLaunchDesktop auf true festgelegt ist und ein Benutzer, für den es nur einen Desktop gibt, sich anmeldet, wird keine Verbindung zu den Anwendungen des Benutzers wiederhergestellt, unabhängig von der Workspace Control-Konfiguration.

Hinweis: Damit Citrix Receiver für Web-Sites Desktops automatisch starten kann, müssen Benutzer, die über Internet Explorer auf eine Site zugreifen, die Site den Zonen "Lokales Intranet" oder "Vertrauenswürdige Sites" hinzufügen.

Deaktivieren der Ordneransicht "Eigene Apps"

Standardmäßig wird in Citrix Receiver für Web die Ordneransicht "Eigene Apps" für Stores ohne Authentifizierung (Zugriff für nicht authentifizierte Benutzer) und für vorgegebene Stores (alle veröffentlichten Anwendungen sind auf dem Homebildschirm verfügbar, ohne dass Benutzer sie abonnieren) angezeigt. Diese Ansicht zeigt Anwendungen in einer Ordnerhierarchie einschließlich einer Breadcrumbspur.

Wichtig: Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der

Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Wenn Sie die Änderungen vorgenommen haben, übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden.

1. Öffnen Sie die Datei web.config für die Citrix Receiver für Web-Site in einem Text-Editor. Die Datei ist normalerweise im Verzeichnis C:\inetpub\wwwroot\Citrix\storenameWeb, wobei storename der Name ist, der beim Erstellen des Stores angegeben wurde.
2. Suchen Sie das folgende Element in der Datei.

3. Ändern Sie den Wert des Attributs enableAppsFolderView in false, um die Ordneransicht "Eigene Apps" in Citrix Receiver für Web zu deaktivieren.

Sichern der StoreFront-Bereitstellung

Nov 27, 2017

In diesem Artikel werden Bereiche behandelt, die sich bei der Bereitstellung und Konfiguration von StoreFront auf die Systemsicherheit auswirken können.

Konfigurieren von Microsoft Internetinformationsdienste (IIS)

Sie können StoreFront mit einer eingeschränkten IIS-Konfiguration konfigurieren. Dies ist jedoch nicht die IIS-Standardkonfiguration.

Dateinamenerweiterungen

Sie können nicht aufgeführte Dateinamenerweiterungen ausschließen.

StoreFront benötigt die Dateinamenerweiterungen beim Filtern der Anforderungen:

- . (leere Erweiterung)
- .appcache
- .aspx
- .cr
- .css
- .dtd
- .gif
- .htm
- .html
- .ica
- .ico
- .jpg
- .js
- .png
- .svg
- .txt
- .xml

Ist Download oder Upgrade von Citrix Receiver für Citrix Receiver für Web aktiviert, sind für StoreFront außerdem diese Dateinamenerweiterung erforderlich:

- .dmg
- .exe

Ist Citrix Receiver für HTML5 aktiviert, sind für StoreFront zusätzlich diese Dateinamenerweiterung erforderlich:

- .eot
- .ttf
- .woff

MIME-Typen

Sie können die MIME-Typen für die folgenden Dateitypen entfernen:

- .exe
- .dll
- .com
- .bat
- .csh

Anforderungsfilterung

StoreFront benötigt die folgenden HTTP-Verben beim Filtern der Anforderungen: Sie können nicht aufgeführte Verben ausschließen.

- GET
- POST
- HEAD

Andere Microsoft IIS-Einstellungen

Für StoreFront ist Folgendes nicht erforderlich:

- ISAPI-Filter
- ISAPI-Erweiterungen
- CGI-Programme
- FastCGI-Programme

> ## Important
>
> - Konfigurieren Sie keine IIS-Autorisierungsregeln. StoreFront unterstützt die direkte Authentifizierung und verwendet oder unterstützt keine IIS-Authentifizierung.
> - Wählen Sie in den SSL-Einstellungen für die StoreFront-Site nicht **Clientzertifikate: Erforderlich** aus. Die StoreFront-Installation konfiguriert die entsprechenden Seiten der StoreFront-Site mit dieser Einstellung.
> - StoreFront benötigt Cookies. Die Verwendung Cookies muss ausgewählt sein. Wählen Sie nicht die Einstellung "cookieless"/URI verwenden.
> - StoreFront erfordert volles Vertrauen. Legen Sie jedoch nicht die globale .NET-Vertrauensebene auf "Hoch" oder niedriger fest.
> - StoreFront unterstützt nicht einen separaten Anwendungspool für jede Site. Ändern Sie diese Siteeinstellungen nicht. Sie können jedoch das Leerlauftimeouts für den Anwendungspools und die Menge des virtuellen Speichers festlegen, die ein Anwendungspool verbraucht.

Konfigurieren von Benutzerrechten

Wenn Sie StoreFront installieren, werden den Anwendungspools die Anmeldeberechtigung **Anmelden als Dienst** und die Privilegien **Anpassen von Speicherkontingenten für einen Prozess, Generieren von Sicherheitsüberwachungen** und **Ersetzen eines Tokens auf Prozessebene** zugewiesen. Dies ist normales Installationsverhalten beim Erstellen von Anwendungspools.

Sie brauchen die Benutzerrechte nicht zu ändern. Diese Privilegien werden von StoreFront nicht verwendet und werden automatisch deaktiviert.

Bei der StoreFront-Installation werden die folgenden Windows-Dienste erstellt:

- Citrix Konfigurationsreplikationsdienst (NT SERVICE\CitrixConfigurationReplication)
- Citrix Clusterbeitrittsdienst (NT SERVICE\CitrixClusterService)
- Citrix Peerauflösungsdienst (NT SERVICE\Citrix Peer Resolution Service)
- Citrix Credential Wallet-Dienst (NT SERVICE\CitrixCredentialWallet)
- Citrix Abonnementstoredienst (NT SERVICE\CitrixSubscriptionsStore)
- Citrix Standarddomänendienste (NT SERVICE\CitrixDefaultDomainService)

Wenn Sie für StoreFront die eingeschränkte Kerberos-Delegierung für XenApp 6.5 konfigurieren, wird der Citrix StoreFront-Protokollübergangsdienst (NT SERVICE\SYSTEM) erstellt. Dieser Dienst benötigt ein Privileg, dass normalweise Windows-Diensten nicht gewährt wird.

Konfigurieren von Diensteinstellungen

Die die oben im Abschnitt "Konfigurieren von Benutzerrechten" aufgelisteten Windows-Dienste für StoreFront verwenden beim Anmelden die Identität "Netzwerkdienst". Der StoreFront-Protokollübergangsdienst meldet sich als "SYSTEM" an. Ändern Sie diese Konfiguration nicht.

Konfigurieren der Gruppenmitgliedschaften

Die StoreFront-Installation fügt die folgenden Dienste der Adminstratorsicherheitsgruppe hinzu:

- Citrix Konfigurationsreplikationsdienst (NT SERVICE\CitrixConfigurationReplication)
- Citrix Clusterbeitrittsdienst (NT SERVICE\CitrixClusterService)

Diese Gruppenmitgliedschaften sind erforderlich damit StoreFront korrekt funktioniert:

- Erstellen, Exportieren, Importieren, Löschen und Festlegen der Zugriffsberechtigungen von Zertifikaten
- Lesen und Schreiben der Windows-Registrierung
- Hinzufügen und Entfernen von Microsoft .NET Framework-Assemblys im globalen Assemblycache (GAC)
- Zugriff auf den Ordner **Programme\Citrix**<*StoreFrontSpeicherort*>
- Hinzufügen, Bearbeiten und Entfernen von App-Poolidentitäten und IIS-Webanwendungen
- Hinzufügen, Bearbeiten und Entfernen von lokalen Sicherheitsgruppen und Firewallregeln
- Hinzufügen und Entfernen von Windows-Diensten und PowerShell-Snap-Ins
- Registrieren von Microsoft Windows Communication Framework (WCF)-Endpunkten

Bei Updates zu StoreFront kann sich diese Liste der Operationen ohne Ankündigung ändern.

Die StoreFront-Installation erstellt außerdem die folgenden lokalen Sicherheitsgruppen:

- CitrixClusterMembers
- CitrixCWServiceReadUsers
- CitrixCWServiceWriteUsers
- CitrixDelegatedAuthenticatorUsers
- CitrixDelegatedDirectoryClaimFactoryUsers
- CitrixPNRSUsers
- CitrixStoreFrontPTServiceUsers
- CitrixSubscriptionServerUsers
- CitrixSubscriptionsStoreServiceUsers
- CitrixSubscriptionsSyncUsers

StoreFront verwaltet die Mitgliedschaft in diesen Sicherheitsgruppen. Sie werden für die Zugriffssteuerung in StoreFront

verwendet und nicht auf Windows-Ressourcen wie Ordner und Dateien angewendet. Bearbeiten Sie diese Gruppenmitgliedschaften nicht.

Zertifikate in StoreFront

Serverzertifikate

Serverzertifikate werden zur Identifikation der Maschinen und für die TLS-Transportsicherheit in StoreFront verwendet. Wenn Sie die ICA-Dateisignierung aktivieren, kann StoreFront auch Zertifikate verwenden, um ICA-Dateien digital zu signieren.

Zum Aktivieren der e-mail-basierten Kontenermittlung für Benutzer, die Citrix Receiver auf einem Gerät zum ersten Mal installieren, müssen Sie ein gültiges Serverzertifikat auf dem StoreFront-Server installieren. Des Weiteren muss die vollständige Kette zum Stammzertifikat gültig sein. Um optimale Benutzerfreundlichkeit zu erzielen, installieren Sie ein Zertifikat, das für Antragsteller oder Alternativer Antragstellername den Eintrag **discoverReceiver.domain**, wobei domainder Name der Active Directory-Domäne mit den E-Mail-Konten der Benutzer ist. Obwohl Sie ein Zertifikat mit Platzhalterzeichen für die Domäne verwenden können, die die E-Mail-Konten der Benutzer enthält, müssen Sie zunächst sicherstellen, dass die Bereitstellung solcher Zertifikate von den Sicherheitsrichtlinien Ihres Unternehmens zugelassen wird. Sie können andere Zertifikate für die Domäne mit den Benutzer-E-Mail-Konten verwenden, den Benutzern wird jedoch bei der ersten Verbindungsherstellung von Citrix Receiver mit dem StoreFront-Server eine Warnung bezüglich des Zertifikats angezeigt. Die e-mail-basierte Kontenermittlung kann nicht mit anderen Zertifikatidentitäten verwendet werden. Weitere Informationen finden Sie unter Konfigurieren der e-mail-basierten Kontenermittlung.

Wenn Benutzer ihre Konten selbst durch Eingeben der Store-URLs in Citrix Receiver konfigurieren, statt über die e-mail-basierte Kontenermittlung, muss das Zertifikat auf dem StoreFront-Server nur für diesen Server gültig sein und eine gültige Kette zum Stammzertifikat haben.

