CITRIX

StoreFront 1912

Contents

StoreFront 1912

January 30, 2020

StoreFront 1912 ist das aktuelle Release von StoreFront. Diese Dokumentation spiegelt die Funktionen und Konfigurationen in dem neuesten Releases wider.

StoreFront ist ein Unternehmensappstore, der Anwendungen und Desktops von Citrix Virtual Apps and Desktops-Sites in einem einzigen benutzerfreundlichen Store für Benutzer zusammenfasst. StoreFront ist eine integrierte Komponente von Citrix Virtual Apps and Desktops, die in Kombination mit mehreren Versionen von Virtual Apps and Desktops verwendet werden kann.

Die Benutzer können mit der Citrix Workspace-App oder unterstützten Versionen von Citrix Receiver auf StoreFront-Stores zugreifen. Unterscheidet sich eine bestimmte Version oder bezieht sich der Text der Benutzeroberfläche auf beides, wird dies angegeben. Andernfalls ist in der Dokumentation von der "Citrix Workspace-App" die Rede.

Frühere Releases

Dokumentation älterer Releases:

- StoreFront 1909
- StoreFront 1906
- StoreFront 1903
- StoreFront 1811
- StoreFront 3.16
- StoreFront 3.12
- StoreFront 3.0
- Frühere StoreFront-Versionen

Informationen zur Produktlebenszyklusstrategie für aktuelle Releases (CR) und Long Term Service Releases (LTSR) von Citrix Virtual Apps and Desktops finden Sie unter Lifecycle Milestones. Zusätzliche Lebenszyklusinformationen für StoreFront finden Sie in CTX200356.

> **Hinweis:**
>
> Upgrades auf das aktuelle Release von StoreFront von früheren nicht unterstützten Versionen werden nicht unterstützt. Wenn Sie aktuelle Versionen verwenden, müssen Sie sicherstellen, dass Sie jederzeit auf einer unterstützten StoreFront-Version sind.

Neue Features

January 30, 2020

StoreFront 1912

StoreFront 1912 enthält die folgenden neuen Features. Informationen zu Fehlerkorrekturen finden Sie unter Behobene Probleme.

StoreFront Protocol Handler-Unterstützung umfasst jetzt Chrome-Geräte mit Workspace-App für Android

Wenn Benutzer von Chrome-Geräten mit installierter Citrix Workspace-App für Android (1912 oder höher) eine Citrix Receiver für Web-Site öffnen, werden im Browser beim Start automatisch ICA-Dateien unter Einsatz der Citrix Workspace-App für Android geöffnet.

Der Workflow zur Clienterkennung für Android, der prüft, ob die Citrix Workspace-App für Android installiert ist, ist jetzt mit dem für Windows- und Macintosh-Clients identisch, wenn der Chrome-Browser auf Chrome-Geräten verwendet wird. In früheren Versionen mussten die Benutzer von Chrome-Geräten zunächst eine heruntergeladene ICA-Datei manuell öffnen.

Unterstützung von App-Schutzrichtlinien

StoreFront 1912 unterstützt App-Schutzrichtlinien zur Erhöhung der Sicherheit, wenn andere Citrix Komponenten wie die Citrix Workspace-App und Delivery Controller von Citrix Virtual Apps and Desktops die App-Schutzfunktion ebenfalls unterstützen. App-Schutzrichtlinien werden auf Bereitstellungsgruppenebene festgelegt, und Citrix Virtual Apps and Desktops bestimmt, ob App-Schutzrichtlinien verwendet werden. Sie müssen die App-Schutzfunktion manuell in StoreFront aktivieren. Wenn StoreFront Anforderungen mit dem HTTP-Header “X-Citrix-AppProtection-Capable” von einer Citrix Workspace-App empfängt, die App-Schutzrichtlinien unterstützt, sendet StoreFront automatisch ein SmartAccess-Tag an Citrix Virtual Apps and Desktops, das angibt, dass es App-Schutzrichtlinien unterstützt. Informationen zum Konfigurieren von Bereitstellungsgruppen mit App-Schutzrichtlinien finden Sie unter App-Schutz.

Um den App-Schutz auf einem StoreFront-Server zu aktivieren, führen Sie den folgenden PowerShell-Befehl auf dem StoreFront-Server aus: `Add-STFFeatureState -Name ”Citrix.StoreFront.AppProtectionPolicy.Control”-IsEnabled $True`. (In einer StoreFront Bereitstellung mit mehreren Servern müssen Sie diese Änderungen manuell auf alle anderen Server in der Servergruppe übertragen. Siehe Weitergeben lokaler Änderungen an eine Servergruppe.)

Um zu überprüfen, ob das Feature auf einem StoreFront-Server aktiviert ist, verwenden Sie den folgenden PowerShell Befehl:
`Get-STFFeatureState -Name "Citrix.StoreFront.AppProtectionPolicy.Control`.

Desktopgerätesites nicht mehr unterstützt

Die StoreFront-Unterstützung für den Zugriff von Benutzern auf Desktops auf Desktopgerätesites wurde in Citrix Virtual Apps and Desktops 7 1811 als veraltet angekündigt. In dieser Version werden Desktopgerätesites nicht mehr unterstützt und Citrix empfiehlt, die Citrix Workspace-App Desktop Lock für alle Anwendungsfälle ohne Domänenbindung zu verwenden.

> **Warnung:**
>
> Wenn Sie ein Upgrade auf StoreFront 1912 ausführen, werden alle Desktopgerätesites in der Bereitstellung automatisch entfernt. Siehe Aktualisieren von StoreFront.

StoreFront PowerShell SDK

Das StoreFront-PowerShell-SDK wurde als Version 1912 neu veröffentlicht. Sie können mit PowerShell keine Desktopgerätesites mehr erstellen oder verwalten.

Behobene Probleme

January 6, 2020

Die folgenden Probleme wurden seit Version 1909 behoben:

- On-Premises-StoreFront kann kein Startgateway für Weblinks in MMC hinzufügen. [WSP-4368]
- LCM-6351: Alte Registrierungsschlüssel von CitrixPrivilegedService_x64.msi wurden nach dem Upgrade von DDC nicht entfernt. [WSP-4785]
- VMware VMTools v10.3.x sind auf Ihrem StoreFront-Server installiert: Wenn Sie versuchen, StoreFront mit dem Metainstaller von Citrix Virtual Apps and Desktops 7 1906 auf Version 1906 zu aktualisieren, schlägt das Upgrade fehl. StoreFront wird erfolgreich mit dem eigenständigen StoreFront 1906-Installer aktualisiert. StoreFront 1906 wird jedoch nicht der Windows-Liste "Software hinzufügen/entfernen" hinzugefügt. [WSP-4895]
- Die Anpassung zum Abschneiden langer App-Namen funktioniert in der X1.1 Purple UI nicht mehr. [WSP-4899]

- Upgrades, die 2.6, 3.0.1, 3.5, 3.8 in ihrem Upgradeverlauf auf 3.12 CU* und höher enthalten, können fehlschlagen, wenn der KCD-Dienst den Status “Angehalten” hat. [WSP-5160]
- Aktualisieren Sie `http://downloadplugins.citrix.com`, um Citrix Workspace-App statt Citrix Receiver-Versionen bereitzustellen, die am Ende der Lebensdauer sind. [WSP-5303]

Bekannte Probleme

January 6, 2020

In diesem Release bestehen die folgenden Probleme.

- Die Abonnementübertragung zwischen Mitgliedern einer StoreFront-Servergruppe schlägt fehl, wenn TLS 1.0 in Windows deaktiviert ist und Windows Server .NET 4.5 Framework Server verwendet. Standardmäßig verwendet .NET 4.5 Framework nur TLS 1.0. Ein Workaround für dieses Problem ist das Aktualisieren von .NET Framework auf dem Server auf Version 4.7 oder höher (die standardmäßig TLS 1.2 verwenden). [STF-2413]
- Es ist ein bekanntes Drittanbieterproblem mit Smartcardauthentifizierung und Microsoft Edge. Zur Problemvermeidung verwenden Sie Internet Explorer. [DNA-47809]
- 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]
- Wenn StoreFront unter Windows Server 2012 R2 installiert wird, kann es sich möglicherweise nicht beim Citrix Analytics-Dienst registrieren. Dies ist der Fall, wenn die C++-Laufzeit-Softwarekomponenten noch nicht installiert sind. Das eigenständige StoreFront-Installationsprogramm installiert diese Komponenten nicht. Ein einfacher Workaround besteht darin, die C ++ Laufzeit vor oder nach der Installation von StoreFront zu installieren. [WSP-4412]

Hinweise zu Drittanbietern

January 6, 2020

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

StoreFront – Hinweise zu Drittanbietern (PDF-Download)

Systemanforderungen

April 1, 2020

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.

> **Hinweis:**
>
> Ein Upgrade auf die aktuelle Version von einer älteren Version, die jetzt das Ende des Lebenszyklus erreicht hat, wird nicht unterstützt. Weitere Informationen finden Sie unter CTX200356.

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

- Windows Server 2019 (Standard- und Datacenter-Editionen)
- Windows Server 2016 (Standard- und Datacenter-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. StoreFront-Servergruppen können maximal sechs Server enthalten. Allerdings bieten basierend auf Simulationen Servergruppen mit mehr als drei Servern für die Kapazität keinen Vorteil. Idealerweise sollten alle Server in einer Servergruppe an demselben Standort sein (Rechenzentrum, Availability Zone). Servergruppen können aber über Standorte innerhalb derselben Region verteilt sein, vorausgesetzt, dass Verbindungen zwischen Servern in der Gruppe diese Latenzkriterien erfüllen. Siehe Skalierbarkeit.

Bevor Sie StoreFront installieren können, müssen Windows PowerShell (Version 4.0 oder höher) und Microsoft Management Console (Version 3.0 oder höher) auf dem Webserver installiert sein. Beide sind Standardkomponenten von Windows Server.

Das StoreFront-Installationsprogramm prüft vor der Installation von StoreFront, ob die folgenden Voraussetzungen installiert und aktiviert sind. Standardmäßig werden diese Voraussetzungen vom Betriebssystem als Featurepakete bereitgestellt. Wenn das StoreFront-Installationsprogramm erkennt, dass eine dieser Voraussetzungen fehlt oder deaktiviert ist, werden sie automatisch installiert und aktiviert:

- Microsoft .NET Framework (Version 4.5.1 oder höher)

- Microsoft ASP.NET (Version 4.5 oder höher)
- Microsoft Visual C++ VC141 x64 Runtime
- Microsoft Internetinformationsdienste (IIS)

  IIS wird von der Webserverrolle “Windows Server” hinzugefügt. Die Version ist vom gewählten Betriebssystem abhängig. Zur Referenz: Das StoreFront-Installationsprogramm fügt die folgenden IIS-Rollen hinzu:

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

  Der relative Pfad zu StoreFront in IIS muss auf allen Servern in einer Servergruppe identisch sein.

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 daher 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.
- TCP-Port 8008 wird (wo aktiviert) von der Citrix Workspace-App für HTML5 oder unterstützten Versionen von Citrix Receiver bzw. der Citrix Workspace-App für die Kommunikation zwischen lokalen Benutzern im internen Netzwerk und den Servern verwendet, die die Desktops und Anwendungen bereitstellen.

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

Speichern von Abonnementdaten mit Microsoft SQL Server

Optional: Speichern von Abonnementdaten mit Microsoft SQL Server. StoreFront unterstützt hierfür dieselben Microsoft SQL Server-Versionen wie die Datenbanken von Citrix Virtual Apps and Desktops. Informationen zu den Systemanforderungen für Citrix Virtual Apps and Desktops finden Sie unter Datenbanken.

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.

- Citrix Virtual Apps and Desktops 7 1912 LTSR
- Citrix Virtual Apps and Desktops 7 1909
- Citrix Virtual Apps and Desktops 7 1906
- Citrix Virtual Apps and Desktops 7 1903
- Citrix Virtual Apps and Desktops 7 1811
- Citrix Virtual Apps and Desktops 7 1808
- XenApp und XenDesktop 7.15 LTSR *
- XenApp und XenDesktop 7.6 LTSR *

* Weitere Informationen zur Verwendung dieser aktuellen Version (CR) in einer LTSR-Umgebung (Long Term Service) und zu anderen häufig gestellten Fragen finden Sie unter Knowledge Center-Artikel.

Anforderungen für Citrix Gateway

Die folgenden Versionen von Citrix Gateway und NetScaler Gateway können verwendet werden, um Benutzern in öffentlichen Netzwerken Zugriff auf StoreFront zu geben.

- Citrix Gateway 13.0
- Citrix Gateway 12.1
- NetScaler Gateway 12.0
- NetScaler Gateway 11.1

Citrix Workspace-App für HTML5-Anforderungen

Um Benutzern den Zugriff auf Desktops und Anwendungen mit der Citrix Workspace-App für HTML5 auf Receiver für Web-Sites zu ermöglichen, gelten die folgenden zusätzlichen Anforderungen.

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

- Citrix Virtual Apps and Desktops 7 1912 LTSR
- Citrix Virtual Apps and Desktops 7 1909
- Citrix Virtual Apps and Desktops 7 1906
- Citrix Virtual Apps and Desktops 7 1903
- Citrix Virtual Apps and Desktops 7 1811
- Citrix Virtual Apps and Desktops 7 1808
- XenApp und XenDesktop 7.15 LTSR
- XenApp und XenDesktop 7.6 LTSR

> **Hinweis:**
>
> Die Citrix Workspace-App für HTML5 startet Desktops und Apps über interne Netzwerkverbindungen nur, wenn sichere Verbindungen zu den VDAs konfiguriert wurden, auf denen die Ressourcen gehostet werden. HTTP-Verbindungen mit VDAs, die die Apps und Desktops hosten, können nicht verwendet werden.

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

- Citrix Gateway 13.0
- Citrix Gateway 12.1
- NetScaler Gateway 12.0
- NetScaler Gateway 11.1

Bei Verbindungen über Citrix Gateway bietet Citrix Workspace-App für HTML5 den Zugriff auf Desktops und Anwendungen folgender Produkte.

- Citrix Virtual Apps and Desktops 7 1912 LTSR
- Citrix Virtual Apps and Desktops 7 1909
- Citrix Virtual Apps and Desktops 7 1906
- Citrix Virtual Apps and Desktops 7 1903
- Citrix Virtual Apps and Desktops 7 1811
- Citrix Virtual Apps and Desktops 7 1808
- XenApp und XenDesktop 7.15 LTSR
- XenApp und XenDesktop 7.6 LTSR

Anforderungen für Benutzergeräte

StoreFront bietet Benutzern verschiedene Optionen für den Zugriff auf Desktops und Anwendungen. Citrix Workspace-App-Benutzer können entweder über die Citrix Workspace-App auf Stores zugreifen

oder einen Webbrowser verwenden, um sich bei einer Citrix Receiver für Web-Site für den Store anzumelden. Benutzern, die die Citrix Workspace-App nicht installieren können, jedoch einen HTML5-kompatiblen Webbrowser haben, können Sie direkten Zugriff auf Desktops und Anwendungen im Webbrowser ermöglichen, indem Sie die Citrix Workspace-App für HTML5 für Ihre Citrix Receiver für Web-Site aktivieren.

Benutzer von 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.

Um Microsoft Application Virtualization (App-V)-Sequenzen für Benutzer bereitzustellen, benötigen Sie außerdem eine unterstützte Version von Microsoft Application Virtualization Desktop Client. Weitere Informationen finden Sie unter Verwalten von gestreamten Anwendungen. Benutzer können nicht über Citrix Receiver für Web-Sites auf Offlineanwendungen oder App-V-Sequenzen zugreifen.

Verwenden der Citrix Workspace-App für den Zugriff auf StoreFront-Stores

Sie können alle derzeit unterstützten Versionen der Citrix Workspace-App für den Zugriff auf StoreFront-Stores über interne Netzwerkverbindungen und über Citrix Gateway verwenden. Informationen zu Lebenszyklusterminen für Citrix Workspace-Apps und Citrix Receiver finden Sie unter https://www.citrix.com/support/product-lifecycle/milestones/receiver.html.

Sie können über Citrix Gateway mit dem Citrix Gateway-Plug-In, ICA-Proxy oder clientloses VPN (cVPN) eine Verbindung zu StoreFront-Stores herstellen. Siehe Einheitliche Benutzeroberfläche.

Zugriff auf Stores über Citrix Receiver für Web-Sites

Verwenden Sie die neueste Version der folgenden Browser, um über interne Netzwerkverbindungen und über Citrix Gateway auf Citrix Receiver für Web-Sites zuzugreifen:

Unter Windows

- Internet Explorer 11
- Microsoft Edge
- Google Chrome
- Mozilla Firefox

Unter Mac

- Safari

- Google Chrome
- Mozilla Firefox

Unter Linux

- Google Chrome
- Mozilla Firefox

Verbindungen über Citrix Gateway können per Citrix Gateway-Plug-In, ICA-Proxy oder clientloses VPN hergestellt werden. Außerdem sind bestimmte Versionen von Citrix Gateway erforderlich, um Verbindungen von außerhalb des Unternehmensnetzwerks zu ermöglichen. Weitere Informationen finden Sie unter Anforderungen an die Infrastruktur.