Tokenverwaltungszertifikate

Sowohl die Authentifizierungsdienste als auch Stores benötigen Zertifikate für die Tokenverwaltung. StoreFront generiert ein selbstsigniertes Zertifikat, wenn ein Authentifizierungsdienst oder Store erstellt wird. Von StoreFront generierte, selbstsignierte Zertifikate sollten für keinen anderen Zweck verwendet werden.

Citrix Delivery Services-Zertifikate

StoreFront hält eine Reihe von Zertifikaten in einem benutzerdefinierten Windows-Zertifikatspeicher (Citrix Delivery Services). Der Citrix Konfigurationsreplikationsdienst, der Citrix Credential Wallet-Dienst und der Citrix Abonnementstoredienst verwenden diese Zertifikate. Jeder StoreFront-Server in einem Cluster hat eine Kopie dieser Zertifikate.Diese Dienste verwenden nicht TLS für die sichere Kommunikation und diese Zertifikate werden nicht als TLS-Serverzertifikate verwendet.Diese Zertifikate werden erstellt, wenn ein StoreFront-Store erstellt oder wenn StoreFront installiert wird.Ändern Sie den Inhalt dieses Windows-Zertifikatspeichers nicht.

Codesignaturzertifikate

StoreFront enthält eine Reihe von PowerShell-Skripts (.ps1) im Ordner \Scripts. Die Standardinstallation von StoreFront verwendet diese Skripts nicht. Sie vereinfachen Konfigurationsschritte für bestimmte, seltene Aufgaben. Diese Skripts sind signiert, so dass StoreFront eine PowerShell-Ausführungsrichtlinie unterstützen kann. Wir empfehlen die Richtlinie **AllSigned**. (Die Richtlinie **Restricted** wird nicht unterstützt, da dadurch das Ausführen von PowerShell-Skripts verhindert wird.) StoreFront ändert die PowerShell-Ausführungsrichtlinie nicht.

Obwohl StoreFront kein Codesignaturzertifikat in der Aufstellung der vertrauenswürdigen Herausgeber installiert, kann

Windows dort automatisch das Codesignaturzertifikat hinzufügen. Dies geschieht, wenn das PowerShell-Skript mit der Option **Immer ausführen** ausgeführt wird. (Wenn Sie die Option **Nie ausführen** wählen, wird das Zertifikat der Aufstellung der nicht vertrauenswürdigen Zertifikate hinzugefügt, und die PowerShell-Skripts von StoreFront werden nicht ausgeführt.) Nachdem das Codesignaturzertifikat der Aufstellung der vertrauenswürdigen Herausgeber hinzugefügt wurde, wird das Ablaufen nicht mehr von Windows geprüft. Sie können dieses Zertifikat aus der Aufstellung der vertrauenswürdigen Herausgeber entfernen, nachdem die StoreFront-Aufgaben abgeschlossen wurden.

StoreFront-Kommunikation

Citrix empfiehlt für Produktionsumgebungen die Verwendung von IPsec (Internet Protocol Security) oder von HTTPS-Protokollen zum Schutz der Datenübertragung zwischen StoreFront und Ihren Servern. IPsec bietet eine Reihe von Standarderweiterungen des Internetprotokolls, die authentifizierte und verschlüsselte Kommunikation mit Datenintegrität und Schutz vor Wiedergabeangriffen bieten. Da IPsec ein Protokollsatz der Vermittlungsschicht ist, können Protokolle höherer Stufen es unverändert verwenden. HTTPS verwendet Secure Sockets Layer (SSL) und Transport Layer Security (TLS) für eine starke Datenverschlüsselung.

SSL-Relay kann verwendet werden, um den Datenverkehr zwischen StoreFront und XenApp-Servern zu schützen. SSL-Relay ist eine Standardkomponente von XenApp, die die Hostauthentifizierung und Datenverschlüsselung übernimmt.

Citrix empfiehlt, die Kommunikation zwischen StoreFront und Benutzergeräten mit NetScaler Gateway und HTTPS zu schützen. Damit HTTPS verwendet werden kann, müssen die Microsoft Internet Information Services (IIS)-Instanz, auf der der Authentifizierungsdienst gehostet wird, und damit verknüpfte Stores für HTTPS konfiguriert sein. Wenn die entsprechende IIS-Konfiguration nicht verfügbar ist, verwendet StoreFront HTTP für die Kommunikation. Citrix empfiehlt dringend, keine ungeschützten Benutzerverbindungen mit StoreFront in einer Produktionsumgebung zu aktivieren.

StoreFront-Sicherheitsisolierung

Falls Sie Webanwendungen in derselben Webdomäne (Domänenname und Port) wie StoreFront bereitstellen, können die mit diesen Webanwendungen verbundenen Sicherheitsrisiken eventuell auch die Sicherheit der StoreFront-Bereitstellung beeinträchtigen. Ist höhere Sicherheit erforderlich, empfiehlt Citrix die Bereitstellung von StoreFront in einer getrennten Webdomäne.

ICA-Dateisignierung

In StoreFront können ICA-Dateien digital mit einem auf dem Server angegebenen Zertifikat signiert werden, damit Citrix Receiver-Versionen, die dieses Feature unterstützen, sicherstellen können, dass die Datei aus einer vertrauenswürdigen Quelle stammt. ICA-Dateien können mit einem Hashalgorithmus signiert werden, der von dem auf dem StoreFront-Server ausgeführten Betriebssystem unterstützt wird, z. B. SHA-1 und SHA-256. Weitere Informationen finden Sie unter Aktivieren der ICA-Dateisignierung.

Benutzerseitige Kennwortänderung

Sie können Benutzern von Receiver für Web-Sites, die sich mit Active Directory-Domänenanmeldeinformationen anmelden, gestatten, ihre Kennwörter zu ändern, und zwar entweder jederzeit oder nur, wenn sie abgelaufen sind. Dadurch werden jedoch vertrauliche Sicherheitsfunktionen für alle Personen offengelegt, die auf einen der Stores, die diesen Authentifizierungsdienst verwenden, zugreifen können. Wenn Ihr Unternehmen eine Sicherheitsrichtlinie hat, die Funktionen zur Änderung des Kennworts nur zur internen Verwendung reserviert, stellen Sie sicher, dass auf keinen der Stores von außerhalb des Unternehmensnetzwerks zugegriffen werden kann. Beim Erstellen des Authentifizierungsdiensts verhindert die Standardkonfiguration, dass Benutzer von Receiver für Web-Sites ihre Kennwörter ändern, selbst wenn die Kennwörter abgelaufen sind. Weitere Informationen finden Sie unter Optimieren der Benutzererfahrung.

Anpassungen

Erstellen Sie aus Sicherheitsgründen keine Anpassungen, mit denen Inhalte oder Skripts von Servern geladen werden, die nicht Ihrer Kontrolle unterstehen. Kopieren Sie den Inhalt bzw. das Skript in den benutzerdefinierten Citrix Receiver für Web-Site-Ordner, wo Sie die Anpassungen erstellen. Wenn StoreFront für HTTPS-Verbindungen konfiguriert ist, müssen alle Links zu benutzerdefinierten Inhalten und Skripts ebenfalls HTTPS verwenden.

Exportieren und Importieren der StoreFront-Konfiguration

Nov 27, 2017

Sie können die gesamte Konfiguration einer StoreFront-Bereitstellung exportieren.Dies schließt Einzelserverbereitstellungen und Servergruppenkonfigurationen ein.Wenn eine vorhandene Bereitstellung bereits auf dem importierenden Server besteht, wird die aktuelle Konfiguration gelöscht und durch die im Backuparchiv enthaltene Konfiguration ersetzt.Wenn der Zielserver eine saubere Werkstandardinstallation ist, wird mit der aus dem Backup importierten Konfiguration eine neue Bereitstellung erstellt.Das exportierte Konfigurationsbackup ist im unverschlüsselten Zustand ein ZIP-Archiv oder eine CTXZIP-Datei, wenn Sie die Backupdatei bei ihrer Erstellung verschlüsseln.

Punkte, die beim Exportieren und Importieren einer StoreFront-Konfiguration zu berücksichtigen sind

PowerShell-Anmeldeinformationsobjekte zum Ver- und Entschlüsseln von StoreFront-Backups

PowerShell-Cmdlets

Beispiele für Konfigurationsexporte und -importe

Punkte, die beim Exportieren und Importieren einer StoreFront-Konfiguration zu berücksichtigen sind

- Möchten Sie die Host-Basis-URL aus dem Backuparchiv verwenden oder eine neue Host-Basis-URL auf dem importierenden Server festlegen?
- Verwenden Sie zurzeit von Citrix veröffentlichte Authentifizierungs-SDKs, wie Magic Word-Authentifizierung oder Authentifizierungsanpassungen von Drittanbietern?In diesem Fall müssen Sie diese Pakete auf ALLEN importierenden Servern installieren, BEVOR Sie eine Konfiguration importieren, die spezielle Authentifizierungsmethoden enthält.Wenn erforderliche Authentifizierungs-SDKs nicht auf den importierenden Servern installiert sind, schlägt der Import der Konfiguration fehl.Beim Importieren einer Konfiguration in eine Servergruppe müssen Sie die Authentifizierungspakete auf allen Mitgliedern der Gruppe installieren.
- Sie können die Konfigurationsbackups ver- und entschlüsseln. Die exportierenden und importierenden PowerShell-Cmdlets unterstützen beide Anwendungsfälle.
- Sie können verschlüsselte Backups (.ctxzip) später entschlüsseln; StoreFront kann unverschlüsselte Backupdateien (.zip) jedoch nicht erneut verschlüsseln.Wenn ein verschlüsseltes Backup erforderlich ist, führen Sie den Export erneut durch und verwenden Sie dabei ein PowerShell-Anmeldeinformationenobjekt mit einem Kennwort Ihrer Wahl.
- Die Site-ID der Website in IIS, in der StoreFront installiert ist (exportierender Server), muss mit der Site-ID der Zielwebsite in IIS (importierender Server) übereinstimmen, für die Sie das Backup der StoreFront-Konfiguration wiederherstellen möchten.

PowerShell-Anmeldeinformationsobjekte zum Ver- und Entschlüsseln von StoreFront-Backups

Ein PowerShell-Anmeldeinformationenobjekt enthält den Benutzernamen und das Kennwort für ein Windows-Konto.PowerShell-Anmeldeinformationsobjekte gewährleisten, dass Ihr Kennwort im Speicher geschützt ist.

> ### Hinweis
>
> Zum Verschlüsseln und Entschlüsseln eines Konfigurationsbackuparchivs benötigen Sie nur das Kennwort. Der im Anmeldeinformationsobjekt gespeicherte Benutzername wird nicht verwendet.Sie müssen in den PowerShell-Sitzungen ein

Anmeldeinformationsobjekt mit demselben Kennwort erstellen, **das auf den exportierenden und importierenden Servern verwendet wird**.Sie können im Anmeldeinformationsobjekt einen beliebigen Benutzer angeben.