Starten von Ressourcen über Citrix Receiver für Web-Sites

Citrix Receiver für Web-Sites unterstützen den Start entweder über eine nativ installierte Citrix Workspace-App oder über Citrix Workspace-App für HTML5. Alle oben aufgeführten Browser sind HTML5-kompatibel und unterstützen HTML5-Ressourcenstarts. Abhängig von der Receiver für Web-Konfiguration können Endbenutzer zwischen den beiden Startmethoden wechseln.

Zugriff auf Stores über XenApp Services-URLs

Sie können XenApp Services-URLs verwenden, um auf StoreFront-Stores mit eingeschränkter Funktionalität zuzugreifen. XenApp Services-URLs bieten abwärtskompatible Legacyunterstützung für Verbindungen von Citrix Receiver 3.4 Enterprise und älteren Clients, die nur Verbindungen über PNAgent unterstützen. Verbindungen über Citrix Gateway, sofern unterstützt, können mit dem Citrix Gateway-Plug-In oder über clientlosen Zugriff hergestellt werden.

Anforderungen für Smartcards

Verwenden von Citrix Receiver für Windows 4.x und Citrix Workspace-App 1808 für Windows und höher 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 Citrix Virtual Apps and Desktops-Dokumentation und unter http://www.citrix.com/ready.

Authentifizierung über Citrix Gateway

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

- Citrix Gateway 13.0
- Citrix Gateway 12.1
- NetScaler Gateway 12.0
- NetScaler Gateway 11.1

Anforderungen für Citrix Analytics

Sie können Citrix StoreFront so konfigurieren, dass die Citrix Workspace-App Daten an Citrix Analytics senden kann. Konfigurationsdetails werden unter Citrix Analytics-Dienst beschrieben. Diese Funktionalität wird für die folgenden Szenarien unterstützt:

- Stores, auf die über Citrix Receiver für Websites mit HTML5-kompatiblen Browsern zugegriffen wird. Beim Starten von Ressourcen über die native Citrix Workspace-App oder HTML5 werden Citrix Analytics Service-Daten bereitgestellt.
- Stores, auf die über die Citrix Workspace-App 1903 für Windows oder höher zugegriffen wird.
- Stores, auf die über die Citrix Workspace-App 1901 für Linux oder höher zugegriffen wird.

Planen der StoreFront-Bereitstellung

January 6, 2020

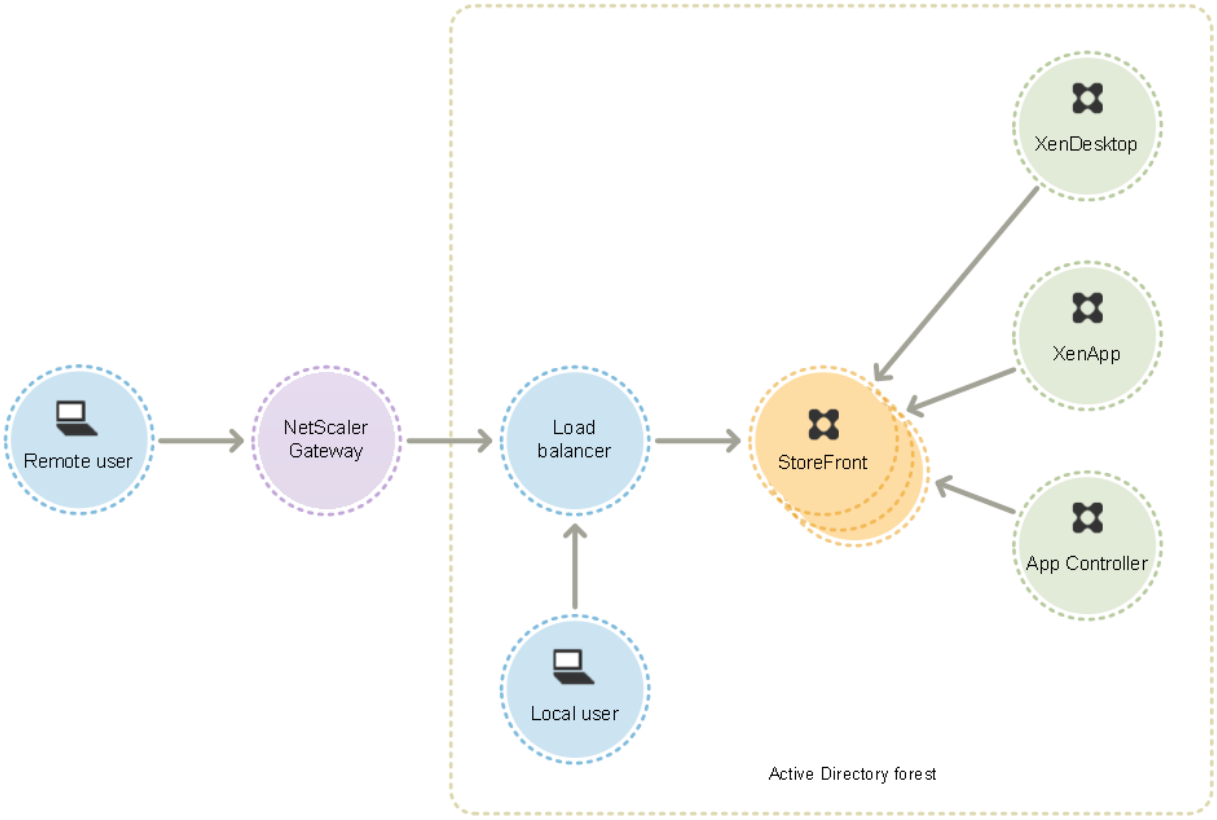
StoreFront nutzt Microsoft .NET-Technologie, die auf Microsoft Internetinformationsdienste (IIS) ausgeführt wird, zur Bereitstellung von Unternehmens-App-Stores, in denen Ressourcen zusammengefasst und Benutzern zur Verfügung gestellt werden. StoreFront kann in Ihre Citrix Virtual Apps and Desktops-Bereitstellungen 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 Citrix Virtual Apps and Desktops aufgelistet und zusammengefasst. Die Benutzer greifen auf Stores über die Citrix Workspace-App, Citrix Receiver für Web-Sites 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.



Lastausgleich

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

Aktiver Lastausgleich von Anfragen, die von StoreFront an Citrix Virtual Desktops-Sites und Citrix Virtual Apps-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. Citrix ADC.

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

Syntax:

```
1  Set-STFWebReceiverCommunication [-WebReceiverService] <
       WebReceiverService> [[-Loopback] <On | Off | OnUsingHttp>] [[-
```



```
        LoopbackPortUsingHttp] <Int32>]
```

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. Dies kann 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:

```
1 $wr = Get-STFWebReceiverService -VirtualPath /Citrix/StoreWeb
2 Set-STFWebReceiverCommunication -WebReceiverService $wr -Loopback
     OnUsingHttp -LoopbackPortUsingHttp 81
```

> **Hinweis:**
>
> Deaktivieren Sie Loopback, 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 Citrix Virtual Apps and Desktops-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, erfordert StoreFront, dass die IIS-Instanz, auf der der Authentifizierungsdienst gehostet wird, und damit verknüpfte Stores für HTTPS konfiguriert ist. 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 Citrix Gateway erforderlich, um sichere Verbindungen für Remotebenutzer zu gewährleisten. Stellen Sie Citrix Gateway außerhalb des Unternehmensnetzwerks bereit und trennen Sie es vom öffentlichen und internen Netzwerk durch Firewalls. Stellen Sie sicher, dass Citrix 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 zum Erstellen von Websites in IIS finden Sie unter Einrichten einer ersten 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 Workspace-App-Benutzer, die von einer StoreFront-Servergruppe unterstützt werden, hängt von der verwendeten Hardware und dem Grad der Benutzeraktivität ab. Basierend auf simulierten Aktivitäten, bei denen sich Benutzer anmelden, 100 veröffentlichte Anwendungen enumerieren und eine Ressource starten, ist zu erwarten, dass ein einzelner StoreFront-Server mit der empfohlenen Mindestanzahl von zwei virtuellen CPUs auf einem Intel Xeon L5520 2,27 Ghz-Prozessorserver bis zu 30.000 Benutzerverbindungen pro Stunde ermöglicht.

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 Citrix Receiver für Web sollten Sie für die Citrix Workspace-App 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:**
>
> StoreFront-Servergruppenbereitstellungen werden nur unterstützt, wenn die Verbindungen zwischen Servern in einer Servergruppe eine Latenz von weniger als 40 ms (bei deaktivierten Abonnements) oder weniger als 3 ms (bei aktivierten Abonnements) haben. Idealerweise sollten alle Server in einer Servergruppe an demselben Standort sein (Rechenzentrum, Availability Zone). Servergruppen können aber über Standorte innerhalb derselben Region verteilt sein, vorausgesetzt, dass Verbindungen zwischen Servern in der Gruppe diese Latenzkriterien erfüllen. Beispiele hierfür sind Servergruppen, die Availability Zones innerhalb einer Cloudregion oder Rechenzentren in einer Metropolregion umfassen. Beachten Sie, dass die Latenz zwischen den

> Zonen je nach Cloudanbieter unterschiedlich ist. Citrix empfiehlt nicht, für die Notfallwiederherstellung standortübergreifende Konfigurationen zu verwenden, sie kann jedoch für eine hohe Verfügbarkeit geeignet sein.
>
> StoreFront-Servergruppen mit unterschiedlichen Betriebssystemversionen, unterschiedlichen Betriebssystemsprachen und unterschiedlichen 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.

Informationen zum Festlegen von Timeouts finden Sie unter Kommunikationstimeoutdauer und Serverwiederholungsversuche und Kommunikationstimeoutdauer und Wiederholungsversuche.

Benutzerzugriffsoptionen

December 23, 2019

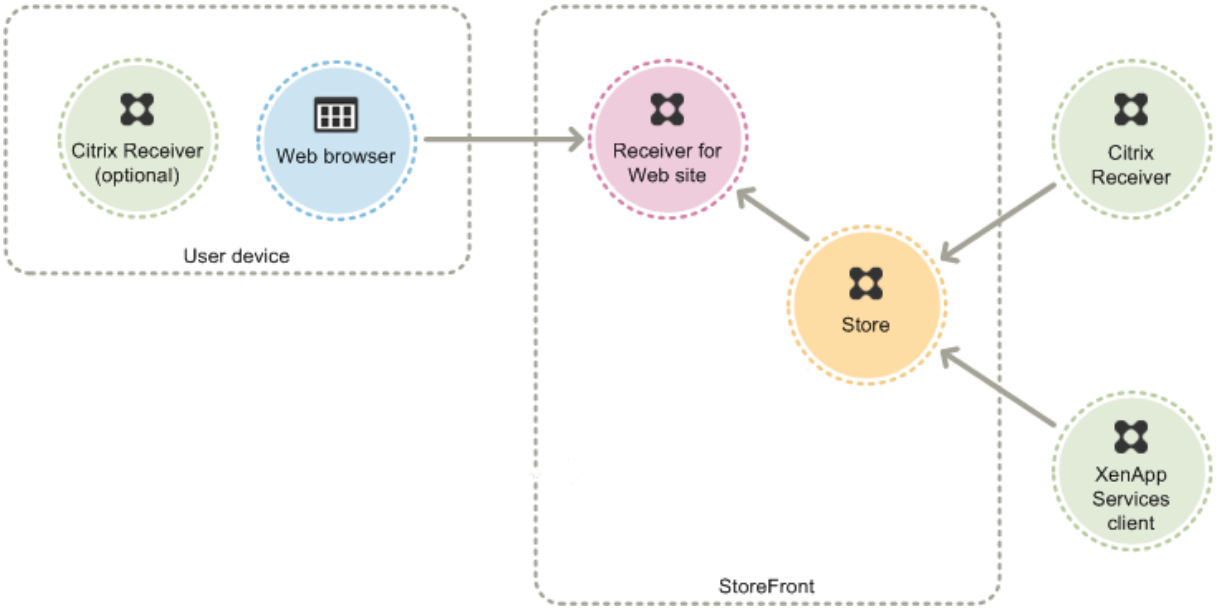
Es gibt drei verschiedene Methoden, wie Benutzer auf StoreFront-Stores zugreifen können.

- Citrix Receiver oder Citrix Workspace-App - Benutzer mit kompatiblen Versionen von Citrix Receiver bzw. der Citrix Workspace-App können direkt von der Citrix Receiver/bzw. Citrix Workspace-App-Benutzeroberfläche auf StoreFront-Stores zugreifen. Dies 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 bzw. der Citrix Workspace-App,

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 bzw. die Citrix Workspace-App zu installieren. Bei der Erstellung eines neuen Stores wird standardmäßig eine Citrix Receiver für Web-Site 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 oder Citrix Workspace-App

Zugriff auf Stores von der Benutzeroberfläche von Citrix Receiver bzw. der Citrix Workspace-App aus bietet die beste Benutzererfahrung und den größten Funktionsumfang. Informationen dazu, mit welchen Citrix Receiver/Citrix Workspace-App-Versionen Sie so auf Stores zugreifen können, finden Sie unter Systemanforderungen. Erläuterungen zur Citrix Workspace-App in diesem Dokument gelten, sofern nicht anders angegeben, auch für die unterstützten Versionen von Citrix Receiver.

Die Citrix Workspace-App verwendet interne und externe URLs als Beacons. Anhand des Versuchs, diese Beacons zu kontaktieren, kann die Citrix Workspace-App 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 die Citrix Workspace-App zurückgegeben werden können. Dadurch wird sichergestellt, dass die Benutzer nicht aufgefordert

werden, sich neu anzumelden, wenn sie auf einen Desktop oder eine Anwendung zugreifen. Weitere Informationen finden Sie unter Konfigurieren von Beacons.

Nach der Installation müssen in der Citrix Workspace-App 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 die Citrix Workspace-App 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 mit Befehlszeilenparametern in der Dokumentation zu Citrix Receiver bzw. zur Citrix Workspace-App für Windows.

Provisioningdateien

Sie können Provisioningdateien mit den Verbindungsinformationen für die Stores der Benutzer bereitstellen. Nach der Installation der Citrix Workspace-App öffnen die 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 von Store-Provisioningdateien für Benutzer.

Automatisch generierte Setup-URLs

Für Mac OS-Benutzer können Sie mit dem Setup URL Generator von Citrix Receiver bzw. der Citrix Workspace-App für Mac eine URL mit den Verbindungsinformationen für einen Store erstellen. Nach der Installation der Citrix Workspace-App klicken die 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 die Citrix Workspace-App eingeben. Weitere Informationen finden Sie in der Dokumentation zur Citrix Workspace-App.

E-Mail-basierte Kontenermittlung

Wenn Benutzer die Citrix Workspace-App auf einem Gerät zum ersten Mal installieren, können sie ihr Konto durch Eingabe ihrer E-Mail-Adresse einrichten, sofern sie die Citrix Workspace-App von der Citrix Website oder einer im internen Netzwerk gehosteten Downloadseite herunterladen. Sie konfigurieren die Locator-Ressourceneinträge der Dienstidentifizierung (SRV) für Citrix Gateway oder StoreFront auf dem Microsoft Active Directory-DNS-Server (Domain Name System). Die Benutzer müssen die Zugriffsinformationen für ihre Stores nicht kennen. Stattdessen geben sie während der Citrix Workspace-App-Erstkonfiguration ihre E-Mail-Adresse an. Die Citrix Workspace-App 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 die Citrix Workspace-App zugreifen können.

Konfigurieren der e-mail-basierten Kontenermittlung

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

Während der Erstkonfiguration fordert die Citrix Workspace-App die Benutzer auf, eine E-Mail-Adresse oder eine Store-URL einzugeben. Wenn ein Benutzer eine E-Mail-Adresse eingibt, ruft die Citrix Workspace-App vom Microsoft Active Directory-DNS-Server für die in der E-Mail-Adresse angegebene die Domäne eine Liste der verfügbaren Stores ab, aus der der Benutzer auswählen kann.

Damit die Citrix Workspace-App verfügbare Stores auf Grundlage der E-Mail-Adressen von Benutzern finden kann, konfigurieren Sie die Ressourceneinträge für den Dienstidentifizierungslocator (SRV) für Citrix Gateway oder StoreFront auf dem DNS-Server. Als Fallback können Sie StoreFront auch auf einem Server namens “discoverReceiver.domain” bereitstellen, wobei domain der Name der Domäne

mit den E-Mail-Konten der Benutzer ist. Wenn kein SRV-Eintrag in der angegebene Domäne gefunden wird, sucht die Citrix Workspace-App nach einer Maschine mit dem Namen “discoverReceiver”, um einen StoreFront-Server zu finden.