PowerShell erfordert die Angabe eines Benutzers beim Erstellen eines neuen Anmeldeinformationsobjekts. Der folgende Beispielcode enthält nur den zurzeit angemeldeten Windows-Benutzer.

```
$User = [System.Security.Principal.WindowsIdentity]::GetCurrent().Name
$Password = "Pa55w0rd"
$Password = $Password | ConvertTo-SecureString -asPlainText -Force
$CredObject = New-Object System.Management.Automation.PSCredential($User,$Password)
```

PowerShell-Cmdlets

Export-STFConfiguration

Parameter	Beschreibung
-TargetFolder (String)	Der Exportpfad für das Backuparchiv. Beispiel: "$env:userprofile\desktop\"
-Credential (PSCredential Object)	Geben Sie ein Anmeldeinformationsobjekt an, um während des Exports ein verschlüsseltes CTXZIP-Backuparchiv zu erstellen. Das PowerShell-Anmeldeinformationsobjekt muss das Kennwort für die Ver- und Entschlüsselung enthalten. Verwenden Sie nicht **-Credential** gleichzeitig mit dem Parameter **-NoEncryption**. Beispiel: $CredObject
-NoEncryption (Switch)	Geben Sie an, dass das Backuparchiv eine unverschlüsselte ZIP-Datei ist. Verwenden Sie nicht **-NoEncryption** gleichzeitig mit dem Parameter **-Credential**.
-ZipFileName (Zeichenfolge)	Der Name des StoreFront-Konfigurationsbackuparchivs.Fügen Sie keine Dateierweiterung wie .zip oder .ctxzip hinzu.Die Dateierweiterung wird automatisch hinzugefügt und hängt davon ab, ob beim Export der Parameter **-Credential** oder **-NoEncryption** angegeben wird. Beispiel: "backup"
-Force (Boolean)	Dieser Parameter überschreibt automatisch Backuparchive mit demselben Dateinamen, die bereits im angegebenen Speicherort vorhanden sind.

Important

Der Parameter **-SiteID** aus StoreFront 3.5 ist in Version 3.6 veraltet.Beim Import muss **SiteID** nicht mehr angegeben werden, da immer die Site-ID aus dem Backuparchiv verwendet wird.Stellen Sie sicher, dass die Site-ID mit der vorhandenen StoreFront-Website übereinstimmt, die bereits in IIS auf dem importierenden Server konfiguriert ist.Konfigurationsimports von **SiteID 1** zu **SiteID 2** (oder umgekehrt) werden NICHT unterstützt.

Import-STFConfiguration

Parameter	Beschreibung
-ConfigurationZip (Zeichenfolge)	Der vollständige Pfad für das Backuparchiv, das Sie importieren.Er muss die Dateierweiterung enthalten.Verwenden Sie .zip für unverschlüsselte und .ctxzip für verschlüsselte Backuparchive. Beispiel: "$env:userprofile\desktop\backup.ctxzip"
-Credential (PSCredential Object)	Geben Sie ein Anmeldeinformationsobjekt an, um während des Imports eine verschlüsselte Backupdatei zu entschlüsseln. Beispiel: $CredObject
-HostBaseURL (Zeichenfolge)	Wenn dieser Parameter enthalten ist, wird die von Ihnen angegebene Host-Basis-URL statt der Host-Basis-URL des exportierenden Servers verwendet. Beispiel: "https://.example.com"

Unprotect-STFConfigurationBackup

Parameter	Beschreibung
-TargetFolder (String)	Der Exportpfad für das Backuparchiv. Beispiel: "$env:userprofile\desktop\"
-Credential (PSCredential Object)	Erstellen Sie mit diesem Parameter eine unverschlüsselte Kopie des verschlüsselten Backuparchivs.Geben Sie das PowerShell-Anmeldeinformationsobjekt an, das das Kennwort für die Entschlüsselung enthält. Beispiel: $CredObject
-EncryptedConfigurationZip	Der vollständige Pfad für das verschlüsselte Backuparchiv, das Sie entschlüsseln möchten.Sie müssen die Dateierweiterung CTXZIP angeben.

(Zeichenfolge)	Beispiel: "$env:userprofile\desktop\backup.ctxzip"
-OutputFolder (Zeichenfolge)	Der Pfad für eine unverschlüsselte Kopie des verschlüsselten Backuparchivs (.ctxzip).Die ursprüngliche verschlüsselte Kopie des Backups bleibt erhalten, sodass sie wiederverwendet werden kann.Geben Sie für die unverschlüsselte Kopie keinen Dateinamen und keine Dateierweiterung an. Beispiel: "$env:userprofile\desktop\"
-Force (Boolean)	Dieser Parameter überschreibt automatisch Backuparchive mit demselben Dateinamen, die bereits im angegebenen Speicherort vorhanden sind.

Beispiele für Konfigurationsexporte und -importe

Importieren des StoreFront SDKs in die aktuelle PowerShell-Sitzung

Öffnen Sie PowerShell Integrated Scripting Environment (ISE) auf dem StoreFront-Server und führen Sie Folgendes aus:

```
$SDKModules = 'C:\Program Files\Citrix\Receiver StoreFront\PowerShellSDK\Modules\Citrix.StoreFront'
Import-Module "$SDKModules\Citrix.StoreFront.psd1" -verbose
Import-Module "$SDKModules.Authentication\Citrix.StoreFront.Authentication.psd1" -verbose
Import-Module "$SDKModules.Roaming\Citrix.StoreFront.Roaming.psd1" -verbose
Import-Module "$SDKModules.Stores\Citrix.StoreFront.Stores.psd1" -verbose
Import-Module "$SDKModules.WebReceiver\Citrix.StoreFront.WebReceiver.psd1" -verbose
Import-Module "$SDKModules.SubscriptionsStore\Citrix.StoreFront.SubscriptionsStore.psd1" -verbose
```

Einzelserverszenarios

Erstellen Sie ein unverschlüsseltes Backup einer vorhandenen Konfiguration auf Server A und stellen Sie es auf derselben Bereitstellung wieder her.

```
Export-STFConfiguration -targetFolder "$env:userprofile\desktop\" -zipFileName "backup" -NoEncryption
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\backup.zip"
```

Erstellen Sie ein verschlüsseltes Backup einer vorhandenen Konfiguration auf Server A und stellen Sie es auf derselben Bereitstellung wieder her.

```
# Create a PowerShell Credential Object
$User = [System.Security.Principal.WindowsIdentity]::GetCurrent().Name
$Password = "Pa55w0rd"
$Password = $Password | ConvertTo-SecureString -asPlainText -Force
$CredObject = New-Object System.Management.Automation.PSCredential($User,$Password)
Export-STFConfiguration -targetFolder "$env:userprofile\desktop\" -zipFileName "backup" -Credential $CredObject
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\backup.ctxzip" -Credential $CredObject
```

Aufheben des Schutzes eines vorhandenen verschlüsselten Backuparchivs

```
$User = [System.Security.Principal.WindowsIdentity]::GetCurrent().Name
$Password = "Pa55w0rd"
$Password = $Password | ConvertTo-SecureString -asPlainText -Force
$CredObject = New-Object System.Management.Automation.PSCredential($User,$Password)
Unprotect-STFConfigurationExport -encryptedConfigurationZip "$env:userprofile\desktop\backup.ctxzip" -credential
$CredObject -outputFolder "c:\StoreFrontBackups" -Force
```

Erstellen Sie ein Backup einer vorhandenen Konfiguration auf Server A und stellen Sie es auf einer neuen Werkstandardinstallation auf Server B wieder her.

Server B ist eine neue Bereitstellung und soll neben Server A existieren. Geben Sie den Parameter **-HostBaseURL** an.Server B ist zudem eine neue StoreFront-Werkstandardinstallation.

1. Erstellen Sie ein PowerShell-Anmeldeinformationsobjekt und exportieren Sie eine verschlüsselte Kopie der Server A-Konfiguration.
2. Erstellen Sie ein PowerShell-Anmeldeinformationsobjekt auf Server B und verwenden Sie dazu das gleiche Kennwort, das Sie zum Verschlüsseln des Backups verwendet haben.
3. Entschlüsseln und importieren Sie die Server A-Konfiguration mit dem Parameter **-HostBaseURL** in Server B.

    ```
    Import-STFConfiguration -configurationZip "$env:userprofile\desktop\backup.ctxzip" -Credential $CredObject -
    HostBaseURL "https://serverB.example.com"
    ```

Erstellen Sie ein Backup einer vorhandenen Konfiguration auf Server A und überschreiben Sie damit eine vorhandene Bereitstellung auf Server B.

Server B ist eine vorhandene Bereitstellung mit einer veralteten Konfiguration. Aktualisieren Sie Server B anhand der Konfiguration von Server A. Server B soll mit Server A koexistieren. Geben Sie den Parameter **-HostBaseURL** an.

1. Erstellen Sie ein PowerShell-Anmeldeinformationsobjekt und exportieren Sie eine verschlüsselte Kopie der Server A-Konfiguration.
2. Erstellen Sie ein PowerShell-Anmeldeinformationsobjekt auf Server B und verwenden Sie dazu das gleiche Kennwort, das Sie zum Verschlüsseln des Backups verwendet haben.
3. Entschlüsseln und importieren Sie die Server A-Konfiguration mit dem Parameter **-HostBaseURL** in Server B.

    ```
    Import-STFConfiguration -configurationZip "$env:userprofile\desktop\backup.ctxzip" –Credential $CredObject -
    HostBaseURL "https://serverB.example.com"
    ```

Erstellen Sie einen Klon einer vorhandenen Bereitstellung mit derselben Host-Basis-URL wie beim Upgrade auf ein neues Serverbetriebssystem und setzen Sie eine überholte StoreFront-Bereitstellung außer Betrieb.

2012R2 Server B ist eine neue Bereitstellung, die den überholten 2008R2 Server A ersetzten soll. Verwenden Sie die HostBaseURL aus dem Sicherungsarchiv. Verwenden Sie während des Imports nicht den Parameter **-HostBaseURL**.Server B ist zudem eine neue StoreFront-Werkstandardinstallation.

1. Erstellen Sie ein PowerShell-Anmeldeinformationsobjekt und exportieren Sie eine verschlüsselte Kopie der 2008R2 Server A-Konfiguration.