Sie müssen ein gültiges Serverzertifikat auf dem Citrix 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. Für eine optimale Benutzererfahrung installieren Sie ein Zertifikat mit dem Eintrag “discoverReceiver.domain” für “Antragsteller” oder “Alternativer Antragstellername”, wobei “domain” die Domäne ist, die die E-Mail-Konten der 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 zwischen Citrix Workspace-App und StoreFront-Server eine Warnung bezüglich des Zertifikats angezeigt. Die e-mail-basierte Kontenermittlung kann nicht mit anderen Zertifikatsidentitäten verwendet werden.[](/en-us/netscaler-gateway/12-1/storefront-integration/ng-clg-session-policies-overview-con/ng-clg-storefront-policies-con/ng-clg-storefront-email-discovery-tsk.html)

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 Citrix 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 dem Windows **Startbildschirm** auf **Verwaltungstools** und klicken Sie im Ordner **Verwaltungstools** 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**.
3. Wählen Sie im Dialogfeld **Ressourceneintragstyp** die Option **Dienstidentifizierung (SRV)** 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 Citrix Gateway-Gerät (Unterstützung lokaler und Remotebenutzer) oder den StoreFront-Server (nur Unterstützung von Benutzern im lokalen Netzwerk) im Format *servername.domäne:port* an.

Wenn Ihre Umgebung sowohl interne als auch externe DNS-Server enthält, können Sie einen SRV-Eintrag mit dem StoreFront-Server-FQDN auf Ihrem internen DNS-Server und einen weiteren Eintrag auf dem externen Server mit dem FQDN von Citrix Gateway hinzufügen. Mit dieser Konfiguration erhalten lokale Benutzer die StoreFront-Details, Remotebenutzer dagegen Citrix Gateway-Verbindungsinformationen.

7. Wenn Sie einen SRV-Eintrag für das Citrix Gateway-Gerät konfiguriert haben, fügen Sie Citrix 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 der Citrix Workspace-App installieren, um auf ihre Desktops und Anwendungen zuzugreifen. Weitere Informationen über die Kombinationen von Citrix Workspace-App 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 die Citrix Workspace-App auf dem Benutzergerät installiert ist, wenn ein Benutzer über einen Computer unter Windows oder Mac OS X auf Citrix Receiver für Web-Sites zugreift. Wenn die Citrix Workspace-App nicht erkannt wird, wird der Benutzer aufgefordert, die App 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 Workspace-App-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 bzw. der Citrix Workspace-App für Windows und Citrix Receiver bzw. der Citrix Workspace-App für Mac finden Sie unter Konfigurieren von Citrix Receiver für Web-Sites.

Citrix Workspace-App für HTML5

Die Citrix Workspace-App für HTML5 ist eine StoreFront-Komponente, die standardmäßig in Citrix Receiver für Web-Sites integriert ist. Sie können die Citrix Workspace-App für HTML5 auf den Citrix Receiver für Web-Sites aktivieren, sodass Benutzer, die die Citrix Workspace-App nicht installieren können, weiterhin Zugriff auf ihre Ressourcen haben. Mit der Citrix Workspace-App für HTML5 können Benutzer direkt in HTML5-kompatiblen Browsern auf Desktops und Anwendungen zugreifen, ohne die Citrix Workspace-App installieren zu müssen. Wenn Sie eine Site erstellen, ist die Citrix

Workspace-App für HTML5 standardmäßig deaktiviert. Weitere Informationen zum Aktivieren der Citrix Workspace-App für HTML5 finden Sie unter citrix-receiver-download-page-template.html.

Für den Zugriff auf Desktops und Anwendungen mit der Citrix Workspace-App 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 der Citrix Workspace-App für HTML5 verwendet werden können, finden Sie unter Anforderungen für Benutzergeräte.

Die Citrix Workspace-App für HTML5 kann von Benutzern im internen Netzwerk und von Remotebenutzern, die eine Verbindung über Citrix Gateway herstellen, verwendet werden. Für Verbindungen über das interne Netzwerk unterstützt die Citrix Workspace-App 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 Citrix Gateway herstellen, können auf Ressourcen zugreifen, die über eine breitere Produktpalette bereitgestellt werden, wenn Sie beim Konfigurieren von StoreFront die Citrix Workspace-App für HTML5 als Option wählen. Bestimmte Versionen von Citrix Gateway sind für die Citrix Workspace-App für HTML5 erforderlich. Weitere Informationen finden Sie unter Anforderungen an die Infrastruktur.

Für lokale Benutzer im internen Netzwerk ist der Zugriff über die Citrix Workspace-App für HTML5 auf Ressourcen, die von Citrix Virtual Apps and Desktops bereitgestellt werden, standardmäßig deaktiviert. Sie aktivieren den lokalen Zugriff auf Desktops und Anwendungen über die Citrix Workspace-App für HTML5, indem Sie die Richtlinie für ICA-WebSockets-Verbindungen auf den Citrix Virtual Apps and Desktops-Servern aktivieren. Stellen Sie sicher, dass die Firewalls und anderen Netzwerkgeräte den Zugriff auf den in der Richtlinie festgelegten Port für die Citrix Workspace-App für HTML5 zulassen. Weitere Informationen finden Sie unter Einstellungen der Richtlinie “WebSockets”.

Standardmäßig werden Desktops und Anwendungen in der Citrix Workspace-App für HTML5 auf einer neuen Browserregisterkarte gestartet. Beim Start von Ressourcen über Verknüpfungen mit der Citrix Workspace-App 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 die Citrix Workspace-App für HTML5 so konfigurieren, dass Ressourcen immer auf der gleichen Registerkarte wie die Receiver für Web-Site gestartet werden. Weitere Informationen finden Sie unter Konfigurieren der Verwendung der Browserregisterkarten für die Citrix Workspace-App 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. 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 Citrix Receiver für Web-Site startet automatisch die Ressource. Im Fall von Anwendungen wird zudem ein Abonnement für die Benutzer erstellt, wenn diese eine Anwen-

dung 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 die Citrix Workspace-App installiert haben oder die Citrix Workspace-App 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 die Citrix Workspace-App 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. Weisen Sie 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 Citrix 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 Citrix 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 Überlegungen

Benutzer, die über eine Citrix Receiver für Web-Site auf Stores zugreifen, profitieren von vielen der Features, die bei Storezugriff in der Citrix Workspace-App verfügbar sind, z. B. der 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 Citrix 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.
- Die Citrix Workspace-App 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 Citrix Gateway herstellt.
- Wenn Benutzer die Citrix Workspace-App 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.

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 die Citrix Workspace-App bei XenApp Services-URLs. Citrix Ready-Partnerprodukte verwenden die Citrix

Fast Connect-API zur Leitung von Benutzeranmeldungen über Citrix Receiver bzw. die Citrix Workspace-App 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 Citrix Virtual Apps and Desktops bereitgestellten Desktops und Anwendungen verbunden. Weitere Informationen finden Sie in der aktuellen Dokumentation unter 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/c wobei "serveraddress" der vollqualifizierte Domänenname des Servers oder der Lastausgleichsumgebung für die StoreFront-Bereitstellung ist und "storename" der Name, den Sie beim Erstellen des Stores angegeben haben. Dies ermöglicht die Verwendung von Citrix Workspace-App-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 Überlegungen

XenApp Services-URLs dienen zur Unterstützung von Benutzern, die nicht auf die Citrix Workspace-App 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 Citrix Virtual Apps and Desktops-Server, die Desktops und Anwendungen für den Store bereitstellen, an den Domänencontroller geleitet. Der StoreFront-Authentifizierungsdienst wird dabei umgangen.

Benutzerauthentifizierung

April 1, 2020

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 Citrix Gateway verwendet, um auf Citrix Receiver für Web zuzugreifen, verwaltet Citrix 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 Citrix Gateway-Sitzung beendet und der Benutzer muss sich neu anmelden. Benutzer von Citrix Receiver bzw. der Citrix Workspace-App 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 Citrix Gateway.

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:

- Citrix Verbundauthentifizierungsdienst implementiert.
- 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 Bereitstellung von Microsoft AD FS 2016 und Microsoft AD FS 2016-Vorgänge.
  - Microsoft AD FS v3.0 (Windows Server 2012 R2)
  - Citrix Gateway (als IdP konfiguriert)
- Konfigurieren Sie die SAML-Authentifizierung in StoreFront über die StoreFront-Verwaltungskonsole in einer neuen Bereitstellung (siehe Erstellen einer neuen Bereitstellung) oder in einer bestehenden Bereitstellung (siehe Konfigurieren des Authentifizierungsdiensts) Sie können die SAML-Authentifizierung auch mit PowerShell-Cmdlets konfigurieren (siehe StoreFront SDK).
- Citrix Receiver (4.6 und höher) bzw. Citrix Workspace-App für Windows oder Citrix Receiver für Web.

Die Verwendung der SAML-Authentifizierung mit Citrix Gateway 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. Sie können die Domänen-Passthrough-Authentifizierung für Benutzer aktivieren, die über die Citrix Workspace-App und XenApp Services-URLs eine Verbindung mit Stores herstellen. Citrix Receiver für Web-Sites unterstützen die Domänen-Passthrough-Authentifizierung für Internet Explorer, Microsoft Edge, Mozilla Firefox und Google Chrome auf domänengebundenen Windows-Clientmaschinen.

Aktivieren der Domänen-Passthrough-Authentifizierung

1. Installieren Sie Citrix Receiver bzw. die Citrix Workspace-App für Windows oder das Citrix Online-Plug-In für Windows auf den Benutzergeräten. Stellen Sie sicher, dass die Passthrough-Authentifizierung aktiviert ist.
2. Aktivieren Sie die Domänen-Passthrough-Authentifizierung in dem Citrix Receiver für Web-Site Knoten in der Verwaltungskonsole.
3. Konfigurieren Sie SSON in Citrix Receiver bzw. der Citrix Workspace-App für Windows (siehe Konfigurieren von Domänen-Passthrough-Authentifizierung). Die Citrix Workspace-App für HTML5 unterstützt keine Passthrough-Authentifizierung für Domänen.
4. Das Standardverhalten von Windows ist automatische Anmeldung nur in der Intranetzone. Konfigurieren Sie für Internet Explorer, Mozilla Firefox und Google Chrome entweder Citrix Receiver

für Web-Sites als Intranetsites in den Internetoptionen oder aktivieren Sie die automatische Anmeldung für die vertrauenswürdige Zonen. Für Microsoft Edge müssen Sie Citrix Receiver für Web-Sites als Intranetsites konfigurieren.

5. Ändern Sie für Mozilla Firefox die erweiterten Browsereinstellungen so, dass sie dem URI von Citrix Receiver bzw. der Citrix Workspace-App für Windows vertrauen.

   > Warnung:
   >
   > Fehlerhafte Änderungen an den erweiterten Einstellungen können zu schwerwiegenden Problemen führen. Änderungen machen Sie auf eigene Gefahr.

   a) Starten Sie Firefox und geben Sie **about:config** im Adressfeld ein und wählen Sie "Ich akzeptiere das Risiko!"
   b) Geben Sie **ntlm** in das Suchfeld ein.
   c) Doppelklicken Sie auf "network.automatic-ntlm-auth.trusted-uris" und geben Sie die Site-URL für Citrix Receiver bzw. die Citrix Workspace-App für Windows in das Popupdialogfeld ein.
   d) Klicken Sie auf **OK**.

Passthrough-Authentifizierung von Citrix Gateway

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

StoreFront unterstützt Passthrough mit den folgenden Citrix Gateway-Authentifizierungsmethoden.

- **Sicherheitstoken.** Die Benutzer melden sich bei Citrix Gateway mit Passcodes an, die von mit Sicherheitstoken generierten Tokencodes abgeleitet werden, in einigen Fällen in Kombination mit persönlichen Identifikationsnummern. 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 Citrix Gateway anmelden, müssen ihre Domänenanmeldeinformationen und ihre Sicherheitstoken-Passcodes eingeben.
- **Clientzertifikat.** Die Benutzer melden sich bei Citrix Gateway an und werden auf Grundlage der Attributen im Clientzertifikat, das Citrix Gateway übergeben wird, authentifiziert. Konfigurieren Sie die Clientzertifikat-Authentifizierung, damit die Benutzer sich bei Citrix 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 Citrix Gateway-Authentifizierungsdienst, damit diese Benutzer ihre Anmeldeinformationen nur einmal eingeben müssen. Standardmäßig ist die Passthrough-Authentifizierung jedoch nur für Benutzer aktiviert, die sich bei Citrix Gateway mit einem Kennwort anmelden. Zum Konfigurieren der Passthrough-Authentifizierung von Citrix Gateway bei StoreFront für Smartcardbenutzer delegieren Sie die Validierung der Anmeldeinformationen an Citrix Gateway. Weitere Informationen finden Sie unter Erstellen und Konfigurieren des Authentifizierungsdiensts.

Die Benutzer können eine Verbindung mit Stores in der Citrix Workspace-App mit Passthrough-Authentifizierung über einen SSL-VPN-Tunnel mit dem Citrix Gateway-Plug-In herstellen. Remotebenutzer, die das Citrix Gateway-Plug-In nicht installieren können, können über den clientlosen Zugriff eine Verbindung mit Stores in der Citrix Workspace-App mit Passthrough-Authentifizierung herstellen. Zur Verwendung des clientlosen Zugriffs für eine Verbindung mit Stores benötigen die Benutzer eine Version der Citrix Workspace-App, die den clientlosen Zugriff unterstützt.

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

Wenn Sie die Zweiquellenauthentifizierung bei Citrix Gateway für Remotebenutzer konfigurieren, die von der Citrix Workspace-App aus auf Stores zugreifen, müssen Sie zwei Authentifizierungsrichtlinien für Citrix 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. Wenn Sie das Citrix Gateway-Gerät zu Ihrer StoreFront-Konfiguration hinzufügen, legen Sie den Anmeldetyp auf “Domäne und Sicherheitstoken” fest. Weitere Informationen finden Sie unter http://support.citrix.com/article/CTX125364

Um die Multidomänenauthentifizierung über Citrix Gateway zu StoreFront zu aktivieren, setzen Sie in der Citrix Gateway-LDAP-Authentifizierungsrichtlinie für jede Domäne das SSO-Namensattribut auf “userPrincipalName”. Sie können festlegen, dass die Benutzer auf der Citrix Gateway-Anmeldeseite eine Domäne angeben müssen, sodass die richtige zu verwendende LDAP Richtlinie ermittelt werden kann. Geben Sie beim Konfigurieren der Citrix 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 Citrix Gateway-Bereitstellung dies unterstützt, können Sie SmartAccess zur Steuerung des Benutzerzugriffs auf Citrix Virtual Apps and Desktops-Ressourcen auf der Basis von Citrix Gateway-Sitzungsrichtlinien verwenden. Weitere Informationen zu SmartAccess finden Sie unter Funktionsweise von SmartAccess für Citrix Virtual Apps and Desktops.

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 die Citrix Workspace-App, Citrix Receiver für Web und XenApp Services-URLs eine Verbindung mit Stores herstellen.

Verwenden Sie die Smartcardauthentifizierung, um den Anmeldeprozess für Ihre Benutzer zu optimieren und gleichzeitig die Sicherheit des Benutzerzugriffs auf Ihre Infrastruktur zu erhöhen. 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 Citrix Virtual Apps and Desktops 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.