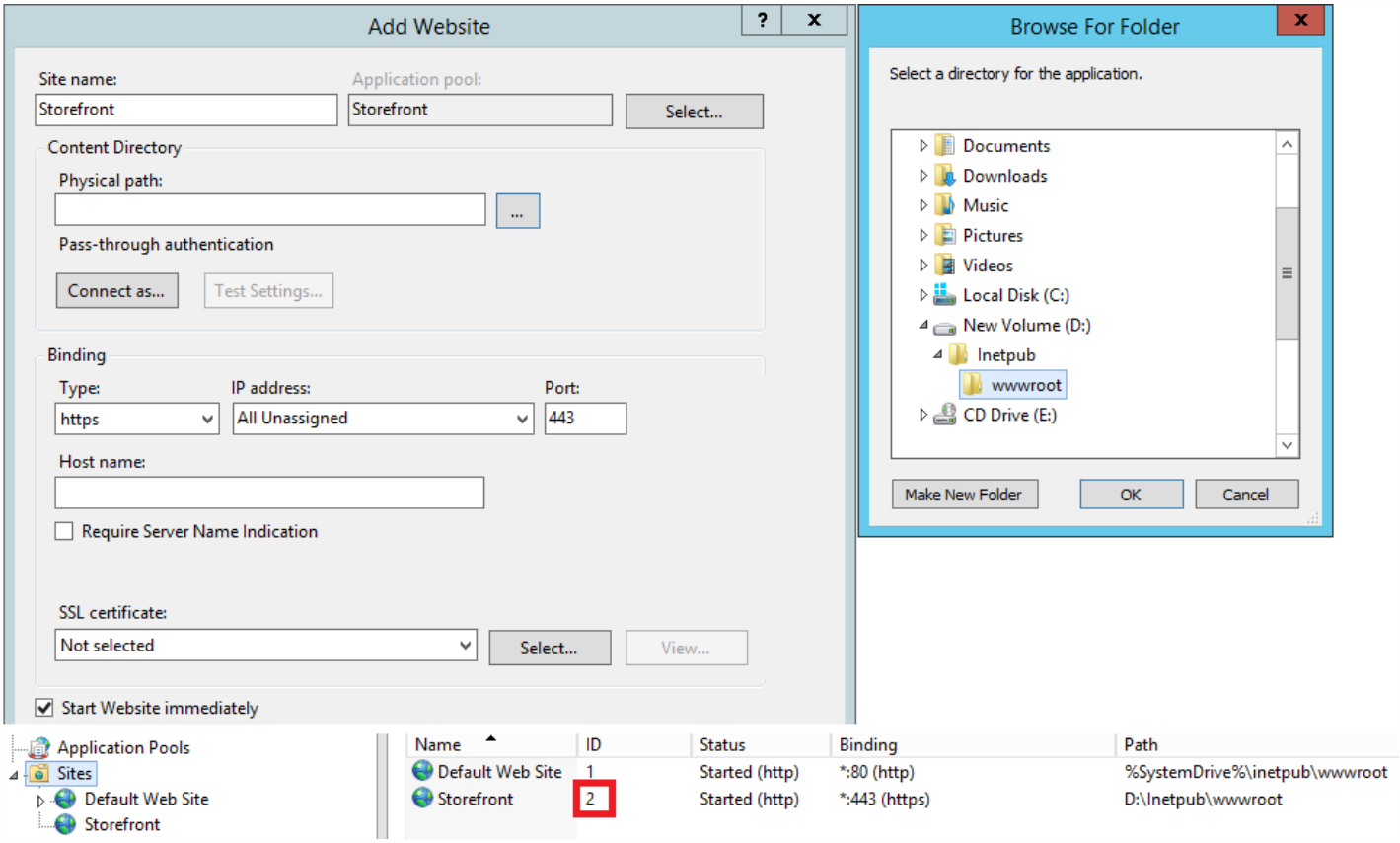
2. Erstellen Sie ein PowerShell-Anmeldeinformationsobjekt auf 2012R2 Server B und verwenden Sie dazu das gleiche Kennwort, das Sie zum Verschlüsseln des Backups verwendet haben.
3. Entschlüsseln und importieren Sie die 2008R2 Server A-Konfiguration mit dem Parameter **-HostBaseURL** in 2012R2 Server B.

    Import-STFConfiguration -configurationZip "$env:userprofile\desktop\backup.ctxzip" -Credential $CredObject -HostBaseURL "https://serverB.example.com"

StoreFront ist bereits auf einer benutzerdefinierten Website in IIS bereitgestellt. Stellen Sie die Konfiguration auf einer anderen benutzerdefinierten Websitebereitstellung wieder her.

Bei Server A ist StoreFront auf einer benutzerdefinierten Website bereitgestellt statt der gewohnten Standardwebsite in IIS.Die IIS Site-ID für die zweite in IIS erstellte Website ist 2.Der physische Pfad der StoreFront-Website kann auf einem anderen Laufwerk sein, das nicht zum System gehört, wie d:\ oder auf dem standardmäßigen Systemlaufwerk c:\. Er sollte jedoch eine IIS Site-ID verwenden, die größer als 1 ist.

In IIS wurde eine neue Website mit dem Namen StoreFront konfiguriert, die **SiteID = 2** verwendet.StoreFront wurde bereits auf der benutzerdefinierten Website in IIS bereitgestellt und der physische Pfad ist d:\inetpub\wwwrooot\.



1. Erstellen Sie ein PowerShell-Anmeldeinformationsobjekt und exportieren Sie eine verschlüsselte Kopie der Server A-Konfiguration.
2. Konfigurieren Sie IIS auf Server B mit einer neuen Website mit dem Namen **StoreFront**, die ebenfalls **SiteID 2** verwendet.
3. Erstellen Sie ein PowerShell-Anmeldeinformationsobjekt auf Server B und verwenden Sie dazu das gleiche Kennwort, das Sie zum Verschlüsseln des Backups verwendet haben.
4. Entschlüsseln und importieren Sie die Server A-Konfiguration mit dem Parameter **-HostBaseURL** in Server B.Die im Backup

enthaltene Site-ID wird verwendet und muss mit der Zielwebsite übereinstimmen, in die Sie die StoreFront-Konfiguration importieren möchten.

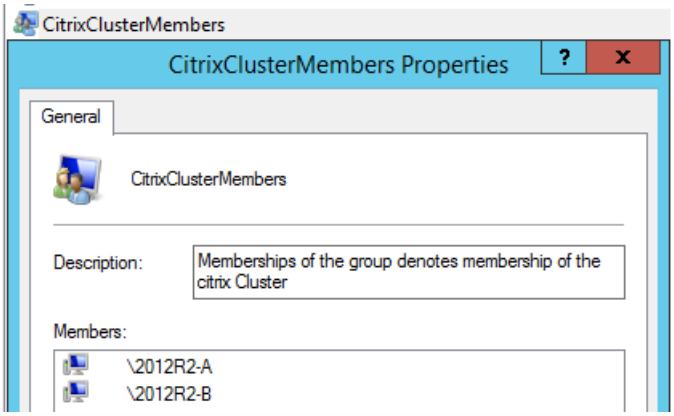
```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\backup.ctxzip" -Credential $CredObject -
HostBaseURL "https://serverB.example.com"
```

Servergruppenszenarios

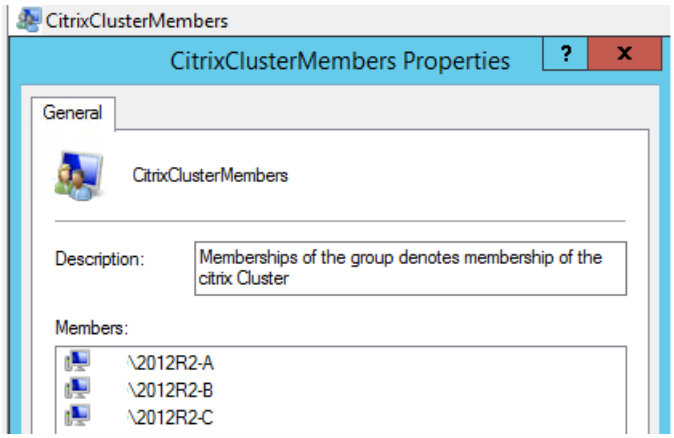
Szenario 1: Erstellen Sie ein Backup einer vorhandenen Servergruppenkonfiguration und stellen Sie die Konfiguration in derselben Servergruppenbereitstellung später wieder her.

Zu einem früheren Zeitpunkt, als die Servergruppe nur zwei StoreFront-Server, 2012R2-A und 2012R2-B, enthielt, wurde ein Backup der Konfiguration erstellt.Das Backuparchiv enthält einen Datensatz der **CitrixClusterMembership**, die zur Zeit des Backups nur die beiden ursprünglichen Server 2012R2-A und 2012R2-B enthielt.Die Größe der StoreFront-Servergruppenbereitstellung ist seit dem ursprünglichen Backup aufgrund des Unternehmensbedarfs angestiegen und ein zusätzlicher Knoten, 2012R2-C, wurde der Servergruppe hinzugefügt.Die zugrunde liegende StoreFront-Konfiguration der Servergruppe im Backup hat sich nicht geändert.Die aktuelle CitrixClusterMembership von drei Servern muss erhalten bleiben, auch wenn ein altes Backup mit nur den zwei ursprünglichen Servergruppenknoten importiert wird.Während des Imports wird die aktuelle Clustermitgliedschaft beibehalten und zurückgeschrieben, wenn die Konfiguration erfolgreich auf den primären Server importiert wurde.Beim Import wird auch die aktuelle CitrixClusterMembership beibehalten, wenn Servergruppenknoten seit dem Erstellen des ursprünglichen Backups entfernt wurden.

1. Exportieren Sie die Konfiguration der Servergruppe 1 aus 2012R2-A, dem primären Server, der die gesamte Servergruppe verwaltet.



2. Fügen Sie der vorhandenen Servergruppe dann einen weiteren Server, 2012R2-C, hinzu.



3. Stellen Sie die Konfiguration der Servergruppe auf einen früheren funktionierenden Zustand wieder her. Während des Importvorgangs erstellt StoreFront ein Backup der aktuellen CitrixClusterMembership der drei Server und stellt sie nach dem Abschluss des Imports wieder her.

4. Importieren Sie die Konfiguration der Servergruppe 1 zurück auf den Knoten 2012R2-A.

Import-STFConfiguration -configurationZip "$env:userprofile\desktop\backup.ctxzip" -Credential $CredObject -HostBaseURL "https://serverB.example.com"

5. Übertragen Sie die importierte Konfiguration auf die gesamte Servergruppe, sodass alle Server nach dem Import eine konsistente Konfiguration aufweisen.

Szenario 2: Erstellen Sie ein Backup einer vorhandenen Konfiguration von Servergruppe 1 und erstellen Sie damit eine neue Servergruppe auf einer anderen Werkstandardinstallation.Sie können dem primären Server dann andere neue Servergruppenmitglieder hinzufügen.