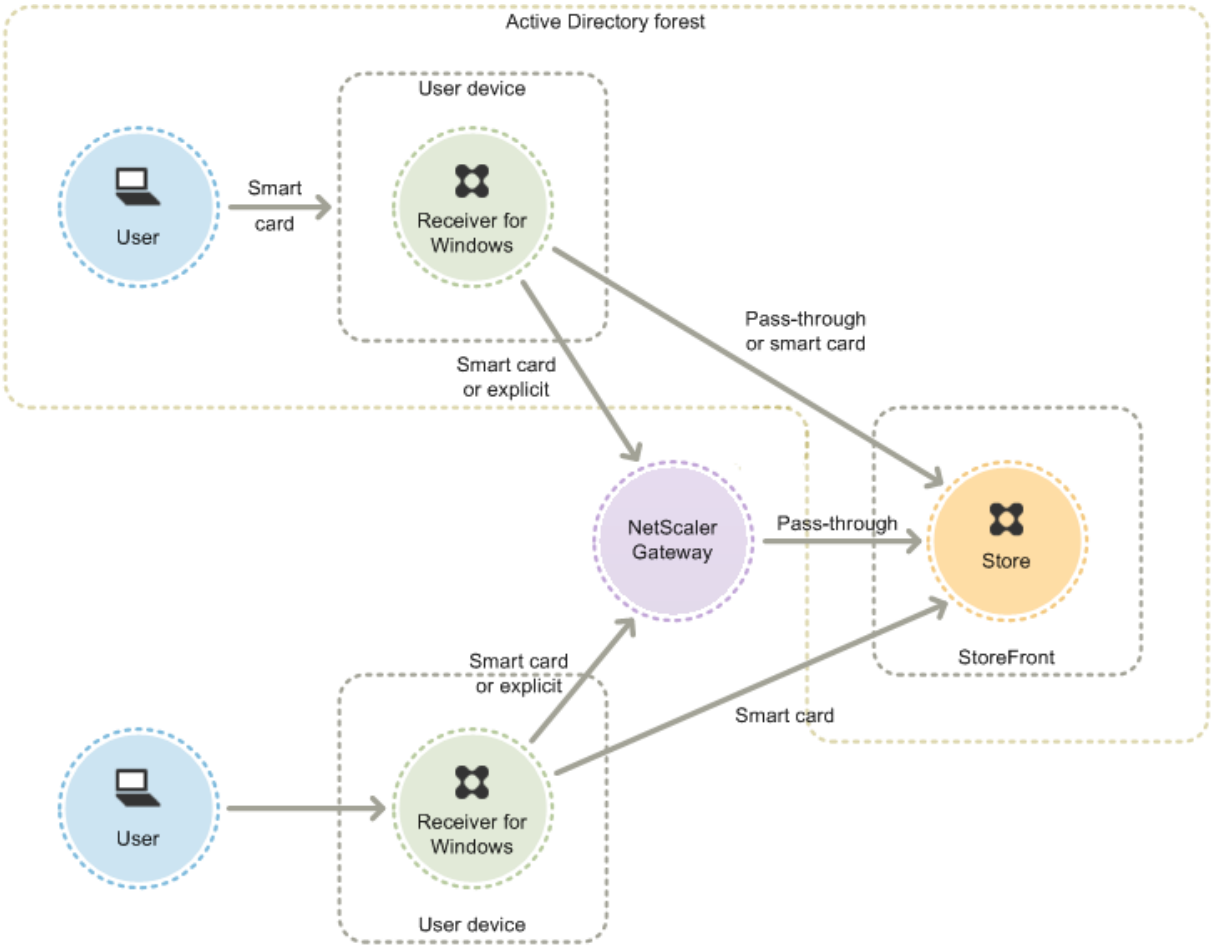
Die Konfiguration der Smartcardauthentifizierung bei StoreFront hängt von den Benutzergeräten, den installierten Clients und davon ab, ob die Geräte in die Domäne eingebunden sind. In diesem Zusammenhang bedeutet in die Domäne eingebunden, das die Geräte in eine Domäne in der Active Directory-Gesamtstruktur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

Verwenden von Smartcards mit Citrix Receiver bzw. der Citrix Workspace-App für Windows

Benutzer mit Geräten, die Citrix Receiver bzw. die Citrix Workspace-App für Windows ausführen, können sich mit Smartcards direkt oder über Citrix Gateway authentifizieren. Es können domänenge-

bundene und nicht domänengebundene Geräte verwendet werden, allerdings bei einer geringfügig anderen Benutzererfahrung.

Die Abbildung zeigt die Optionen für die Smartcardauthentifizierung über Citrix Receiver bzw. die Citrix Workspace-App 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/die Citrix Workspace-App für Windows für Passthrough-Authentifizierung und aktivieren Domänen-Passthrough-Authentifizierung für StoreFront.

Die Benutzer melden sich beim Gerät an und authentifizieren sich dann bei Citrix Receiver bzw. der Citrix Workspace-App 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 bzw. der Citrix

Workspace-App 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 Citrix 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 Citrix Gateway bei StoreFront und delegieren die Anmeldeinformationenvalidierung an Citrix Gateway. Erstellen Sie dann einen weiteren virtuellen Citrix Gateway-Server und leiten Sie über ihn die Benutzerverbindungen zu Ressourcen. Für in Domänen eingebundene Geräte müssen Sie zudem Citrix Receiver bzw. die Citrix Workspace-App für Windows für Passthrough-Authentifizierung konfigurieren.

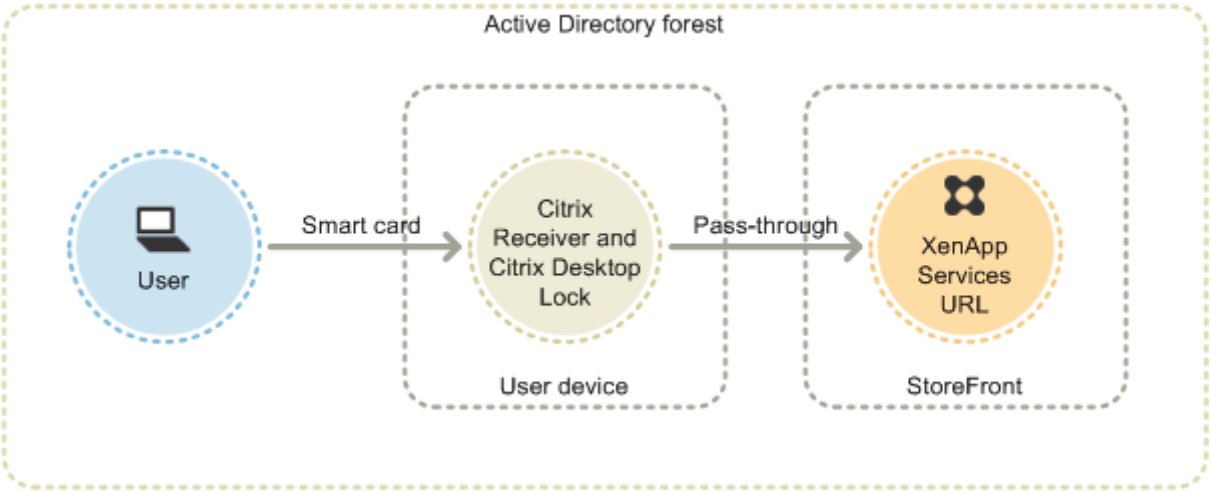
> **Hinweis:**
>
> Wenn Sie Citrix Receiver bzw. die Citrix Workspace-App für Windows verwenden, können Sie einen zweiten virtuellen Server einrichten und durch Verwendung des optimalen Gateway-Routings die PIN-Eingabeaufforderungen beim Starten von Apps und Desktops vermeiden.

Die Benutzer können sich bei Citrix Gateway mit Smartcard und PIN oder mit expliziten Anmeldeinformationen anmelden. Sie erhalten so die Möglichkeit, für die Anmeldung bei Citrix Gateway auf die explizite Authentifizierung zurückzugreifen. Konfigurieren Sie die Passthrough-Authentifizierung von Citrix Gateway an StoreFront und delegieren Sie die Validierung der Anmeldeinformationen für Smartcardbenutzer an Citrix Gateway, sodass Benutzer automatisch bei StoreFront authentifiziert werden.

Verwenden von Smartcards mit XenApp Services-URLs

Benutzer 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 Desktopgerät in der Domäne, 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 werden nicht noch einmal aufgefordert, ihre PIN einzugeben.

Verwenden von Smartcards mit Citrix Receiver für Web

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

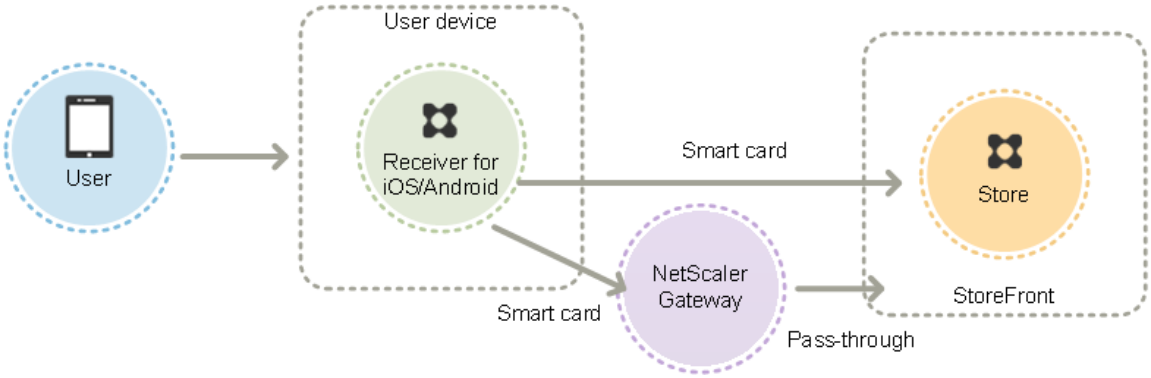
1. Wählen Sie den Knoten “Citrix Receiver für Web” im linken Bereich aus.
2. Wählen Sie die Site aus, für die Sie die Smartcardauthentifizierung verwenden möchten.
3. Wählen Sie die Aufgabe Authentifizierungsmethoden auswählen im rechten Bereich.
4. Aktivieren Sie das Smartcardkontrollkästchen im Popupdialogfeld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

Wenn Sie die Passthrough-Authentifizierung mit Smartcards bei Citrix Virtual Apps and Desktops für Benutzer von Citrix Receiver bzw. der Citrix Workspace-App für Windows aktivieren, die domänengebundene Geräte verwenden und nicht über Citrix 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 Citrix Virtual Apps and Desktops für Benutzer von Citrix Receiver bzw. der Citrix Workspace-App für Windows aktivieren, die domänengebundene Geräte verwenden und über Citrix 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 der Citrix Workspace-App für iOS und Android

Benutzer, die die Citrix Workspace-App für iOS oder Android ausführen, können sich mit Smartcards direkt oder über Citrix 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 Workspace-App-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 Citrix 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 Citrix Gateway bei StoreFront und delegieren die Anmeldeinformationenvalidierung an Citrix Gateway. Erstellen Sie dann einen weiteren virtuellen Citrix Gateway-Server und leiten Sie über ihn die Benutzerverbindungen zu Ressourcen.

Users can log on to Citrix Gateway using either their smart cards and PINs or with explicit credentials, depending on how you specified the authentication for the connection. Konfigurieren Sie die Passthrough-Authentifizierung von Citrix Gateway an StoreFront und delegieren Sie die Validierung der Anmeldeinformationen für Smartcardbenutzer an Citrix Gateway, sodass Benutzer automatisch bei StoreFront authentifiziert werden. Wenn Sie die Authentifizierungsmethode wechseln möchten, müssen Sie die Verbindung löschen und neu erstellen.

Verwenden von Smartcards mit Citrix Receiver bzw. der Citrix Workspace-App für Linux

Benutzer mit Citrix Receiver bzw. der Citrix Workspace-App für Linux 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 bzw. der Citrix Workspace-App 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 bzw. der Citrix Workspace-App für Windows konfigurieren. Siehe Konfigurieren der Smartcardauthentifizierung. Informationen zur Verwendung von Smartcards finden Sie unter Citrix Receiver für Linux.

Die Mindestzahl der Anmeldeaufforderungen an Benutzer ist 1. Die Benutzer melden sich beim Gerät an und authentifizieren sich dann bei Citrix Receiver bzw. der Citrix Workspace-App 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 oder der Citrix Workspace-App 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 Citrix 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 Citrix Gateway bei StoreFront und delegieren die Anmeldeinformationenvalidierung an Citrix Gateway. Erstellen Sie dann einen weiteren virtuellen Citrix Gateway-Server und leiten Sie über ihn die Benutzerverbindungen zu Ressourcen.

Die Benutzer können sich bei Citrix Gateway mit Smartcard und PIN oder mit expliziten Anmeldeinformationen anmelden. Sie erhalten so die Möglichkeit, für die Anmeldung bei Citrix Gateway auf die explizite Authentifizierung zurückzugreifen. Konfigurieren Sie die Passthrough-Authentifizierung von Citrix Gateway an StoreFront und delegieren Sie die Validierung der Anmeldeinformationen für Smartcardbenutzer an Citrix Gateway, sodass Benutzer automatisch bei StoreFront authentifiziert werden.

Smartcards für Citrix Receiver bzw. die Citrix Workspace-App für Linux werden auf den XenApp Services-Supportsites nicht unterstützt.

Wenn die Smartcard-Unterstützung sowohl auf dem Server als auch in der Citrix Workspace-App ak-

tiviert 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 Virtual Apps and Desktops-Servern.
- Smartcard-Anwendungsunterstützung: Zugriff auf lokale Smartcardgeräte über smartcard-fähige 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 Workspace-App 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 die PowerShell.

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

Wichtige Überlegungen

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

- Zur Verwendung eines VPN-Tunnels mit Smartcardauthentifizierung müssen die Benutzer das Citrix 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 Citrix 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 Citrix Virtual Apps and Desktops für Benutzer von Citrix Receiver bzw. der Citrix Workspace-App für Windows aktivieren, die domänengebundene Geräte verwenden und nicht über Citrix 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 Citrix Virtual Apps and Desktops für Benutzer von Citrix Receiver bzw. der Citrix Workspace-App für Windows aktivieren, die domänengebundene Geräte verwenden und über Citrix 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 Citrix 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

December 23, 2019

StoreFront hat Features zur Verbesserung der Benutzererfahrung. Diese sind standardmäßig konfiguriert, wenn Sie neue Stores und die zugehörigen Citrix Receiver für Web-Sites 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 wieder verbunden, 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 die Citrix Workspace-App auf den Geräten der Benutzer installiert ist oder wenn die Citrix Workspace-App 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 Startmenü mit der Citrix Workspace-App 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 Citrix Virtual Apps and Desktops 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.

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 Citrix Virtual Desktops-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 der Citrix Workspace-App 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

Berücksichtigen Sie die folgenden Optionen bei der Bereitstellung von Anwendungen mit Citrix Virtual Apps and Desktops, um die Benutzerfreundlichkeit beim Zugreifen auf Anwendungen über Ihre Stores

zu erhöhen. 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. Die von Ihnen in Citrix Virtual Apps and Desktops erstellten Ordner werden in der Citrix Workspace-App als Kategorien angezeigt. Sie können beispielsweise Anwendungen nach Typ gruppieren oder alternativ Ordner für verschiedene Benutzerrollen in Ihrer Organisation erstellen.
- Verwenden Sie aussagekräftige Beschreibungen für veröffentlichte Anwendungen, da die Beschreibungen in der Citrix Workspace-App angezeigt werden.
- Sie können für alle Benutzer einen Basissatz von Anwendungen festlegen, die sich nicht vom Homebildschirm der Citrix Workspace-App 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 **Appis available in Citrix Receiver or Citrix Workspace app 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 den Benutzern Citrix Virtual Apps and Desktops-Anwendungen an oder listen Sie häufig verwendete Anwendungen in der Highlightliste in Citrix Workspace-App auf. 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 Citrix Virtual Apps and Desktops 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 die Citrix Workspace-App nach dem angegebenen Namen oder Pfad auf dem Gerät des Benutzers, um zu ermitteln, ob die Anwendung bereits lokal installiert ist. Wenn die Anwendung gefunden wird, abonniert die Citrix Workspace-App die bereitgestellte Anwendung für den Benutzer, erstellt jedoch keine Verknüpfung. Wenn der Benutzer die übermittelte Anwendung mit der Citrix Workspace-App startet, wird stattdessen die lokal installierte Instanz ausgeführt. Weitere Informationen finden Sie unter Konfigurieren der Anwendungsbereitstellung.
- Wenn Benutzer eine veröffentlichte Anwendung auf einem veröffentlichten Desktop starten, können Administratoren in Citrix Virtual Apps and Desktops 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 bzw. die Citrix Workspace-App 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 unter CTX232210, dem Artikel Anwendungen in Citrix Virtual Apps and Desktops und der Dokumentation zu Citrix Receiver für Windows.

Hohe Verfügbarkeit und Multisitekonfiguration für StoreFront

September 10, 2019

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 Citrix Virtual Apps and Desktops-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 Citrix Virtual Apps and Desktops-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 Citrix Virtual Apps and Desktops-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 Citrix Gateway-Routing

Wenn Sie konfigurierte separate Citrix 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 Citrix 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 Citrix 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 Citrix Gateway-Routing können Sie auch in dem Spezialfall verwenden, wo lokale Benutzer im internen Netzwerk sich für die Endpunktanalyse an Citrix Gateway anmelden müssen. Mit dieser Konfiguration stellen Benutzer eine Verbindung mit dem Store über das Citrix 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 Citrix Gateway geleitet werden. Sie müssen auch eine spezifische interne virtuelle Server-IP-Adresse für das Citrix Gateway-Gerät konfigurieren. Außerdem müssen Sie einen nicht zugänglichen internen Beacon festlegen, damit die Citrix Workspace-App unabhängig vom Netzwerkstandort des Benutzers immer angefordert wird, eine Verbindung zu Citrix Gateway herzustellen.

Globaler Serverlastausgleich mit Citrix Gateway

StoreFront unterstützt für den globalen Serverlastausgleich konfigurierte Citrix 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 Citrix Gateway.

Weitere Informationen zum Lastausgleich finden Sie unter Lastausgleich mit Citrix ADC.

Wichtige Überlegungen

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 die Citrix Workspace-App 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

March 3, 2020

Vorbereiten der Installation

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

1. Wenn Sie mit StoreFront Citrix Virtual Apps and Desktops-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 Citrix ADC zum Lastausgleich zu verwenden, müssen Sie einen virtuellen Server als Proxyserver für die StoreFront-Server definieren. Weitere Informationen zum Konfigurieren von Citrix ADC für den Lastausgleich finden Sie unter Lastausgleich mit Citrix ADC.

a) Stellen Sie sicher, dass der Lastausgleich auf dem Citrix ADC-Gerät aktiviert ist.

b) Erstellen Sie für jeden StoreFront-Server nach Bedarf individuelle HTTP- oder SSL-Lastausgleichsdienste. Verwenden Sie dazu den Monitortyp “StoreFront”.

c) 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.

d) Erstellen Sie einen virtuellen Server und binden Sie die Dienste an den virtuellen Server.

e) Konfigurieren Sie auf dem virtuellen Server Persistenz unter Verwendung der **Client-IP-** oder der **Cookie-Insert-**Methode. 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 von 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 die Citrix Workspace-App HTTPS-Verbindungen zu Stores. Zum Konfigurieren von IIS, sodass Sie eine HTTPS-HostBaseURL in StoreFront verwenden können, erstellen Sie eine HTTPS-Bindung an die Standardwebsite und verknüpfen Sie sie mit dem StoreFront-Serverzertifikat. Weitere Hinweise zum Hinzufügen einer HTTPS-Bindung zu einer IIS-Site finden Sie unter Sichern der StoreFront-Bereitstellung.

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. Verwenden Sie die Citrix StoreFront-Verwaltungskonsole zum Konfigurieren des Servers.

Installieren von StoreFront

> **Wichtig**
>
> 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. Suchen Sie die Datei CitrixStoreFront-x64.exe und führen Sie sie als Administrator aus.
5. Lesen und akzeptieren Sie die Lizenzvereinbarung und klicken Sie auf **Weiter**.

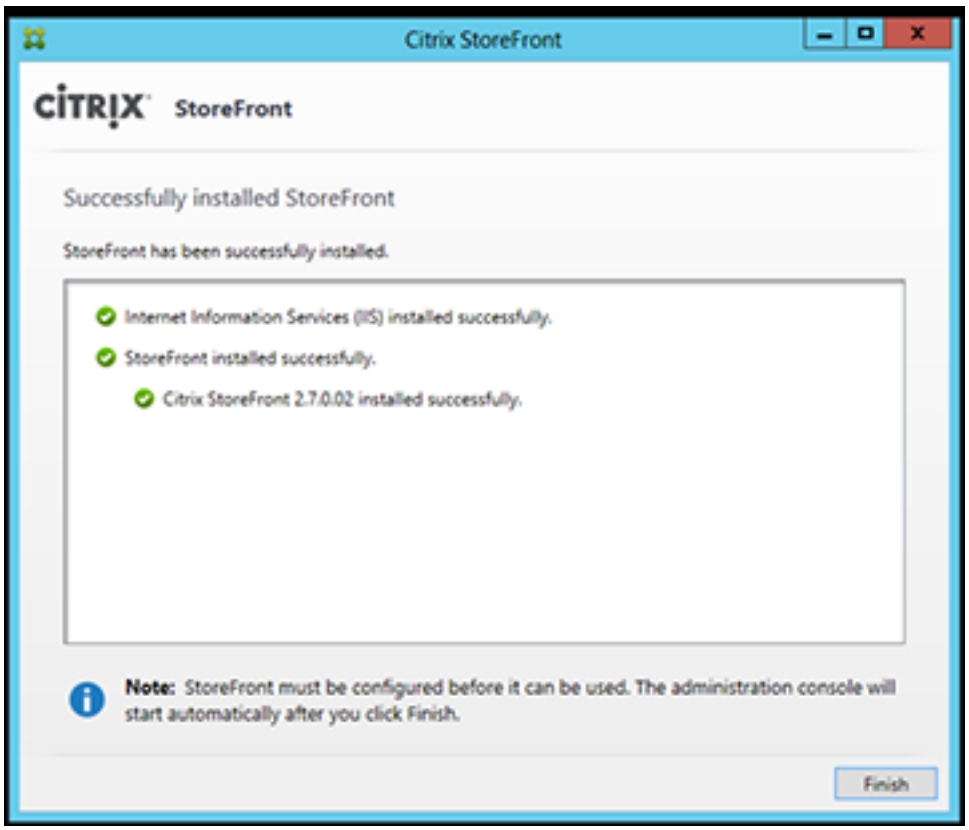
6. Wenn die Seite “Voraussetzungen prüfen” angezeigt wird, klicken Sie auf **Weiter**.
7. Prüfen Sie auf der Seite “Bereit zur Installation” die Voraussetzungen und StoreFront-Komponenten für die Installation und klicken Sie auf **Installieren**.

   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**.

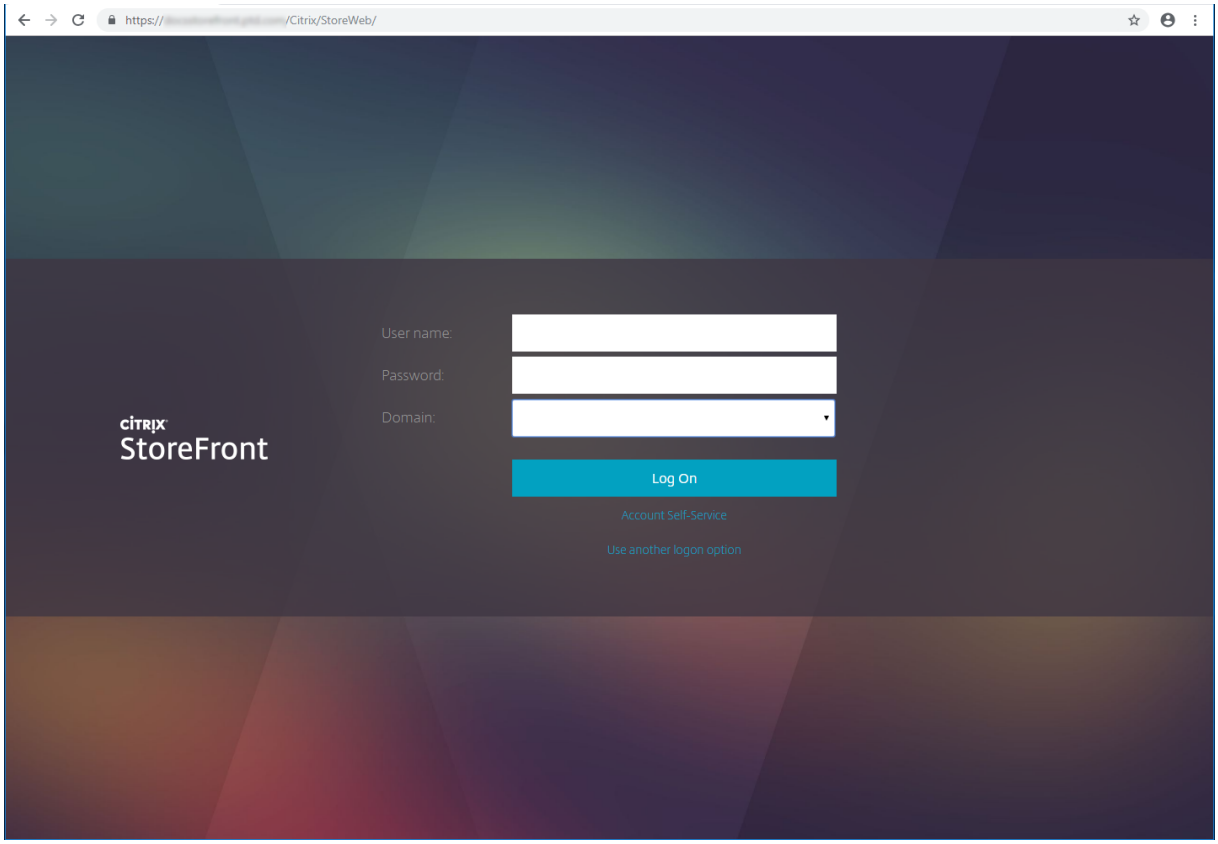
a) Geben Sie die URL des StoreFront-Servers im Feld **Basis-URL** an.
b) Geben Sie auf der Seite **Storename** einen Namen für den Store an und klicken Sie auf **Weiter**.

Geben Sie auf der Seite **Delivery Controller** Details zu den Citrix Virtual Apps and Desktops-Bereitstellungen ein, über die Sie Ressourcen im Store bereitstellen möchten.

1. Legen Sie die Parameter **Transporttyp** und **Port** fest. Beispiel: HTTP und Port 80 oder HTTPS und Port 443. Klicken Sie auf **OK**.
2. Wählen Sie auf der Seite **Remotezugriff** die Option “Keine” aus. Wenn Sie Citrix Gateway verwenden, wählen Sie “Kein VPN-Tunnel” und geben Sie die Gateway-Details ein.
3. 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 für Web-Site zur Verfügung, d. h. sie können über eine Webseite auf ihre Desktops und Apps zugreifen.

Die URL, über die Benutzer auf die Citrix Receiver für Web-Site für den neuen Store zugreifen, wird angezeigt. Beispiel: `example.net/Citrix/StoreWeb/`. Wenn Sie sich anmelden, greifen Sie auf die neue Benutzeroberfläche in der Citrix Workspace-App zu.



Installieren von StoreFront über eine Eingabeaufforderung

1. Melden Sie sich mit einem Konto mit lokalen Administratorberechtigungen bei StoreFront an.
2. Stellen Sie sicher, dass die Voraussetzungen für die Installation von StoreFront erfüllt sind, bevor Sie StoreFront installieren. Weitere Informationen finden Sie unter Vorbereiten der Installation.
3. Navigieren Sie im Installationsmedium oder Downloadpaket zu der Datei CitrixStoreFront-x64.exe und kopieren Sie die Datei an einen temporären Speicherort auf dem Server.
4. Navigieren Sie in der Befehlszeile zu dem Ordner, der die Installationsdatei enthält, 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 eine automatische Installation von StoreFront und seiner Voraussetzungen durchzuführen. Standardmäßig wird StoreFront unter C:\Programme\Citrix\Receiver StoreFront\ installiert. Sie können einen anderen Speicherort für die Installation mit dem Argument **-INSTALLDIR** angeben, wobei *installationlocation* das Verzeichnis ist, in dem StoreFront installiert werden soll. 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 die Citrix Workspace-App auf einem Windows- oder Mac OS X-Gerät nicht erkennt, wird der Benutzer standardmäßig aufgefordert, die für seine Plattform geeignete Version der Citrix Workspace-App von der Citrix Website herunterzuladen und zu installieren. Sie können dieses Verhalten insofern ändern, dass Benutzer die Citrix Workspace-App-Installationsdateien von dem StoreFront-Server herunterladen. Weitere Informationen finden Sie unter Konfigurieren der Anzeige von Ressourcen für Benutzer.

   Wenn Sie eine solche Konfigurationsänderung beabsichtigen, geben Sie die Argumente **-WINDOWS_CLIENT** und **-MAC_CLIENT** an, um die Installationsdateien für Citrix Receiver bzw. die Citrix Workspace-App für Windows und Receiver bzw. die Citrix Workspace-App 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 Installationsdatei. Die Installationsdateien für Citrix Receiver/die Citrix Workspace-App für Windows und Citrix Receiver/Citrix Workspace-App für Mac sind auf dem Installationsmedium für Citrix Virtual Apps and Desktops enthalten.

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 ein Backup der Registrierung, bevor Sie sie bearbeiten.

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

```
Location: HKLM:\Software\Citrix\Telemetry\CEIP
Name: Enabled
Type: REG_DWORD
Value: 0 = disabled, 1 = enabled
```

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

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

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

> **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”).
HTML5-Einstellung für Citrix Receiver für Web	Liste von Zeichenfolgen, die die HTML5-Einstellung für Web Receiver angeben (“Always”, “Fallback” oder “Off”).
Workspace Control für Citrix Receiver bzw. die Citrix Workspace-App aktiviert	Liste boolescher Werte, die angeben, ob Workspace Control für jeden Web Receiver aktiviert ist (“True” oder “False”).
Remotezugriff für den Store aktiviert	Liste von Zeichenfolgen, die angeben, ob Remotezugriff für die Stores in der Bereitstellung aktiviert ist (“ENABLED” oder “DISABLED”).
Gateways	Anzahl der in der Bereitstellung konfigurierten Citrix Gateways.

Citrix Analytics-Dienst

Citrix Cloud-Kunden mit einer StoreFront-Bereitstellung im eigenen Rechenzentrum können StoreFront so konfigurieren, dass Daten an Citrix Analytics in Citrix Cloud gesendet werden. Bei entsprechender Konfiguration senden die Citrix Workspace-App und Citrix Receiver für Websites, sofern darauf über einen HTML5-kompatiblen Browser zugegriffen wird, Benutzerereignisse zur Verarbeitung an Citrix Analytics. Citrix Analytics aggregiert Kennzahlen zu Benutzern, Anwendungen,

Endpunkten, Netzwerken und Daten für detaillierte Einblicke in das Benutzerverhalten. Informationen zu diesem Feature finden Sie in der Citrix Analytics-Dokumentation unter Onboarding von Virtual Apps and Desktops-Sites mit StoreFront.

Führen Sie zum Konfigurieren dieses Verhaltens folgende Schritte aus:

- Laden Sie eine Konfigurationsdatei von Citrix Analytics herunter.
- Importieren Sie Citrix Analytics-Daten per PowerShell in Ihre StoreFront-Bereitstellung.

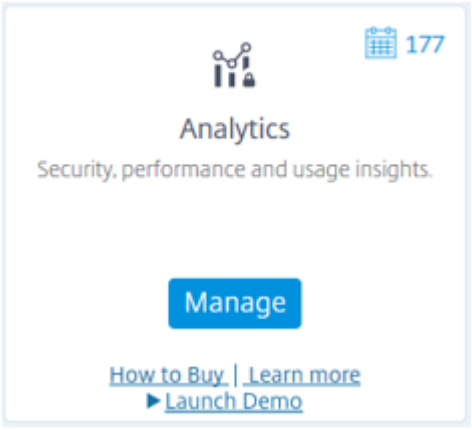
Nach dem Konfigurieren von StoreFront kann die Citrix Workspace-App Daten aus StoreFront-Stores senden, wenn dies von Citrix Analytics angefordert wird.

> **Wichtig:**
>
> Ihre StoreFront-Bereitstellung muss in der Lage sein, die folgenden Adressen über Port 443 zu kontaktieren, damit dieses Feature ordnungsgemäß funktioniert und Citrix Cloud-Dienste nutzen kann:
>
> - `https://*.cloud.com`
> - `https://*.citrixdata.com`

Herunterladen der Konfigurationsdatei von Citrix Analytics

> **Wichtig:**
>
> Für die Erstkonfiguration ist eine Konfigurationsdatei mit vertraulichen Informationen erforderlich. Schützen Sie die Datei nach dem Herunterladen vor unbefugtem Zugriff. Geben Sie die Datei nicht an Personen außerhalb Ihrer Organisation weiter. Nach der Konfiguration können Sie die Datei löschen. Wenn Sie die Konfiguration auf einem anderen Computer neu anwenden müssen, können Sie die Datei erneut über die Citrix Analytics-Dienstverwaltungskonsole herunterladen.

1. Melden Sie sich mit einem Administratorkonto bei Citrix Cloud (`https://citrix.cloud.com/`) an.
2. Wählen Sie einen Citrix Cloud-Kunden
3. Öffnen Sie die Citrix Analytics-Verwaltungskonsole, indem Sie auf **Manage** klicken.



4. Wählen Sie in der Citrix Analytics-Verwaltungskonsole **Settings > Data Source**.
5. Wählen Sie auf der Karte “Virtual App and Desktops” das Menüsymbol (⊠) und dann **Connect StoreFront deployment**.
6. Wählen Sie auf der Seite “Connect StoreFront Deployment” **Download File**, um die Datei *StoreFrontConfigurationFile.json* herunterzuladen.

Beispiel einer Konfigurationsdatei

```
{

  ”customerId”: ”<yourcloudcustomer>”,
  ”enablementService”: ” https://api.analytics.cloud.com /casvc/<
     yourcloudcustomer>/ctxana/v1/cas/<yourcloudcustomer>/XenDesktop/<
     deviceid>/dsconfigdata”,
  ”cwsServiceKey”: ”PFJTPn …… .. T4=”,
  ”enablementServiceStatus”: ” https://api.analytics.cloud.com /casvc/<
     yourcloudcustomer>/ctxana/v1/cas/storefront/config”,
  ”instanceId”: ”d98f21d0-56e0-11e9-ba52-5136d90862fe”,
  ”name”: ”CASSingleTenant”
 }
```

wobei

customerId ist die eindeutige ID des Citrix Cloud-Kunden.

cwsServiceKey ist ein eindeutiger Schlüssel zur Identifizierung des Citrix Cloud-Kundenkontos.