Servergruppe 2 wird mit zwei neuen Servern erstellt: 2012R2-C und 2012R2-D. Die Konfiguration von Servergruppe 2 basiert auf der Konfiguration einer vorhandenen Bereitstellung, Servergruppe 1, die ebenfalls zwei Server enthält: 2012R2-A und 2012R2-B.Die im Backuparchiv enthaltene CitrixClusterMembership wird beim Erstellen einer neuen Servergruppe nicht verwendet. Von der aktuellen CitrixClusterMembership wird immer ein Backup erstellt und sie wird nach dem Abschluss des Imports wiederhergestellt. Wenn Sie mit einer importierten Konfiguration eine neue Bereitstellung erstellen, enthält die Sicherheitsgruppe CitrixClusterMembership nur den importierenden Server, bis weitere Server der neuen Gruppe hinzugefügt werden.Servergruppe 2 ist eine neue Bereitstellung und soll neben Servergruppe 1 bestehen. Geben Sie den Parameter -HostBaseURL an.Servergruppe 2 wird mit einer neuen StoreFront-Werkstandardinstallation erstellt.

1. Exportieren Sie die Konfiguration der Servergruppe 1 aus 2012R2-A, dem primären Server, der die gesamte Servergruppe verwaltet.

2. Importieren Sie die Konfiguration der Servergruppe 1 auf den Knoten 2012R2-C, der der primäre Server zum Verwalten der neu erstellten Servergruppe 2 ist.

Import-STFConfiguration -configurationZip "$env:userprofile\desktop\backup.ctxzip" -Credential $CredObject -HostBaseURL "https://serverB.example.com"

3. Verknüpfen Sie alle weiteren Server, die zur neuen Bereitstellung "Servergruppe 2" gehören sollen.Die neu aus Servergruppe 1 importierte Konfiguration wird automatisch auf alle neuen Mitglieder der Servergruppe 2 übertragen, da dies Teil des normalen Verknüpfungsvorgangs ist, wenn ein neuer Server hinzugefügt wird.

Szenario 3: Erstellen Sie ein Backup einer vorhandenen Konfiguration von Servergruppe A und überschreiben Sie damit die vorhandene Konfiguration der Servergruppe B.

Servergruppe 1 und Servergruppe 2 sind bereits in zwei verschiedenen Datencentern vorhanden.An Servergruppe 1 werden viele StoreFront-Konfigurationsänderungen vorgenommen, die Sie auf Servergruppe 2 im anderen Datencenter übertragen müssen.Sie können die Änderungen von Servergruppe 1 auf Servergruppe 2 per Port übertragen.Verwenden Sie **CitrixClusterMembership** nicht im Backuparchiv auf der Servergruppe 2.Legen Sie den Parameter **-HostBaseURL** während des Imports fest, da die Host-Basis-URL für Servergruppe 2 nicht in den gleichen vollqualifizierten Domänennamen (FQDN) geändert werden sollte, den die Servergruppe 1 zurzeit verwendet.Servergruppe 2 ist eine vorhandene Bereitstellung.

1. Exportieren Sie die Konfiguration der Servergruppe 1 aus 2012R2-A, dem primären Server, der die gesamte Servergruppe verwaltet.

2. Importieren Sie die Konfiguration der Servergruppe 1 auf die Werkstandardinstallation auf Knoten 2012R2-C, der der primäre Server der neu erstellten Servergruppe 2 ist.

```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\backup.ctxzip" -Credential $CredObject -HostBaseURL "https://serverB.example.com"
```

StoreFront SDK

Nov 27, 2017

Citrix StoreFront bietet ein SDK, das auf Modulen von Windows PowerShell Version 3.0 beruht. Mit dem SDK können Sie die gleichen Tasks wie mit der Citrix StoreFront-Verwaltungskonsole ausführen und darüber hinaus weitere Tasks, die mit der Konsole allein nicht möglich sind.

Die SDK-Referenz finden Sie unter StoreFront SDK.

Hauptunterschiede zwischen dem SDK von StoreFront 3.0 und dem aktuellen StoreFront SDK.

- **High-Level-SDK-Beispiele**: Diese Version bietet High-Level-SDK-Beispielskripts, mit denen Sie StoreFront-Bereitstellungen schnell und mühelos automatisieren können. Sie können diese Muster gemäß Ihren spezifischen Anforderungen anpassen und neue Bereitstellungen durch einfache Ausführung eines Skripts erstellen.
- **Neues Low-Level-SDK**: Citrix bietet ein Low-Level-StoreFront-SDK mit Dokumentation an, das die Konfiguration von Bereitstellungen einschließlich Stores, Authentifizierungsmethoden Citrix Receiver für Web- und einheitliche Citrix Receiver-Sites und Remotezugriff über NetScaler Gateway ermöglicht.
- **Abwärtskompatibilität**: StoreFront 3.6 enthält die APIs für StoreFront 3.0 und ältere Versionen, damit vorhandene Skripts nach und nach in das neue SDK übertragen werden können.

> ### Important
>
> Die Rückwärtskompatibilität mit StoreFront 3.0 wurde beibehalten, wenn es möglich und praktikabel war. Citrix empfiehlt jedoch, für neue Skripts die neuen **Citrix.StoreFront.***-Module zu verwenden, da das StoreFront 3.0-SDK veraltet ist und künftig entfernt wird.

Verwenden des SDKs

Das SDK enthält mehrere PowerShell-Snap-Ins, die automatisch vom Installationsassistenten installiert werden, wenn Sie verschiedene StoreFront-Komponenten installieren und konfigurieren.

Zugreifen auf die Cmdlets:

1. Starten Sie eine Shell in PowerShell 3.0.
   Zum Ausführen der Shell bzw. des Skripts müssen Sie als Mitglied der lokalen Administratorgruppe auf dem StoreFront-Server angemeldet sein.

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 Befehl **Add -Module** in der Windows PowerShell-Konsole die Module hinzu, die Sie in der PowerShell-Umgebung benötigen. Geben Sie beispielsweise
   Folgendes ein: Import-Module Citrix.StoreFront
   Geben Sie zum Importieren aller Cmdlets Folgendes ein:

   ```
   Get-Module -ListAvailable | Where-Object { $_.Name.StartsWith("Citrix.StoreFront") } | Import-Module
   ```

Nach dem Import haben Sie Zugriff auf die Cmdlets und die zugehörige Hilfe.

Erste Schritte mit dem SDK

Führen Sie folgende Schritte für das Erstellen eines Skripts aus:

1. Verwenden Sie eines der SDK-Beispiele, die zusammen mit StoreFront im Ordner **%ProgramFiles%\Citrix\Receiver StoreFront\PowerShellSDK\Examples** installiert wurden.
2. Das Beispielsskript zeigt die Aufgaben der verschiedenen Teile und hilft Ihnen, Ihr eigenes Skript anzupassen. Weitere Informationen finden Sie im Beispiel eines Anwendungsfalls, in dem die Skriptaktionen ausführlich beschrieben werden.
3. Passen Sie die Beispielskripts für Ihre Zwecke an. Gehen Sie hierzu folgendermaßen vor:
   - Verwenden Sie die PowerShell-ISE oder ein ähnliches Tool zum Bearbeiten des Skripts.
   - Verwenden Sie Variablen für Werte, die wiederverwendet oder geändert werden sollen.
   - Entfernen Sie alle Befehle, die nicht erforderlich sind.
   - StoreFront-Cmdlets können mit dem Präfix "STF" gekennzeichnet werden.
   - Verwenden Sie das Cmdlet "Get-Help" unter Angabe des Cmdlet-Namens und des Parameters "-Full", um Informationen zu einem bestimmten Befehl aufzurufen.

Beispiele

Hinweis: Um beim Erstellen eines Skripts sicherzustellen, dass Sie immer die aktuellen Verbesserungen und Fixes erhalten, empfiehlt Citrix, dass Sie den oben erläuterten Schritten folgen, anstatt das Beispielskript zu kopieren und einzufügen.

Beispiele	Beschreibung
	Skript: erstellt eine einfache Bereitstellung mit einem StoreFront-Controller, der mit einem einzelnen XenDesktop-Server konfiguriert ist.
	Skript: erstellt eine Bereitstellung wie im vorherigen Skript plus Remotezugriff.
	Skript: erstellt eine Bereitstellung wie im vorherigen Skript und ermöglicht das Hinzufügen bevorzugter Gateways für den optimalen Start zur Verbesserung der Benutzererfahrung.
	Skript: erstellt eine einfache Bereitstellung plus Konfiguration einer Desktopgerätesite.

Beispiel: Erstellen einer einfachen Bereitstellung

Anhand des folgenden Beispiels wird die Erstellung einer einfachen Bereitstellung mit einem einzelnen XenDesktop-Controller erläutert.

Bevor Sie beginnen, stellen Sie sicher, dass Sie die in Erste Schritte mit dem SDK aufgeführten Schritte ausführen. Das Beispiel kann unter Verwendung der beschriebenen Methoden zur Erstellung eines Skripts für die Automatisierung der StoreFront-Bereitstellung angepasst werden.

Hinweis: Um sicherzustellen, dass Sie immer die aktuellen Verbesserungen und Fixes erhalten, empfiehlt Citrix, dass Sie den in diesem Dokument beschriebenen Schritten folgen, anstatt das Beispielskript zu kopieren und einzufügen.

Inhalt des Skripts

In diesem Abschnitt wird die Funktion jedes Teils des Skripts erläutert, das StoreFront erstellt. Dies hilft Ihnen bei der Anpassung des eigenen Skripts.

- Legt Fehlerbehandlungsanforderungen fest und importiert die erforderlichen StoreFront-Module. Importe sind in neueren Versionen von PowerShell nicht erforderlich.

```
Param(
  [Parameter(Mandatory=$true)]
  [Uri]$HostbaseUrl,
  [long]$SiteId = 1,
  [ValidateSet("XenDesktop","XenApp","AppController","VDIinaBox")]
  [string]$Farmtype = "XenDesktop",
  [Parameter(Mandatory=$true)]
  [string[]]$FarmServers,
  [string]$StoreVirtualPath = "/Citrix/Store",
  [bool]$LoadbalanceServers = $false,
  [int]$Port = 80,
  [int]$SSLRelayPort = 443,
  [ValidateSet("HTTP","HTTPS","SSL")]
  [string]$TransportType = "HTTP"
)

# Importieren der StoreFront-Module. Erforderlich für PowerShell-Versionen vor 3.0, die automatisches Laden nicht unterstützen
Import-Module Citrix.StoreFront
Import-Module Citrix.StoreFront.Stores
Import-Module Citrix.StoreFront.Authentication
Import-Module Citrix.StoreFront.WebReceiver
```

- Automatisiert den virtuellen Pfad der Authentifizierungs- und Citrix Receiver für Web-Dienste basierend auf der Angabe **$StoreVirtualPath**.

```
# Ermitteln der für Authentifizierung und Receiver zu verwendenden virtuellen Pfade basierend auf dem Store

$authenticationVirtualPath = "$($StoreIISPath.TrimEnd('/'))Auth"

$receiverVirtualPath = "$($StoreVirtualPath.TrimEnd('/'))Web"
```

- Erstellt eine neue Bereitstellung, sofern es noch keine gibt, zur Vorbereitung auf das Hinzufügen der erforderlichen StoreFront-Dienste. **-Confirm:$false** unterdrückt die Anforderung einer Bestätigung zum Fortfahren der Bereitstellung.

```
# Prüfen, ob Bereitstellung bereits existiert

$existingDeployment = Get-STFDeployment

if(-not $existingDeployment)

{

   # Installieren der erforderlichen StoreFront-Komponenten

   Add-STFDeployment -HostBaseUrl $HostbaseUrl -SiteId $SiteId -Confirm:$false

}

elseif($existingDeployment.HostbaseUrl -eq $HostbaseUrl)

{

   # Bereitstellung vorhanden, jedoch für die gewünschte Hostebase-URL konfiguriert

  Write-Output "Eine Bereitstellung mit der angegebenen Hostbasis-URL wurde auf diesem Server bereits erstellt und wird verwendet."

}

else

{

  Write-Error "Eine Bereitstellung mit einer anderen Hostbasis-URL wurde auf diesem Server bereits erstellt."

}
```

- Erstellt, sofern noch nicht vorhanden, einen neuen Authentifizierungsdienst an dem angegebenen virtuellen Pfad. Die Standardauthentifizierungsmethode mit Benutzernamen und Kennwort ist aktiviert.

```
# Ermitteln, ob der Authentifizierungsdienst an dem angegebenen virtuellen Pfad vorhanden ist

$authentication = Get-STFAuthenticationService -VirtualPath $authenticationVirtualPath

if(-not $authentication)
```



```
{
  # Authentifizierungsdienst hinzufügen, IIS-Pfad des Stores durch Auth angehängt
   $authentication = Add-STFAuthenticationService $authenticationVirtualPath
}
else
{
  Write-Output "Ein Authentifizierungsdienst ist an dem angegebenen Pfad bereits vorhanden und wird verwendet."
}
```

- Erstellt, sofern noch nicht vorhanden, einen neuen Authentifizierungsdienst an dem angegebenen virtuellen Pfad. Die Standardauthentifizierungsmethode mit Benutzernamen und Kennwort ist aktiviert.

```
# Ermitteln, ob der Authentifizierungsdienst an dem angegebenen virtuellen Pfad vorhanden ist
$authentication = Get-STFAuthenticationService -VirtualPath $authenticationVirtualPath
if(-not $authentication)
{
  # Authentifizierungsdienst hinzufügen, IIS-Pfad des Stores durch Auth angehängt
   $authentication = Add-STFAuthenticationService $authenticationVirtualPath
}
else
{
  Write-Output "Ein Authentifizierungsdienst ist an dem angegebenen Pfad bereits vorhanden und wird verwendet."
}
```

- Erstellt einen neuen Storedienst mit einem XenDesktop-Controller und mit im Array **$XenDesktopServers** definierten Servern an dem angegebenen Pfad, sofern noch nicht vorhanden.

```
# Ermitteln, ob der Store-Dienst an dem angegebenen virtuellen Pfad vorhanden ist
$store = Get-STFStoreService -VirtualPath $StoreVirtualPath
if(-not $store)
{
# Store hinzufügen, der den zur Veröffentlichung der von den Servern zur Verfügung gestellten Ressourcen neu
```



```
konfigurierten Authentifizierungsdienst verwendet

$store = Add-STFStoreService -VirtualPath $StoreVirtualPath -AuthenticationService $authentication -
FarmName $Farmtype -FarmType $Farmtype -Servers $FarmServers -LoadBalance $LoadbalanceServers `

    -Port $Port -SSLRelayPort $SSLRelayPort -TransportType $TransportType

}

else

{

  Write-Output "Ein Storedienst ist an dem angegebenen Pfad bereits vorhanden und wird verwendet. Farm und
Server werden an diesen Store angefügt."

  # Anzahl der im Store konfigurierten Farmen abrufen

  $farmCount = (Get-STFStoreFarmConfiguration $store).Farms.Count

 # Farm an Store mit eindeutigem Namen anhängen

   Add-STFStoreFarm -StoreService $store -FarmName "Controller$($farmCount + 1)" -FarmType $Farmtype -
Servers $FarmServers -LoadBalance $LoadbalanceServers -Port $Port `

    -SSLRelayPort $SSLRelayPort -TransportType $TransportType

}
```

- Fügt einen Citrix Receiver für Web-Dienst an dem angegebenen virtuellen Pfad ein für den Zugriff auf Anwendungen, die in dem oben erstellten Store veröffentlicht wurden.

```
# Ermitteln, ob der Receiver-Dienst an dem angegebenen virtuellen Pfad vorhanden ist

$receiver = Get-STFWebReceiverService -VirtualPath $receiverVirtualPath

if(-not $receiver)

{

  # Receiver für Web-Site hinzufügen, damit die Benutzer auf die im Store veröffentlichten Anwendungen und
Desktops zugreifen können

   $receiver = Add-STFWebReceiverService -VirtualPath $receiverVirtualPath -StoreService $store

}

else

{

  Write-Output "Ein Receiver für Web-Dienst ist an dem angegebenen Pfad bereits vorhanden und wird
verwendet.

}
```

- Aktiviert XenApp-Dienste für den Store, damit ältere Citrix Receiver-Clients eine Verbindung mit veröffentlichten Anwendungen herstellen können.

```
# Ermitteln, ob PNA für den Store-Dienst konfiguriert ist

$storePnaSettings = Get-STFStorePna -StoreService $store

if(-not $storePnaSettings.PnaEnabled)

{

  # XenApp Services für den Store aktivieren und als Standard für den Server festlegen

  Enable-STFStorePna -StoreService $store -AllowUserPasswordChange -DefaultPnaService

}
```

Beispiel: Erstellen einer Remotezugriffbereitstellung

Das folgende, auf dem vorherigen Skript aufbauende Beispiel dient zum Erstellen einer Bereitstellung mit Remotezugriff.

Bevor Sie beginnen, führen Sie die in Erste Schritte mit dem SDK aufgeführten Schritte aus. Das Beispiel kann unter Verwendung der beschriebenen Methoden zur Erstellung eines Skripts für die Automatisierung der StoreFront-Bereitstellung angepasst werden.

Hinweis: Um sicherzustellen, dass Sie immer die aktuellen Verbesserungen und Fixes erhalten, empfiehlt Citrix, dass Sie den in diesem Dokument beschriebenen Schritten folgen, anstatt das Beispielskript zu kopieren und einzufügen.

Inhalt des Skripts

In diesem Abschnitt wird die Funktion jedes Teils des Skripts erläutert, das StoreFront erstellt. Dies hilft Ihnen bei der Anpassung des eigenen Skripts.

- Legt Fehlerbehandlungsanforderungen fest und importiert die erforderlichen StoreFront-Module. Importe sind in neueren Versionen von PowerShell nicht erforderlich.

```
Param(

  [Parameter(Mandatory=$true)]

  [Uri]$HostbaseUrl,

  [Parameter(Mandatory=$true)]

  [long]$SiteId = 1,

  [string]$Farmtype = "XenDesktop",

  [Parameter(Mandatory=$true)]

  [string[]]$FarmServers,

  [string]$StoreVirtualPath = "/Citrix/Store",

  [bool]$LoadbalanceServers = $false,
```



```
    [int]$Port = 80,
    [int]$SSLRelayPort = 443,
    [ValidateSet("HTTP","HTTPS","SSL")]
    [string]$TransportType = "HTTP",
    [Parameter(Mandatory=$true)]
    [Uri]$GatewayUrl,
    [Parameter(Mandatory=$true)]
    [Uri]$GatewayCallbackUrl,
    [Parameter(Mandatory=$true)]
    [string[]]$GatewaySTAUrls,
    [string]$GatewaySubnetIP,
    [Parameter(Mandatory=$true)]
    [string]$GatewayName
)
Set-StrictMode -Version 2.0

# Jeder Fehler ist ein Fehler mit Beenden als Folge.
$ErrorActionPreference = 'Stop'
$ReportErrorShowStackTrace = $true
$ReportErrorShowInnerException = $true
# Importieren der StoreFront-Module. Erforderlich für PowerShell-Versionen vor 3.0, die automatisches Laden nicht unterstützen
Import-Module Citrix.StoreFront
Import-Module Citrix.StoreFront.Stores
Import-Module Citrix.StoreFront.Roaming
```

- Erstellt eine StoreFront-Bereitstellung mit internem Zugriff unter Aufruf des vorherigen Beispielskripts. Die Basisbereitstellung wird um Unterstützung des Remotezugriffs erweitert.

```
# Einfache Bereitstellung durch Aufrufen des SimpleDeployment-Beispiels erstellen
$scriptDirectory = Split-Path -Path $MyInvocation.MyCommand.Definition -Parent
```



```
$scriptPath = Join-Path $scriptDirectory "RemoteAccessDeployment.ps1"

& $scriptPath -HostbaseUrl $HostbaseUrl -SiteId $SiteId -FarmServers $FarmServers -StoreVirtualPath
$StoreVirtualPath -Farmtype $Farmtype `

  -LoadbalanceServers $LoadbalanceServers -Port $Port  -SSLRelayPort $SSLRelayPort -TransportType
$TransportType
```

- Ruft die für die einfache Bereitstellung erstellten Dienste ab, da sie für die Unterstützung des Remotezugriffs aktualisiert werden müssen.

```
# Ermitteln der Authentifizierungs- und Receiver-Sites basierend auf dem Store

$store = Get-STFStoreService -VirtualPath $StoreVirtualPath

$authentication = Get-STFAuthenticationService -StoreService $store

$receiverForWeb = Get-STFWebReceiverService -StoreService $store
```

- Aktiviert CitrixAGBasic in dem für Remotezugriff mit NetScaler Gateway erforderlichen Citrix Receiver für Web-Dienst.Ruft die Citrix Receiver für Web CitrixAGBasic- und die ExplicitForms-Authentifizierungsmethode von den unterstützten Protokollen ab.

```
# Ruft die Citrix Receiver für Web CitrixAGBasic- und die ExplicitForms-Authentifizierungsmethode von den
unterstützten Protokollen ab

# Wird zum Zweck der Veranschaulichung angeführt, da der Protokollname, sofern bekannt, direkt verwendet werden
kann

$receiverMethods = Get-STFWebReceiverAuthenticationMethodsAvailable | Where-Object { $_ -match "Explicit" -or
$_ -match "CitrixAG" }

# CitrixAGBasic in Receiver für Web aktivieren (für Remotezugriff erforderlich)

Set-STFWebReceiverService $receiverForWeb -AuthenticationMethods $receiverMethods
```