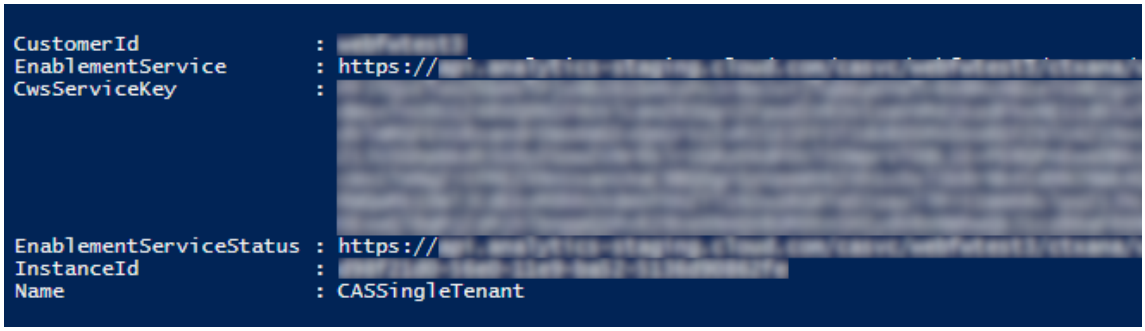
instanceID ist eine generierte ID, die zum Signieren von (sicheren) Anforderungen aus der Citrix Workspace-App an Citrix Analytics verwendet wird. Wenn Sie mehrere StoreFront-Server oder -Servergruppen bei Citrix Cloud registrieren, verfügt jeder/jede über eine eigene instanceID.

Importieren von Citrix Analytics-Daten in Ihre StoreFront-Bereitstellung

1. Kopieren Sie die Datei *StoreFrontConfigurationFile.json* in einen geeigneten Ordner auf dem lokalen StoreFront-Server (bzw. einem Server in einer StoreFront-Servergruppe). Die folgenden Befehle basieren auf einer Datei, die auf dem Desktop gespeichert ist.
2. Öffnen Sie PowerShell ISE, und wählen Sie **Als Administrator ausführen**.
3. Führen Sie die folgenden Befehle aus:

```
1 Import-STFCasConfiguration -Path ”$Env:UserProfile\Desktop\
     StoreFrontConfigurationFile.json”
2 Get-STFCasConfiguration
```

4. Dieser Befehl gibt eine Kopie der importierten Daten zurück und zeigt sie in der PowerShell-Konsole an.



> **Hinweis:**
>
> Für On-Premises-StoreFront-Server mit Windows Server 2012 R2 müssen die C++-Laufzeit-Softwarekomponenten evtl. manuell installiert werden, damit sie sich bei der ZS registrieren können. Wird StoreFront im Rahmen der Citrix Virtual Apps and Desktops-Installation installiert, ist dieser Schritt nicht erforderlich, da der Citrix Virtual Apps and Desktops-Metainstaller die C++-Laufzeitkomponenten installiert. Wird StoreFront nur mit dem CitrixStoreFront-x64.exe-Metainstaller ohne C++-Laufzeitumgebung installiert, kann es sich möglicherweise nicht bei Citrix Cloud registrieren, nachdem Sie die ZS-Konfigurationsdatei importiert haben.

Verteilen von Citrix Analytics-Daten an eine StoreFront-Servergruppe

Wenn Sie diese Aktionen an einer StoreFront-Servergruppe ausführen, müssen Sie die importierten Citrix Analytics-Daten an alle Mitglieder der Gruppe verteilen. Dieser Schritt ist bei Bereitstellungen mit nur einem StoreFront-Server nicht erforderlich.

Zur Verteilung der Daten gibt es folgende Möglichkeiten:

- Verwenden Sie die StoreFront-Verwaltungskonsole.
- Verwenden Sie das PowerShell-Cmdlet **Publish-STFServerGroupConfiguration**.

Prüfen der StoreFront-Servergruppen-ID

Um zu überprüfen, ob Ihre Bereitstellung erfolgreich bei Citrix Analytics registriert wurde, können Sie mithilfe von PowerShell die “ServerGroupID” für Ihre Bereitstellung erkennen lassen.

1. Melden Sie sich bei Ihrem StoreFront-Server oder bei einem StoreFront-Server in der Servergruppe an.
2. Öffnen Sie PowerShell ISE, und wählen Sie **Als Administrator ausführen**.
3. Führen Sie die folgenden Befehle aus:

```
$WebConfigPath = ”C:\Program Files\Citrix\Receiver StoreFront\
    Framework\FrameworkData\Framework.xml”
$XMLObject = (Get-Content $WebConfigPath) -as [Xml]
$XMLObject.framework.properties.property
```

   Diese Befehle erzeugen eine Ausgabe, die in etwa so aussieht:

```
name value
---- -----
ClusterId 8b8ff5c8-44ba-46e4-87f0-2df8cff31432
HostBaseUrl https://storefront.example.com/
SelectedIISWebSiteId 1
AdminConsoleOperationMode Full
```

Beenden der Datenübertragung aus StoreFront an Citrix Analytics

1. Öffnen Sie PowerShell ISE, und wählen Sie **Als Administrator ausführen**.
2. Führen Sie die folgenden Befehle aus:

   ```
   Remove-STFCasConfiguration
   ```

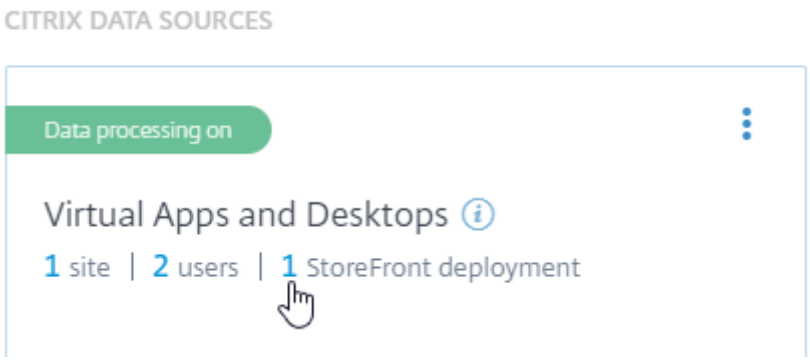
   ```
   Get-STFCasConfiguration
   ```

   Get-STFCasConfiguration gibt nichts zurück, wenn die zuvor importierten Citrix Analytics-Daten erfolgreich entfernt wurden.
3. Wenn Sie diese Aktionen an einer StoreFront-Servergruppe ausführen, verteilen Sie die Änderung zum Entfernen der Citrix Analytics-Daten von allen Mitgliedern der Gruppe. Führen Sie auf einem Server in der Servergruppe den folgenden Befehl aus:

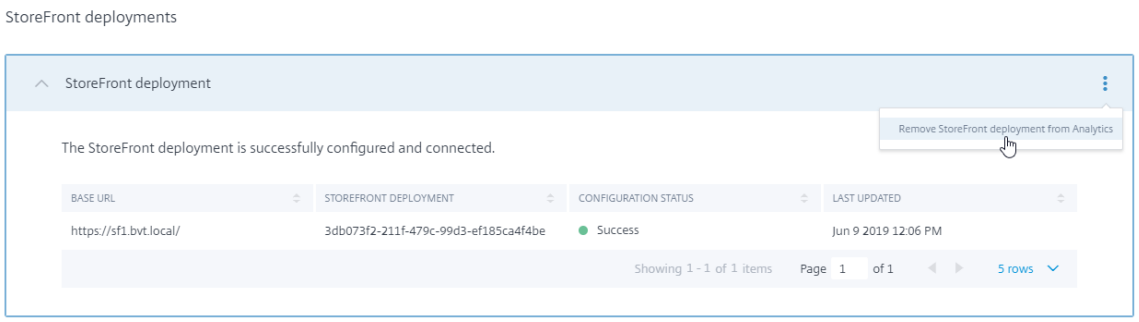
   ```
   Publish-STFServerGroupConfiguration
   ```
4. Führen Sie auf den anderen Mitgliedern der Servergruppe den folgenden Befehl aus, um zu prüfen, ob die Citrix Analytics-Konfiguration erfolgreich entfernt wurde:

   ```
   Get-STFCasConfiguration
   ```


5. Melden Sie sich mit einem Administratorkonto bei Citrix Cloud (`https://citrix.cloud.com/`) an.
6. Wählen Sie einen Citrix Cloud-Kunden
7. Öffnen Sie die Citrix Analytics-Verwaltungskonsole, indem Sie auf **Manage** klicken.
8. Wählen Sie in der Citrix Analytics-Verwaltungskonsole **Settings > Data Source**.
9. Wählen Sie auf der Karte "Virtual Apps and Desktops" die Anzahl der StoreFront-Bereitstellungen aus:



10. Identifizieren Sie die StoreFront-Bereitstellung, die Sie entfernen möchten, anhand der Host-Basis-URL und der ServerGroupID.
11. Wählen Sie im Menü (⊠) die Option **Remove StoreFront deployment from Analytics**.



> **Hinweis:**
>
> Wenn Sie die Konfiguration serverseitig entfernen, jedoch nicht aus Citrix Analytics, bleibt der StoreFront-Serverbereitstellungseintrag in Citrix Analytics, es werden jedoch keine Daten von StoreFront empfangen. Wenn Sie die Konfiguration nur aus Citrix Analytics entfernen, wird der StoreFront-Serverbereitstellungseintrag beim nächsten App-Pool-Recycle wieder hinzugefügt (bei einer IIS-Zurücksetzung oder automatisch alle 24 Stunden).

Konfigurieren von StoreFront für die Verwendung eines Webproxys zur Verbindung mit Citrix Cloud und Registrierung bei Citrix Analytics

Wenn StoreFront auf einem Hostwebserver hinter einem Webproxy ausgeführt wird, schlägt die Registrierung bei Citrix Analytics fehl. Wenn StoreFront-Administratoren einen HTTP-Proxy in ihrer Citrix Bereitstellung verwenden, muss der StoreFront-Datenverkehr in das Internet den Webproxy durchlaufen, bevor er Citrix Analytics in der Cloud erreicht. StoreFront verwendet nicht automatisch die Proxyeinstellungen des Hostbetriebssystems. Zusätzliche Konfiguration ist erforderlich, um den Store anzuweisen, ausgehenden Datenverkehr über den Webproxy zu senden. Sie können eine <system.net>-Proxykonfiguration erstellen, indem Sie der Datei web.config einen neuen Abschnitt hinzufügen. Tun Sie dies für jeden Store auf dem StoreFront-Server, der zum Senden von Daten an Citrix Analytics verwendet wird.

Methode 1: Festlegen der Proxykonfiguration über PowerShell für einen oder mehrere Stores (empfohlen)

Das Powershell-Skript “Config-StoreProxy.ps1” automatisiert diesen Prozess für einen oder mehrere Stores und fügt automatisch einen gültigen XML-Eintrag zum Konfigurieren von <system.net> ein. Das Skript sichert auch die web.config-Datei des Stores auf dem Desktop des aktuellen Benutzers, sodass sie bei Bedarf wiederhergestellt werden kann.

> **Hinweis:**
>
> Das mehrfache Ausführen des Skripts kann dazu führen, dass mehrere <system.net-XML-Einträge hinzugefügt werden. Jeder Store darf nur einen Eintrag für <system.net> haben. Das Hinzufügen mehrerer Einträge führt zur Fehlfunktion der Store-Proxykonfiguration.

1. Öffnen Sie die PowerShell ISE und wählen Sie **Als Administrator ausführen**.
2. Legen Sie `$Stores = @(”Store”,”Store2”)` fest, um die Stores einzuschließen, die Sie mit einem Webproxy konfigurieren möchten.
3. Geben Sie den Webproxy an über:
   - eine IP-Adresse ODER
   - einen FQDN
4. Führen Sie folgendes PowerShell-Skript aus:

```
$Stores = @(”Store”,”Store2”)
$ProxyIP = ”10.0.0.1”
$ProxyFQDN = ”proxyserver.example.com”
$ProxyPort = 8888

# Set this for every Store using Stores array
function Set-StoreProxyServer() # Tested with both IP and FQDN
```



```
8  {
9
10     [CmdletBinding()]
11     param([Parameter(Mandatory=$true,ParameterSetName="ProxyIP")][
           Parameter(Mandatory=$true,ParameterSetName="ProxyFQDN")][
           array]$Stores,
12         [Parameter(Mandatory=$true,ParameterSetName="ProxyIP")][
              string]$ProxyIP,
13         [Parameter(Mandatory=$true,ParameterSetName="ProxyFQDN")][
              string]$ProxyFQDN,
14         [Parameter(Mandatory=$true,ParameterSetName="ProxyIP")][
              Parameter(Mandatory=$true,ParameterSetName="ProxyFQDN")
              ][int]$ProxyPort)
15
16     foreach($Store in $Stores)
17     {
18
19         Write-Host "Backing up the Store web.config file for store
               $Store before making changes..." -ForegroundColor "
              Yellow"
20         Write-Host "`n"
21
22         if(!(Test-Path "$env:UserProfile\desktop$Store"))
23         {
24
25             Write-Host "Creating $env:UserProfile\desktop$Store\
                  directory for backup..." -ForegroundColor "Yellow"
26             New-Item -Path "$env:UserProfile\desktop$Store" -
                  ItemType "Directory" | Out-Null
27             Write-Host "`n"
28          }
29
30
31         Write-Host "Copying c:\inetpub\wwwroot\Citrix$Store\web.
              config to $env:UserProfile\desktop$Store..." -
              ForegroundColor "Yellow"
32         Copy-Item -Path "c:\inetpub\wwwroot\Citrix$Store\web.
              config" -Destination "$env:UserProfile\desktop$Store" -
              Force | Out-Null
33
34         if(Test-Path "$env:UserProfile\desktop$Store\web.config")
35         {
36
37             Write-Host "$env:UserProfile\desktop$Store\web.config
                  file backed up" -ForegroundColor "Green"
```



```
38          }
39
40          else
41          {
42
43              Write-Host "$env:UserProfile\desktop$Store\web.config
                    file NOT found!" -ForegroundColor "Red"
44          }
45
46          Write-Host "`n"
47
48          Write-Host "Setting the proxy server to $ProxyAddress for
                Store $Store..." -ForegroundColor "Yellow"
49          Write-Host "`n"
50
51          $StoreConfigPath = "c:\inetpub\wwwroot\Citrix$Store\web.
                config"
52          $XMLObject = (Get-Content $StoreConfigPath) -as [Xml]
53
54          if([string]::IsNullOrEmpty($ProxyFQDN))
55          {
56
57              $ProxyServer = ("HTTP://$ProxyIP"+":"+$ProxyPort)
58          }
59
60          else
61          {
62
63              $ProxyServer = ("HTTP://$ProxyFQDN"+":"+$ProxyPort)
64          }
65
66
67          $XMLObject = (Get-Content $StoreConfigPath) -as [Xml]
68
69          # Create 3 elements
70          $SystemNet = $XMLObject.CreateNode("element","system.net",
                "")
71          $DefaultProxy = $XMLObject.CreateNode("element","
                defaultProxy","")
72          $Proxy = $XMLObject.CreateNode("element","proxy","")
73          $Proxy.SetAttribute("proxyaddress","$ProxyServer")
74          $Proxy.SetAttribute("bypassonlocal","true")
75
76          # Move back up the XML tree appending new child items in
                reverse order
```

```
        $DefaultProxy.AppendChild($Proxy)
        $SystemNet.AppendChild($DefaultProxy)
        $XMLObject.configuration.AppendChild($SystemNet)

        # Save the modified XML document to disk
        $XMLObject.Save($StoreConfigPath)

        Write-Host "Getting the proxy configuration for c:\inetpub
            \wwwroot\Citrix$Store..." -ForegroundColor "Yellow"
        $XMLObject = (Get-Content $StoreConfigPath) -as [Xml]
        $ConfiguredProxyServer = $XMLObject.configuration.'system.
            net'.defaultProxy.proxy.proxyaddress | Out-Null
        Write-Host ("Configured proxy server for Store $Store"+":
            "+ $ConfiguredProxyServer) -ForegroundColor "Green"
        Write-Host "`n"
     }

    Write-Host "Restarting IIS..." -ForegroundColor "Yellow"
    IISReset /RESTART
 }


Set-StoreProxyServer -Stores $Stores -ProxyFQDN $ProxyFQDN -
    ProxyPort $ProxyPort
# OR
Set-StoreProxyServer -Stores $Stores -ProxyIP $ProxyIP -ProxyPort
    $ProxyPort
```

5. Überprüfen Sie, ob C:\inetpub\wwwroot\Citrix < Store>\web.config einen neuen<system.net >-Abschnitt am Dateiende enthält.

```
        </dependentAssembly>
    </assemblyBinding>
</runtime>
<system.net>
    <defaultProxy>
    <proxy proxyaddress="HTTP://proxyserver.example.com:8888"
        bypassonlocal="true" />
    </defaultProxy>
</system.net>
</configuration>
```

6. Importieren Sie die Citrix Analytics-Daten wie unter Importieren von Citrix Analytics-Daten in Ihre StoreFront-Bereitstellung beschrieben.

Methode 2: Manuelles Hinzufügen eines `<system.net>`-Abschnitts zur web.config-Datei

Dieses Verfahren muss für jeden Store auf dem StoreFront-Server ausgeführt werden, der zum Senden von Daten an Citrix Analytics verwendet wird.

1. Sichern Sie die Datei web.config für den Store und kopieren Sie sie an einen anderen Speicherort außerhalb von C:\inetpub\wwwroot\Citrix< Store>\web.config.
2. Ändern Sie den folgenden XML-Eintrag unter Verwendung Ihrer Proxyeinstellungen entweder unter Angabe von FQDN-und-Port oder von IP-und-Port.

   Für FQDN-und-Port verwenden Sie beispielsweise das folgende <system.net>-Element:

   ```
   <system.net>
       <defaultProxy>
       <proxy proxyaddress="HTTP://proxyserver.example.com:8888"
          bypassonlocal="true" />
       </defaultProxy>
   </system.net>
   ```

   Für IP-und-Port verwenden Sie beispielsweise das folgende <system.net>-Element:

   ```
   <system.net>
       <defaultProxy>
       <proxy proxyaddress="HTTP://10.0.0.1:8888" bypassonlocal="true
          " />
       </defaultProxy>
   </system.net>
   ```

3. Fügen Sie am Ende der Datei web.config das <system.net>-Element wie hier gezeigt ein:

   ```
   <runtime>
   <gcServer enabled="true" />
   <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
       <dependentAssembly>
       <assemblyIdentity name="System.Web.MVC" publicKeyToken="31
          BF3856AD364E35" culture="neutral" />
       <bindingRedirect oldVersion="0.0.0.0-5.0.0.0" newVersion="
          5.0.0.0" />
       </dependentAssembly>
       <dependentAssembly>
       <assemblyIdentity name="Newtonsoft.Json" publicKeyToken="30
          ad4fe6b2a6aeed" culture="neutral" />
       <bindingRedirect oldVersion="0.0.0.0-9.0.0.0" newVersion="
          9.0.0.0" />
       </dependentAssembly>
   </assemblyBinding>
   ```



```
</runtime>

Insert the <system.net> element here

</configuration>
```

4. Importieren Sie die Citrix Analytics-Daten wie unter Importieren von Citrix Analytics-Daten in Ihre StoreFront-Bereitstellung beschrieben.

Aktualisieren von StoreFront

> **Warnung:**
>
> Wenn Sie ein Upgrade auf StoreFront 1912 ausführen, werden alle Desktopgerätesites in der Bereitstellung automatisch entfernt. Wenn Sie Desktopgerätesites beibehalten müssen, führen Sie kein Upgrade durch. Als Alternative empfiehlt Citrix die Verwendung der Citrix Workspace-App Desktop Lock für alle Anwendungsfälle ohne Domänenbindung.

Beim Upgrade bleibt die StoreFront-Konfiguration unverändert. Darüber hinaus bleiben die Anwendungsabonnementdaten erhalten, sodass die Benutzer nicht alle ihre Anwendungen neu abonnieren müssen. Im Gegensatz dazu werden beim Deinstallieren von StoreFront auch StoreFront und die zugehörigen Dienste, Sites, Anwendungsabonnementdaten (auf eigenständigen Servern) und die zugehörige Konfiguration entfernt.

Nützliche Info

- 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.
- Ein Upgrade auf die aktuelle StoreFront-Version von einer älteren Version, die jetzt das Ende des Lebenszyklus erreicht hat, wird nicht unterstützt. Weitere Informationen finden Sie unter CTX200356.
- StoreFront unterstützt keine Multiserverbereitstellung mit mehreren Produktversionen. Daher müssen alle Server einer Gruppe auf dieselbe Version aktualisiert werden, bevor Zugriff auf die Bereitstellung erteilt wird.
- StoreFront unterstützt keine Bereitstellung mit mehreren Servern, auf denen unterschiedliche Betriebssysteme ausgeführt werden. Auf allen Servern in einer Servergruppe muss dasselbe Windows Server-Betriebssystem ausgeführt werden.
- Ein Upgrade aller Server in Bereitstellungen mit mehreren Servern in einem Arbeitsgang wird nicht unterstützt. Die Server müssen nacheinander aktualisiert werden.

- Alle Stores, die die klassische Benutzeroberfläche verwenden, werden auf die einheitliche Benutzeroberfläche aktualisiert, wenn Sie ein Upgrade auf diese StoreFront-Version durchführen. Citrix empfiehlt, dass Sie die Benutzer über die neue Benutzeroberfläche (siehe Einheitliche Benutzeroberfläche) informieren. Wenn Sie die einheitliche Benutzeroberfläche angepasst haben, bleiben Ihre Anpassungen beim Upgrade auf diese StoreFront-Version erhalten. Überprüfen Sie, dass das Erscheinungsbild Ihrer Anpassungen mit der neuen vereinheitlichten Benutzeroberfläche weiterhin richtig ist.
- Bevor das StoreFront-Upgrade ausgeführt wird, erfolgen mehrere Prüfungen. Wird eine nicht bestanden, dann wird das Upgrade nicht gestartet und Sie werden über den Fehler benachrichtigt. Die StoreFront-Installation bleibt unverändert. Führen Sie nach dem Beheben des Fehlers das Upgrade erneut aus.
- Wenn das StoreFront-Upgrade selbst fehlschlägt, geht die ursprüngliche Konfiguration der StoreFront-Installation u. U. verloren. Stellen Sie die StoreFront-Installation in einen funktionierenden Zustand wieder her und führen Sie das Upgrade erneut aus. Zum Wiederherstellen von StoreFront gibt es folgende Möglichkeiten:
  - Wiederherstellen des VM-Snapshots, den Sie vor dem Upgrade erstellt haben
  - Importieren der StoreFront-Konfiguration, die Sie vor dem Upgrade exportiert haben (siehe Exportieren und Importieren der StoreFront-Konfiguration)
  - Durchführung der Anleitung zur Fehlerbehebung unter Behandlung von StoreFront-Upgradeproblemen
- Alle StoreFront-Upgradefehler im Citrix Virtual Apps and Desktops-Metainstaller werden in einem Dialogfeld mit einem Link zum entsprechenden Fehlerprotokoll gemeldet.

Vorbereitung des Upgrades

Citrix empfiehlt die Durchführung folgender Schritte vor einem Upgrade, um Fehlern beim Upgrade vorzubeugen:

- Planen Sie die Sicherung vor dem Upgrade.
- Schließen Sie alle anderen Anwendungen auf dem StoreFront-Server.
- Schließen Sie die StoreFront-Verwaltungskonsole.
- Schließen Sie alle Befehlszeilen- und PowerShell-Fenster.
- Schließen Sie alle StoreFront-relevanten Ordner wie C:\inetpub\wwwroot\Citrix\Store und C:\inetpub\wwwroot\Citrix\StoreWeb. Dadurch wird verhindert, dass die Ordner durch Windows Explorer gesperrt werden.
- Starten Sie vor einem Serverupgrade den Server neu, um sicherzustellen, dass keine exklusiven Sperren für StoreFront-Dateien oder -Ordner vorhanden sind. (Der Neustart des Explorer-Prozesses, z. B. durch Schließen aller Instanzen von Windows-Explorer, ist *nicht* ausreichend).
- Führen Sie das Upgrade sofort aus, ohne andere Programme auf dem Server zu starten.

- Verwenden Sie zum Durchführen des Serverupgrades ein Administratorkonto, das keine anderen Installationen ausführt und möglichst wenige andere Anwendungen geöffnet hat.

Upgrade eines eigenständigen StoreFront-Servers

1. Trennen Sie alle Benutzerverbindungen mit der StoreFront-Bereitstellung, damit die Benutzer während des Upgrades nicht auf die Server zugreifen. So wird sichergestellt, dass das Installationsprogramm während des Upgrades auf alle StoreFront-Dateien zugreifen kann. Kann das Installationsprogramm auf eine Datei nicht zugreifen, dann wird diese nicht ersetzt und das Upgrade schlägt fehl, wodurch die vorhandene StoreFront-Konfiguration entfernt wird.
2. Sichern Sie den Server, indem Sie einen VM-Snapshot erstellen.
3. Exportieren der StoreFront-Konfiguration (empfohlen).
4. Führen Sie die Installationsdatei dieser Version von StoreFront aus.

Upgrade einer StoreFront-Servergruppe

Beim Upgrade von StoreFront-Servergruppen wird ein Server verwendet, um die anderen Server aus der Gruppe zu entfernen. Die entfernten Server behalten die mit der Gruppe zusammenhängende Konfiguration bei, wodurch verhindert werden kann, dass sie einer neuen Servergruppe hinzugefügt werden. Bevor sie zum Erstellen neuer Servergruppen oder als eigenständige StoreFront-Server wiederverwendet werden können, müssen sie auf die Werkseinstellungen zurückgesetzt oder StoreFront muss neu auf ihnen installiert werden.

Vor dem Upgrade einer Servergruppe:

- Sichern Sie alle Server in der Servergruppe durch Erstellen von VM-Snapshots. Auf diese Weise können Sie schnell eine funktionierende Servergruppe mit drei Knoten wiederherstellen, wenn das Upgrade nicht wie geplant läuft.
- Exportieren der StoreFront-Konfiguration (empfohlen). Exportieren Sie die Servergruppenkonfiguration nur von einem Server. Sofern Sie alle Änderungen zwischen den Servern einer Gruppe verteilt haben, ist die Konfiguration auf allen identisch. Mithilfe dieser Sicherung können Sie problemlos eine neue Servergruppe erstellen.

Beispiel 1: Upgrade einer StoreFront-Servergruppe mit drei Knoten während der geplanten Wartung

Beschrieben wird das Upgrade einer StoreFront-Servergruppe mit den Servern A, B und C während einer geplanten Wartungsdowntime.

1. Deaktivieren Sie den Benutzerzugriff auf die Servergruppe, indem Sie die Lastausgleichs-URL deaktivieren. Dadurch wird verhindert, dass Benutzer während des Upgrades eine Verbindung mit der Bereitstellung herstellen.
2. Verwenden Sie Server A, um Server B und C aus der Gruppe zu entfernen.

   Server B und C sind nun kein Teil der Servergruppe mehr.
3. Führen Sie auf Server A die Installationsdatei dieser Version von StoreFront aus.
4. Stellen Sie sicher, dass Server A erfolgreich aktualisiert wurde.
5. Deinstallieren Sie auf den Servern B und C StoreFront und installieren Sie die neue StoreFront-Version.
6. Verbinden Sie die Server B und C mit Server A, um eine aktualisierte Servergruppe zu erstellen. Die Servergruppe besteht aus einem aktualisierten Server (A) und zwei neu installierten Servern (B und C).

   Der Prozess Beitreten zu einer vorhandenen Servergruppe verteilt automatisch alle Konfigurationsdaten und Abonnementdaten auf die neuen Server B und C.
7. Überprüfen Sie, ob alle Server ordnungsgemäß funktionieren.
8. Aktivieren Sie den Benutzerzugriff auf die aktualisierte Servergruppe, indem Sie die Lastausgleichs-URL aktivieren.

Beispiel 2: Upgrade einer StoreFront-Servergruppe mit drei Knoten ohne geplante Wartung

Beschrieben wird das Upgrade einer StoreFront-Servergruppe mit den Servern A, B und C ohne geplante Wartungsdowntime.

Vor dem Upgrade einer Servergruppe:

1. Exportieren Sie Abonnementdaten von Server A unter Verwendung von **Export-STFStoreSubscriptions**. Diese Sicherung ist notwendig, da die Server später auf die Werkseinstellungen zurückgesetzt werden, wodurch Abonnement- und Konfigurationsdaten gelöscht werden. Siehe Verwalten von Abonnementdaten für einen Store.
2. Deaktivieren Sie den Benutzerzugriff auf Server C, indem Sie den Lastausgleichsdienst für Server C deaktivieren. Dadurch wird verhindert, dass Benutzer während des Upgrades eine Verbindung mit Server C herstellen. Lassen Sie den Lastausgleich für Server A und B aktiviert, damit die Benutzer diese Server weiterhin verwenden können.
3. Verwenden Sie Server A, um Server C aus der Gruppe zu entfernen.
   Server A und B bieten weiterhin Zugriff auf die Ressourcen für die Benutzer. Server C ist nun aus der Servergruppe entfernt und wird auf die Werkseinstellungen zurückgesetzt.
4. Verwenden Sie zum Zurücksetzen von Server C auf die Werkseinstellungen **Clear-STFDeployment**.

5. Importieren Sie die StoreFront-Konfiguration, die Sie zuvor exportiert hatten, mit **Import-STFConfiguration** auf Server C.
6. Führen Sie auf Server C die Installationsdatei dieser Version von StoreFront aus. Server C hat nun dieselbe Konfiguration wie die alte Servergruppe und wurde auf die neue StoreFront-Version aktualisiert.
7. Importieren Sie die Abonnementdaten, die Sie zuvor exportiert hatten, auf Server C. Dieser Schritt muss später *nicht* wiederholt werden. Die Abonnementdaten müssen nur auf einem Server vorliegen, von wo aus sie auf andere Server verteilt werden, die der Gruppe beitreten.
8. Wiederholen Sie die Schritte 2 bis 6 mit Server B. Während dieser Zeit bietet nur Server A Benutzern Zugriff auf Ressourcen. Es empfiehlt sich daher, diesen Schritt zu einer Zeit auszuführen, zu der die StoreFront-Servergruppe nur minimal ausgelastet ist.
9. Verbinden Sie Server B mit Server C über den Prozess Beitreten zu einer vorhandenen Servergruppe. Damit erhalten Sie eine Einzelserverbereitstellung für die aktuelle StoreFront-Version (Server A) und eine neue Servergruppe mit zwei Knoten in der neuen StoreFront-Version (Server B und C).
10. Aktivieren Sie den Lastausgleich für Server B und C, damit diese die Arbeit von Server A übernehmen können.
11. Deaktivieren Sie den Lastausgleich für Server A, damit die Benutzer auf die aktualisierten Server B und C weitergeleitet werden.
12. Wiederholen Sie die Schritte 2 bis 6 mit Server A.
    Das Upgrade der Servergruppe ist damit abgeschlossen. Server A, B und C verfügen über identische Konfigurations- und Abonnementdaten aus der ursprünglichen Gruppe.

> **Hinweis:**
>
> Während des kurzen Zeitraums, in dem Server A der einzige zugängliche Server ist, können Abonnementdaten verloren gehen (Schritt 9). Dies kann dazu führen, dass die neue Servergruppe nach dem Upgrade eine leicht veraltete Kopie der Abonnementdatenbank hat und jegliche neuen Abonnementdatensätze verloren gehen.
>
> Dies hat keine Auswirkungen auf die Funktion, da Abonnementdaten nicht unbedingt benötigt werden, damit die Benutzer sich anmelden und Ressourcen starten können. Die Benutzer müssen in diesem Fall jedoch eine Ressource erneut abonnieren, wenn Server A auf die Werkseinstellungen zurückgesetzt und der neu aktualisierten Gruppe hinzugefügt wurde. Es gehen zwar in den allermeisten Fällen nur wenige Abonnementdatensätze verloren, dies ist jedoch als mögliche Folge eines Upgrades in einer aktiven StoreFront-Produktionsumgebung zu bedenken.

Konfigurieren von StoreFront

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

- Erstellen einer Bereitstellung. 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.
- Beitreten zu einer vorhandenen Servergruppe. 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. Citrix empfiehlt, einer Servergruppe maximal 6 Server hinzuzufügen.

Deinstallieren Sie StoreFront

Neben dem Produkt selbst werden bei der Deinstallation von StoreFront der Authentifizierungsdienst, die Stores, Citrix Receiver für Web-Sites sowie XenApp Services-URLs und die zugeordneten Konfigurationen entfernt. Der Abonnementstoredienst, der die Anwendungsabonnementdaten der Benutzer enthält, wird ebenfalls gelöscht. Bei Einzelserverbereitstellungen gehen die Details zu den Anwendungsabonnements der Benutzer daher verloren. Bei Multiserverbereitstellungen werden diese Daten jedoch auf den anderen Servern der Gruppe beibehalten. Erforderliche Komponenten, 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. Schließen Sie die StoreFront-Verwaltungskonsole, wenn diese geöffnet ist.
3. Schließen Sie alle PowerShell-Sitzungen, mit denen Sie ggf. StoreFront verwaltet haben.
4. Navigieren Sie auf der Windows-Startseite oder auf der **Apps**-Seite zur Kachel **Citrix StoreFront**. Klicken Sie mit der rechten Maustaste auf die Kachel und klicken Sie auf **Deinstallieren**.
5. Wählen Sie im Dialogfeld **Programme und Funktionen Citrix StoreFront** aus und klicken Sie auf **Deinstallieren**, um alle StoreFront-Komponenten vom Server zu entfernen.
6. Klicken Sie im Dialogfeld **Citrix StoreFront deinstallieren** auf **Ja**. Wenn die Deinstallation abgeschlossen ist, klicken Sie auf **OK**.

Erstellen einer neuen Bereitstellung

April 1, 2020

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.
4. Klicken Sie auf **Weiter**, um den Authentifizierungsdienst zur Authentifizierung von Benutzern bei Microsoft Active Directory einzurichten.

   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 die Citrix Workspace-App 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.