- Aktiviert CitrixAGBasic für den Authentifizierungsdienst. Dies ist für den Remotezugriff erforderlich.

```
# CitrixAGBasic-Authentifizierungsmethode aus den installierten Protokollen abrufen

# Wird zum Zweck der Veranschaulichung angeführt, da der Protokollname, sofern bekannt, direkt verwendet werden
kann

$citrixAGBasic = Get-STFAuthenticationProtocolsAvailable | Where-Object { $_ -match "CitrixAGBasic" }

# CitrixAGBasic im Authentifizierungsdienst aktivieren (erforderlich für Remotezugriff)

Enable-STFAuthenticationServiceProtocol -AuthenticationService $authentication -Name $citrixAGBasic
```

- Fügt ein neues Remotezugriffsgateway hinzu sowie die optionale Subnetz-IP-Adresse, falls diese angegeben wird, und registriert es bei dem Store für den Remotezugriff.

```
# Neues Gateway für den Remotezugriff auf den neuen Store hinzufügen
```

```
Add-STFRoamingGateway -Name "NetScaler10x" -LogonType Domain -Version Version10_0_69_4 -GatewayUrl
$GatewayUrl '

-CallbackUrl $GatewayCallbackUrl -SecureTicketAuthorityUrls $GatewaySTAUrls

# Neues Gateway aus der Konfiguration abrufen (Add-STFRoamingGateway gibt das neue Gateway zurück, wenn der
Parameter "-PassThru" angegeben wird)

$gateway = Get-STFRoamingGateway -Name $GatewayName

# Wurde das Gatewaysubnetz angegeben, legen Sie es für das Gatewayobjekt fest

if($GatewaySubnetIP)

{

   Set-STFRoamingGateway -Gateway $gateway -SubnetIPAddress $GatewaySubnetIP

}

# Gateway bei dem neuen Store registrieren

Register-STFStoreGateway -Gateway $gateway -StoreService $store -DefaultGateway
```

Beispiel: Erstellen einer Remotezugriffbereitstellung mit Gateway für den optimalen Start

Das folgende, auf dem vorherigen Skript aufbauende Beispiel dient zum Erstellen einer Bereitstellung mit Remotezugriff und Gateway für den optimalen Start.

Bevor Sie beginnen, stellen Sie sicher, dass Sie die in Erste Schritte mit dem SDK aufgeführten Schritte ausführen. Das Beispiel kann unter Verwendung der beschriebenen Methoden zur Erstellung eines Skripts für die Automatisierung der StoreFront-Bereitstellung angepasst werden.

Hinweis: Um sicherzustellen, dass Sie immer die aktuellen Verbesserungen und Fixes erhalten, empfiehlt Citrix, dass Sie den in diesem Dokument beschriebenen Schritten folgen, anstatt das Beispielskript zu kopieren und einzufügen.

Inhalt des Skripts

In diesem Abschnitt wird die Funktion jedes Teils des Skripts erläutert, das StoreFront erstellt. Dies hilft Ihnen bei der Anpassung des eigenen Skripts.

- Legt Fehlerbehandlungsanforderungen fest und importiert die erforderlichen StoreFront-Module. Importe sind in neueren Versionen von PowerShell nicht erforderlich.

```
Param(

   [Parameter(Mandatory=$true)]

   [Uri]$HostbaseUrl,

   [long]$SiteId = 1,

   [string]$Farmtype = "XenDesktop",

   [Parameter(Mandatory=$true)]
```



```
    [string[]]$FarmServers,
    [string]$StoreVirtualPath = "/Citrix/Store",
    [bool]$LoadbalanceServers = $false,
    [int]$Port = 80,
    [int]$SSLRelayPort = 443,
    [ValidateSet("HTTP","HTTPS","SSL")]
    [string]$TransportType = "HTTP",
    [Parameter(Mandatory=$true)]
    [Uri]$GatewayUrl,
    [Parameter(Mandatory=$true)]
    [Uri]$GatewayCallbackUrl,
    [Parameter(Mandatory=$true)]
    [string[]]$GatewaySTAUrls,
    [string]$GatewaySubnetIP,
    [Parameter(Mandatory=$true)]
    [string]$GatewayName,
    [Parameter(Mandatory=$true)]
    [Uri]$OptimalGatewayUrl,
    [Parameter(Mandatory=$true)]
    [string[]]$OptimalGatewaySTAUrls,
    [Parameter(Mandatory=$true)]
    [string]$OptimalGatewayName
)
Set-StrictMode -Version 2.0
# Jeder Fehler ist ein Fehler mit Beenden als Folge.
$ErrorActionPreference = 'Stop'
$ReportErrorShowStackTrace = $true
$ReportErrorShowInnerException = $true
```

```
# Importieren der StoreFront-Module. Erforderlich für PowerShell-Versionen vor 3.0, die automatisches Laden nicht unterstützen

Import-Module Citrix.StoreFront

Import-Module Citrix.StoreFront.Stores

Import-Module Citrix.StoreFront.Roaming
```

- Ruft das Skript zur Erstellung einer Remotezugriffbereitstellung zum Konfigurieren der einfachen Bereitstellung mit Remotezugriff auf.

```
# Erstellen einer Remotezugriffbereitstellung

$scriptDirectory = Split-Path -Path $MyInvocation.MyCommand.Definition -Parent

$scriptPath = Join-Path $scriptDirectory "RemoteAccessDeployment.ps1"

& $scriptPath -HostbaseUrl $HostbaseUrl -SiteId $SiteId -FarmServers $FarmServers -StoreVirtualPath $StoreVirtualPath -Farmtype $Farmtype `

  -LoadbalanceServers $LoadbalanceServers -Port $Port  -SSLRelayPort $SSLRelayPort -TransportType $TransportType `

  -GatewayUrl $GatewayUrl -GatewayCallbackUrl $GatewayCallbackUrl -GatewaySTAUrls $GatewaySTAUrls -GatewayName $GatewayName
```

- Fügt das bevorzugte Gateway für den optimalen Start hinzu und ruft es aus der Liste der konfigurierten Gateways ab.

```
# Neues Gateway für den HDX-Remotezugriff auf Desktops und Apps hinzufügen

$gateway = Add-STFRoamingGateway -Name $OptimalGatewayName -LogonType UsedForHDXOnly -GatewayUrl $OptimalGatewayUrl -SecureTicketAuthorityUrls $OptimalGatewaySTAUrls -PassThru
```

- Bewirkt, dass der Storedienst das optimale Gateway verwendet und es für Startvorgänge aus der angegebenen Farm registriert.

```
# Durch SimpleDeployment.ps1 konfigurierten Store abrufen

$store = Get-STFStoreService -VirtualPath $StoreVirtualPath

# Gateway bei dem neuen Store für den Start in allen Farmen (derzeit nur eine) registrieren

$farmNames = @($store.FarmsConfiguration.Farms | foreach { $_.FarmName })

Register-STFStoreOptimalLaunchGateway -Gateway $gateway -StoreService $store -FarmName $farmNames
```

Beispiel: Erstellen einer Bereitstellung mit Desktopgerätesite

Das folgende, auf dem Skript zum Erstellen einer einfachen Bereitstellung aufbauende Beispiel dient zum Hinzufügen einer Bereitstellung mit Desktopgerätesite.

Bevor Sie beginnen, stellen Sie sicher, dass Sie die in Erste Schritte mit dem SDK aufgeführten Schritte ausführen. Das Beispiel kann unter Verwendung der beschriebenen Methoden zur Erstellung eines Skripts für die Automatisierung der

StoreFront-Bereitstellung angepasst werden.

Hinweis: Um sicherzustellen, dass Sie immer die aktuellen Verbesserungen und Fixes erhalten, empfiehlt Citrix, dass Sie den in diesem Dokument beschriebenen Schritten folgen, anstatt das Beispielskript zu kopieren und einzufügen.

Inhalt des Skripts

In diesem Abschnitt wird die Funktion jedes Teils des Skripts erläutert, das StoreFront erstellt. Dies hilft Ihnen bei der Anpassung des eigenen Skripts.

- Legt Fehlerbehandlungsanforderungen fest und importiert die erforderlichen StoreFront-Module. Importe sind in neueren Versionen von PowerShell nicht erforderlich.

```
Param(
  [Parameter(Mandatory=$true)]
  [Uri]$HostbaseUrl,
  [long]$SiteId = 1,
  [string]$Farmtype = "XenDesktop",
  [Parameter(Mandatory=$true)]
  [string[]]$FarmServers,
  [string]$StoreVirtualPath = "/Citrix/Store",
  [bool]$LoadbalanceServers = $false,
  [int]$Port = 80,
  [int]$SSLRelayPort = 443,
  [ValidateSet("HTTP","HTTPS","SSL")]
  [string]$TransportType = "HTTP",
  [Parameter(Mandatory=$true)]
  [Uri]$GatewayUrl,
  [Parameter(Mandatory=$true)]
  [Uri]$GatewayCallbackUrl,
  [Parameter(Mandatory=$true)]
  [string[]]$GatewaySTAUrls,
  [string]$GatewaySubnetIP,
  [Parameter(Mandatory=$true)]
  [string]$GatewayName,
```

```
    [Parameter(Mandatory=$true)]
    [Uri]$OptimalGatewayUrl,
    [Parameter(Mandatory=$true)]
    [string[]]$OptimalGatewaySTAUrls,
    [Parameter(Mandatory=$true)]
    [string]$OptimalGatewayName
)
Set-StrictMode -Version 2.0
# Jeder Fehler ist ein Fehler mit Beenden als Folge.
$ErrorActionPreference = 'Stop'
$ReportErrorShowStackTrace = $true
$ReportErrorShowInnerException = $true
# Importieren der StoreFront-Module. Erforderlich für PowerShell-Versionen vor 3.0, die automatisches Laden nicht unterstützen
Import-Module Citrix.StoreFront
Import-Module Citrix.StoreFront.Stores
Import-Module Citrix.StoreFront.Roaming
```

- Automatisiert einen Desktopgerätepfad auf der Basis des $StoreVirtualPath-Pfads.

```
$desktopApplianceVirtualPath = "$($StoreIISPath.TrimEnd('/'))Appliance"
```

- Ruft das einfache Bereitstellungsskript zum Einrichten der Standardbereitstellung mit den grundlegenden Diensten auf.

```
# Erstellen einer Remotezugriffbereitstellung
$scriptDirectory = Split-Path -Path $MyInvocation.MyCommand.Definition -Parent
$scriptPath = Join-Path $scriptDirectory "RemoteAccessDeployment.ps1"
& $scriptPath -HostbaseUrl $HostbaseUrl -SiteId $SiteId -FarmServers $FarmServers -StoreVirtualPath $StoreVirtualPath -Farmtype $Farmtype `
  -LoadbalanceServers $LoadbalanceServers -Port $Port  -SSLRelayPort $SSLRelayPort -TransportType $TransportType `
  -GatewayUrl $GatewayUrl -GatewayCallbackUrl $GatewayCallbackUrl -GatewaySTAUrls $GatewaySTAUrls -GatewayName $GatewayName
```

- Bewirkt, dass der Storedienst die Desktopgerätesite verwendet. Verwenden Sie das Cmdlet **Add-**

STFDesktopApplianceService, um die neue Multidesktop-Site mit expliziter Authentifizierung über Benutzernamen und Kennwort hinzuzufügen.

```
$store = Get-STFStoreService -VirtualPath $StoreVirtualPath

# Neue Desktopgerätesite mit den von dem Storedienst veröffentlichten Desktops erstellen

Add-STFDesktopApplianceService -VirtualPath $desktopApplianceVirtualPath -StoreService $store -EnableExplicit
```

Beispiel: Austausch von Metadaten zwischen Identitäts- und Dienstanbieter (StoreFront) für die SAML-Authentifizierung

Die SAML-Authentifizierung kann in der StoreFront-Verwaltungskonsole konfiguriert werden (siehe Konfigurieren des Authentifizierungsdiensts). Alternativ können folgende PowerShell-Cmdlets verwendet werden: Export-STFSamlEncryptionCertificate, Export-STFSamlSigningCertificate Import-STFSamlEncryptionCertificate, Import-STFSamlSigningCertificate New-STFSamlEncryptionCertificate, New-STFSamlIdPCertificate New-STFSamlSigningCertificate.

Sie können Sie das Cmdlet **Update STFSamlIdPFromMetadata** verwenden, wenn Metadaten (IDs, Zertifikate, Endpunkte und andere Konfigurationselemente) zwischen Identitäts- und Dienstanbieter, in diesem Fall StoreFront, ausgetauscht werden sollen.

Metadatenendpunkt für einen StoreFront-Store namens "Store" mit dediziertem Authentifizierungsdienst:

https:///Citrix/StoreAuth/SamlForms/ServiceProvider/Metadata

Wenn Ihr Identitätsanbieter den Metadatenimport unterstützt, können Sie ihn an die oben aufgeführte URL verweisen. **Hinweis**: Dies muss über HTTPS erfolgen.

Damit StoreFront Metadaten eines Identitätsanbieters nutzen kann, kann das folgende PowerShell-Skript verwendet werden:

Befehl KOPIEREN

```
Get-Module "Citrix.StoreFront*" -ListAvailable | Import-Module



# Remember to change this with the virtual path of your Store.

$StoreVirtualPath = "/Citrix/Store"



$store = Get-STFStoreService -VirtualPath $StoreVirtualPath

$auth = Get-STFAuthenticationService -StoreService $store



# To read the metadata directly from the Identity Provider, use the following:

# Note again this is only allowed for https endpoints

Update-STFSamlIdPFromMetadata -AuthenticationService $auth -Url https://example.com/FederationMetadata/2007-06/FederationMeta



# If the metadata has already been download, use the following:

# Note: Ensure that the file is encoded as UTF-8

Update-STFSamlIdPFromMetadata -AuthenticationService $auth -FilePath "C:\Users\exampleusername\Downloads\FederationMetadata
```

Beispiel: Auflisten der Metadaten und ACS-Endpunkte für einen bestimmten Store für die SAML-Authentifizierung

Mit dem folgenden Skript können Sie die Metadaten und ACS-Endpunkte (Assertion Consumer Service) für einen bestimmten Store auflisten.

Befehl KOPIEREN

```
# Change this value for your Store

$storeVirtualPath = "/Citrix/Store"



$auth = Get-STFAuthenticationService -Store (Get-STFStoreService -VirtualPath $storeVirtualPath)

$spId = $auth.AuthenticationSettings["samlForms"].SamlSettings.ServiceProvider.Uri.AbsoluteUri

$acs = New-Object System.Uri $auth.Routing.HostbaseUrl, ($auth.VirtualPath + "/SamlForms/AssertionConsumerService")

$md = New-Object System.Uri $auth.Routing.HostbaseUrl, ($auth.VirtualPath + "/SamlForms/ServiceProvider/Metadata")

$samlTest = New-Object System.Uri $auth.Routing.HostbaseUrl, ($auth.VirtualPath + "/SamlTest")

Write-Host "SAML Service Provider information:

Service Provider ID: $spId

Assertion Consumer Service: $acs

Metadata: $md

Test Page: $samlTest"
```

Beispiel für die Ausgabe

Befehl KOPIEREN

SAML Service Provider information:

Service Provider ID: https://storefront.example.com/Citrix/StoreAuth

Assertion Consumer Service: https://storefront.example.com/Citrix/StoreAuth/SamlForms/AssertionConsumerService

Metadata: https://storefront.example.com/Citrix/StoreAuth/SamlForms/ServiceProvider/Metadata

Test Page: https://storefront.example.com/Citrix/StoreAuth/SamlTest

Problembehandlung bei StoreFront

Nov 27, 2017

Bei der Installation oder Deinstallation von StoreFront werden vom StoreFront-Installationsprogramm die folgenden Protokolldateien unter C:\Windows\Temp\ erstellt. Die Dateinamen lassen die Komponenten erkennen, die sie erstellt haben, und enthalten einen Zeitstempel.

- Citrix-DeliveryServicesRoleManager-*.log: wird bei der interaktiven Installation von StoreFront erstellt.
- Citrix-DeliveryServicesSetupConsole-*.log: wird bei der Installation von StoreFront ohne Benutzereingriffe und bei Deinstallation mit oder ohne Benutzereingriffe erstellt.
- CitrixMsi-CitrixStoreFront-x64-*.log: wird bei der Installation und Deinstallation von StoreFront mit oder ohne Benutzereingriffe erstellt.

StoreFront unterstützt die Windows-Ereignisprotokollierung für den Authentifizierungsdienst, Stores und Receiver für Web-Sites. Alle generierten Ereignisse werden in das StoreFront-Anwendungsprotokoll geschrieben, das über die Ereignisanzeige unter Anwendungs- und Dienstprotokolle > Citrix Delivery Services oder Windows-Protokolle > Anwendung angezeigt werden kann. Sie können die Anzahl der doppelten Protokolleinträge für ein einzelnes Ereignis steuern, indem Sie die Konfigurationsdateien für den Authentifizierungsdienst, die Stores und Receiver für Web-Sites bearbeiten.

Die Citrix StoreFront-Verwaltungskonsole speichert automatisch Ablaufverfolgungsinformationen. Standardmäßig ist die Ablaufverfolgung für andere Vorgänge deaktiviert und muss manuell aktiviert werden. Von Windows PowerShell-Befehlen erstellte Protokolle werden im Verzeichnis \Admin\logs\ der StoreFront-Installation, die normalerweise in C:\Programme\Citrix\Receiver StoreFront\ ist, gespeichert. Die Protokolldateinamen enthalten Befehlsaktionen und Themen sowie einen Zeitstempel, anhand derer zwischen den Befehlssequenzen unterschieden werden kann.

Wichtig: Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Wenn Sie die Änderungen vorgenommen haben, übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden.

Konfigurieren der Protokolldrosselung

1. Öffnen Sie die Datei web.config für den Authentifizierungsdienst, Store oder die Receiver für Web-Site mit einem Text-Editor. Die Dateien sind normalerweise im Verzeichnis C:\inetpub\wwwroot\Citrix\Authentication\, C:\inetpub\wwwroot\Citrix\storename\, und C:\inetpub\wwwroot\Citrix\storenameWeb\, wobei storename für den Namen steht, der beim Erstellen des Stores angegeben wurde.
2. Suchen Sie das folgende Element in der Datei.
   Standardmäßig wird in der Konfiguration von StoreFront die Anzahl der doppelten Protokolleinträge auf 10 pro Minute beschränkt.

3. Ändern Sie den Wert des Attributs duplicateInterval , um den Zeitraum, in dem doppelte Protokolleinträge überwacht werden, in Stunden, Minuten und Sekunden festzulegen. Legen Sie mit dem Attribut duplicateLimit fest, wie viele doppelte Einträge im angegebenen Zeitraum protokolliert werden müssen, um die Protokolldrosselung auszulösen.

Wenn die Protokolldrosselung ausgelöst wird, wird eine Warnmeldung aufgezeichnet, um anzugeben, dass weitere identische Protokolleinträge unterdrückt werden. Nach Ablauf des Zeitraums wird die normale Protokollierung fortgesetzt und es wird eine Informationsmeldung aufgezeichnet, die angibt, dass doppelte Protokolleinträge nicht mehr unterdrückt werden.

Aktivieren der Ablaufverfolgung

Achtung: Die StoreFront- und PowerShell-Konsolen können nicht gleichzeitig geöffnet sein. Schließen Sie immer zuerst die StoreFront-Verwaltungskonsole, bevor Sie die PowerShell-Konsole zum Verwalten der StoreFront-Konfiguration öffnen. Schließen Sie ebenso immer alle Instanzen von PowerShell, bevor Sie die StoreFront-Konsole öffnen.

1. Starten Sie Windows PowerShell von einem Konto mit lokalen Administratorrechten und geben Sie an der Eingabeaufforderung die folgenden Befehle ein. Starten Sie den Server neu, damit die Ablaufverfolgung aktiviert wird.
   Add-PSSnapin Citrix.DeliveryServices.Framework.Commands

   Set-DSTraceLevel -All -TraceLevel Verbose
   Zulässige Werte für - TraceLevel sind, in zunehmender Detailtiefe der Ablaufverfolgung: Off, Error, Warning, Info, Verbose. StoreFront zeichnet automatisch Fehlermeldungen für die Ablaufverfolgung auf. Aufgrund der großen Datenmenge, die möglicherweise erstellt wird, kann die Ablaufverfolgung erhebliche Auswirkungen auf die StoreFront-Leistung haben. Es empfiehlt sich daher, Info und Verbose nur zu verwenden, wenn es ausdrücklich für die Problembehandlung erforderlich ist.

   Optionale Argumente für das Set-DSTraceLevel-Cmdlet:
   -FileCount: gibt die Zahl der Ablaufverfolgungsdateien an (Standardwert = 3)
   -FileSizeKb: gibt die maximale Größe der einzelnen Ablaufverfolgungsdateien an (Standardwert = 1000)
   -ConfigFile : Alternative zu "-All", die zum Aktualisieren einer spezifischen Konfigurationsdatei anstelle aller Konfigurationsdateien dient. Wird als Wert für "-ConfigFile" beispielsweise "c:\inetpub\wwwroot\Citrix\\web.config" angegeben, wird die Ablaufverfolgung für den Store namens "" festgelegt.

2. Um die Ablaufverfolgung zu deaktivieren, geben Sie folgende Befehle ein und starten den Server neu.
   Add-PSSnapin Citrix.DeliveryServices.Framework.Commands

   Set-DSTraceLevel -All -TraceLevel Off

Ist die Ablaufverfolgung aktiviert, werden die Ablaufverfolgungsinformationen in das Verzeichnis \Admin\Trace\ der StoreFront-Installation unter C:\Programme\Citrix\Receiver StoreFront\ geschrieben.