   Sie können mit **Basis-URL ändern** in der StoreFront-Verwaltungskonsole jederzeit von HTTP zu HTTPS wechseln, vorausgesetzt, dass die Microsoft-Internetinformationsdienste (IIS) für HTTPS konfiguriert sind.
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 der Citrix Workspace-App unter den Konten der Benutzer. Wählen Sie daher einen Namen, anhand dessen die Benutzer den Inhalt des Stores erkennen können.

6. Listen Sie auf der Seite **Delivery 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 unter Hinzufügen von Citrix Virtual Apps and Desktops-Ressourcen zum Store beschriebene Verfahren. Sie können Stores konfigurieren, die Ressourcen aus einer beliebigen Zusammenstellung von Citrix Virtual Apps and Desktops-Bereitstellungen bieten. Wiederholen Sie die Verfahren bei Bedarf, um alle Bereitstellungen, von Ressourcen für den Store hinzuzufügen.
7. Wenn Sie dem Store alle erforderlichen Ressourcen hinzugefügt haben, klicken Sie auf der Seite **Delivery Controller** auf **Weiter**.
8. Geben Sie auf der Seite **Remotezugriff** an, ob und wie Benutzer, die eine Verbindung aus einem öffentlichen Netzwerk herstellen, auf interne Ressourcen zugreifen können:
   - Soll der Store Benutzern in öffentlichen Netzwerken zur Verfügung stehen, aktivieren Sie die Option **Remotezugriff aktivieren**. 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 Citrix Gateway verfügbar machen möchten, wählen Sie **Benutzern nur Zugriff auf Ressourcen geben, die über StoreFront bereitgestellt werden (kein VPN-Tunnel)**. Die Benutzer melden sich entweder über ICAProxy oder ein clientloses VPN (CVPN) bei Citrix Gateway an und benötigen das Citrix Gateway-Plug-In nicht für ein vollständiges VPN.
   - 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)**. Die Benutzer benötigen das Citrix Gateway-Plug-In für das Erstellen des VPN-Tunnels.

   Wenn Sie Remotezugriff auf den Store konfigurieren, wird automatisch die **Passthrough-Authentifizierung von Citrix Gateway** aktiviert. Die Benutzer authentifizieren sich bei Citrix Gateway und werden beim Zugriff auf ihre Stores automatisch angemeldet.
9. Wenn Sie Remotezugriff aktiviert haben, werden in der Liste **Citrix Gateway-Geräte** die Bereitstellungen angezeigt, über die die Benutzer auf den Store zugreifen können. Folgen Sie zum Hinzufügen einer Citrix Gateway-Bereitstellung zur Liste den Anweisungen unter Konfigurieren des Remotezugriffs auf den Store über ein Citrix Gateway-Gerät. Wiederholen Sie ggf. die Schritte, um weitere Bereitstellungen hinzuzufügen.
10. Wählen Sie in der Liste **Citrix Gateway-Geräte** die Bereitstellungen aus, über die die Benutzer auf den Store zugreifen können. Wenn Sie Zugriff über mehrere Bereitstellungen aktivieren, geben Sie das **Standardgerät** für den Zugriff auf den Store an. Klicken Sie auf **Weiter**.
11. Wählen Sie auf der Seite **Authentifizierungsmethoden** die Methoden, die Benutzer zum Authentifizieren und Zugreifen auf den Store verwenden, 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 einem Identitätsanbieter und werden beim Zugriff auf ihre Stores automatisch angemeldet.
- **Domänen-Passthrough-Authentifizierung**: Die 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.
- **HTTP Basic**: Benutzer authentifizieren sich über den IIS-Webserver des StoreFront-Servers.
- **Passthrough-Authentifizierung von Citrix Gateway**: Die Benutzer authentifizieren sich bei Citrix Gateway und werden beim Zugriff auf ihre Stores automatisch angemeldet. Diese Option wird automatisch aktiviert, wenn Remotezugriff aktiviert wird.1. Wählen Sie auf der Seite **Kennwortvalidierung konfigurieren** die Delivery Controller, die die Kennwortvalidierung bereitstellen, und klicken Sie auf **Weiter**.

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 unter Konfigurieren und Verwalten von Stores.

Der Store steht jetzt für den Zugriff durch Benutzer über die Citrix Workspace-App 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 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 5 angegebene Name.

Zum schnellen Hinzufügen weiterer Server wählen Sie die Option zum Beitreten zu einer vorhandenen Servergruppe, wenn Sie weitere Instanzen von StoreFront installieren.

Hinzufügen von Citrix Virtual Apps and Desktops-Ressourcen zum Store

Führen Sie die folgenden Schritte aus, um von Citrix Virtual Apps and Desktops 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. 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**.
2. Geben Sie im "Dialogfeld Delivery Controller hinzufügen" einen **Anzeigenamen** an, über den Sie die Bereitstellung identifizieren können, und wählen Sie unter **Typ** aus, wie die Ressourcen, die Sie über den Store verfügbar machen möchten, bereitgestellt werden. Der Typ ist standardmäßig auf Citrix Virtual Apps and Desktops festgelegt. XenApp 6.5 steht als Typ zur Auswahl, hat jedoch im Juni 2018 das Ende des Lebenszyklus erreicht und wird jetzt vom Extended Support-Programm abgedeckt.
3. Um Desktops und Anwendungen, die von Citrix Virtual Apps and Desktops und XenApp 6.5 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 Citrix Virtual Apps and Desktops-Sites Details der Delivery Controller an. Listen Sie für XenApp 6.5-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 TLS (Transport Layer Security) zu senden. Wenn Sie diese Option für Citrix Virtual Apps and Desktops-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 6.5-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 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 dem Server verwenden soll. Der Standardport ist 80 für Verbindungen über HTTP und SSL-Relay bzw. 443 für HTTPS-Verbindungen. Bei Citrix Virtual Apps and Desktops-Servern muss der angegebene Port dem vom Citrix XML-Dienst verwendeten Port entsprechen.
6. Wenn Sie SSL-Relay verwenden, um Verbindungen zwischen StoreFront und dem XenApp 6.5-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.
7. Klicken Sie auf **OK**. Sie können Stores konfigurieren, die Ressourcen aus einer beliebigen Zusammenstellung von Citrix Virtual Apps and Desktops-Bereitstellungen bieten. Zum Hinzufügen weiterer Citrix Virtual Desktops-Sites oder Citrix Virtual Apps-Farmen wiederholen Sie das obige 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 Citrix Gateway-Gerät

Führen Sie die folgenden Schritte aus, um Remotezugriff über ein Citrix 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 in der StoreFront-Verwaltungskonsole auf der Seite **Remotezugriff** des Dialogfelds “Store erstellen” auf **Hinzufügen**.
2. Geben im Dialogfeld **Citrix Gateway-Gerät hinzufügen** auf der Seite **Allgemeine Einstellungen** einen Anzeigenamen für das Citrix Gateway-Gerät an, über den die Benutzer dieses identifizieren können.

   Den Benutzern wird der Anzeigename angezeigt, den Sie in der Citrix Workspace-App angegeben haben. Nehmen Sie deshalb relevante Informationen in den Namen auf, damit die Benutzer leichter entscheiden können, ob sie das Gateway verwenden möchten. Beispielsweise können Sie den geographischen Standort in die Anzeigenamen der Citrix Gateway-Bereitstellungen einfügen, damit Benutzer problemlos das nächstgelegene Gateway für ihren Standort identifizieren können.
3. Geben Sie für **Citrix Gateway-URL** die URL:Port-Kombination des virtuellen Citrix Gateway-Servers Ihrer Bereitstellung ein. Wird kein Port angegeben, wird der Standard-`https://`-Port 443 verwendet. Port 443 muss in der URL nicht angegeben werden.

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. Wählen Sie aus den verfügbaren Optionen die **Verwendung oder Rolle** des Citrix Gateways aus.
   - **Authentifizierung und HDX-Routing:** Das Citrix Gateway wird für die Authentifizierung und das Routing von HDX-Sitzungen verwendet.
   - **Nur Authentifizierung:** Das Citrix Gateway wird nur für die Authentifizierung, jedoch nicht für das HDX-Sitzungsrouting verwendet.
   - **Nur HDX-Routing:** Das Citrix Gateway wird für das HDX-Routing, nicht aber für die Authentifizierung verwendet.
5. Fügen Sie für alle Bereitstellungen, in denen Sie Ressourcen von Citrix Virtual Apps and Desktops oder XenApp 6.5 im Store verfügbar machen, auf der Seite **Secure Ticket Authority** die **STA-URLs** für Server hinzu, 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 Citrix Virtual Apps and Desktops- bzw. XenApp 6.5-Servern gehostet und gibt Sitzungstickets als Reaktion auf Verbindungsanforderungen aus. Auf diesen Sitzungstickets basiert die Authentifizierung und Autorisierung für den Zugriff auf Citrix Virtual Apps and Desktops- bzw. XenApp 6.5-Ressourcen. Verwenden Sie die richtige STA URL (`HTTPS://` oder `HTTP://`) je nachdem, wie Ihre Delivery Controller konfiguriert sind. Die STA URL muss mit der in Citrix Gateway auf dem virtuellen Server konfigurierten URL identisch sein.
6. Um sicherzustellen, dass Citrix Virtual Apps and Desktops bzw. XenApp 6.5 getrennte Sitzungen aufrechterhält, während die Citrix Workspace-App eine automatische Wiederverbindung versucht, wählen Sie **Sitzungszuverlässigkeit aktivieren**.
7. Aktivieren Sie **Tickets von zwei Secure Ticket Authoritys anfordern (falls verfügbar)**, wenn Sie mehrere STAs konfigurieren und sicherstellen möchten, dass Sitzungszuverlässigkeit immer gegeben ist. StoreFront ruft dann Tickets von zwei verschiedenen Secure Ticket Authoritys ab und Benutzersitzungen werden nicht unterbrochen, 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. Geben Sie auf der Seite **Authentifizierungseinstellungen** die **vServer-IP-Adresse** (VIP) des Citrix Gateway-Geräts ein.

   Verwenden Sie die private IP-Adresse des virtuellen Citrix Gateway-Servers und nicht die öffentliche, die der privaten per Netzwerkadressübersetzung zugeordnet ist. Gateways werden von StoreFront normalerweise über ihre URL identifiziert. Wenn Sie Global Server Load Balanc-

ing (GSLB) verwenden, müssen Sie die VIP jedem Gateway hinzufügen. Dadurch kann StoreFront mehrere Gateways identifizieren, die alle dieselbe URL (GSLB-Domänennamen) als separate Gateways verwenden. Beispielsweise können für den Store drei Gateways mit der URL `https://gslb.domain.com` konfiguriert werden, jedes hat jedoch eine eindeutige VIP (z. B. 10.0.0.1, 10.0.0.2 und 10.0.0.3).

9. Wenn Sie ein Gerät mit Citrix Gateway hinzufügen, wählen Sie aus der Liste **Anmeldetyp** die Authentifizierungsmethode aus, die Sie auf dem Gerät für Benutzer der Citrix Workspace-App konfiguriert haben.

    - 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** 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**.

10. Wenn Sie StoreFront für Citrix Gateway konfigurieren und SmartAccess verwenden möchten, müssen Sie eine **Callback-URL** eingeben. StoreFront fügt automatisch den Standardteil der URL an. Geben Sie die intern zugängliche URL des Geräts ein. StoreFront kontaktiert den Citrix Gateway-Authentifizierungsdienst, um zu überprüfen, ob von Citrix Gateway empfangene Anforderungen auch tatsächlich von diesem Gerät ausgehen.

    Bei Verwendung von GSLB empfiehlt es sich, eine eindeutige Callback-URL für jedes GSLB-Gateway zu konfigurieren. StoreFront muss jede eindeutige Callback-URL in die private VIP auflösen können, die für den jeweiligen virtuellen GSLB-Gateway-Server konfiguriert ist. Beispielsweise müssen `emeagateway.domain.com`, `usgateway.domain.com` und `apacgateway.domain.com` in die korrekte Gateway-VIP aufgelöst werden.

11. Klicken Sie auf **Erstellen**, um das Citrix Gateway-Gerät der Liste im Dialogfeld **Remotezugriffeinstellungen** hinzuzufügen.

    Die Informationen zur Konfiguration von Citrix Gateway-Geräten werden der CR-Provisioningdatei für den Store hinzugefügt. Dadurch kann die Citrix Workspace-App die richtige Verbindungsanforderung senden, wenn ein Gerät zum ersten Mal kontaktiert wird.

12. Kehren Sie zu Schritt 10 unter “Neue Bereitstellung erstellen” weiter oben zurück.

Vorhandener Servergruppe beitreten

September 10, 2019

Eine Servergruppe kann maximal fünf Server enthalten. Allerdings bieten basierend auf Simulationen Servergruppen mit mehr als drei Servern für die Kapazität keinen Vorteil.

Bevor Sie StoreFront auf einem Server installieren, den Sie der Gruppe hinzufügen möchten, stellen Sie Folgendes sicher:

- Auf dem Server, den Sie der Gruppe hinzufügen, muss die gleiche Betriebssystemversion mit dem gleichen Gebietsschema ausgeführt werden, wie auf den anderen Servern in der Gruppe. StoreFront-Servergruppen mit unterschiedlichen Betriebssystemversionen und Gebietsschemas werden nicht unterstützt.
- Der relative Pfad zu StoreFront in IIS auf dem Server, den Sie hinzufügen, muss mit dem auf den anderen Servern in der Gruppe identisch sein.

Wurde der StoreFront-Server zuvor aus einer Servergruppe entfernt, kann er erst dann wieder zur gleichen oder einer anderen Servergruppe hinzugefügt werden, wenn Sie ihn auf die werkseitigen Standardeinstellungen zurückgesetzt haben. Siehe Zurücksetzen eines Servers auf die Werkseinstellungen

> **Wichtig:**
>
> 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 beitreten 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.

Zurücksetzen eines Servers auf die Werkseinstellungen

June 12, 2019

Es kann notwendig werden, eine StoreFront-Installation auf den ursprünglichen Installationsstatus zurückzusetzen. Das ist beispielsweise dann erforderlich, wenn Sie einen StoreFront-Server einer Servergruppe erneut hinzufügen möchten.

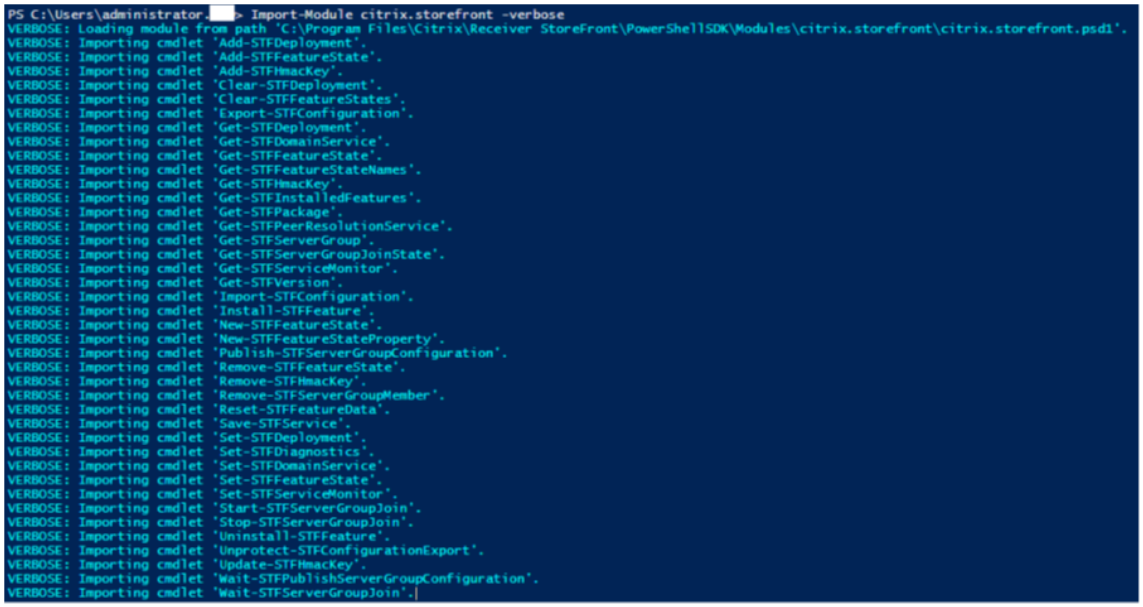
Eine manuelle Deinstallation und Neuinstallation ist zwar möglich, dies ist jedoch zeitaufwändiger und kann unvorhergesehene Probleme verursachen. Stattdessen können Sie das PowerShell-Cmdlet **Clear-STFDeployment** ausführen, um den StoreFront-Server auf die werkseitigen Standardeinstellungen zurückzusetzen.

1. Stellen Sie sicher, dass die StoreFront-Verwaltungskonsole geschlossen ist.
2. Öffnen Sie PowerShell ISE, und wählen Sie **Als Administrator ausführen**.
3. Legen Sie den PowerShell-Pfad fest:

```
1 $env:PSModulePath = [Environment]::GetEnvironmentVariable('
    PSModulePath','Machine')
```

4. Importieren Sie das Citrix StoreFront-Modul.

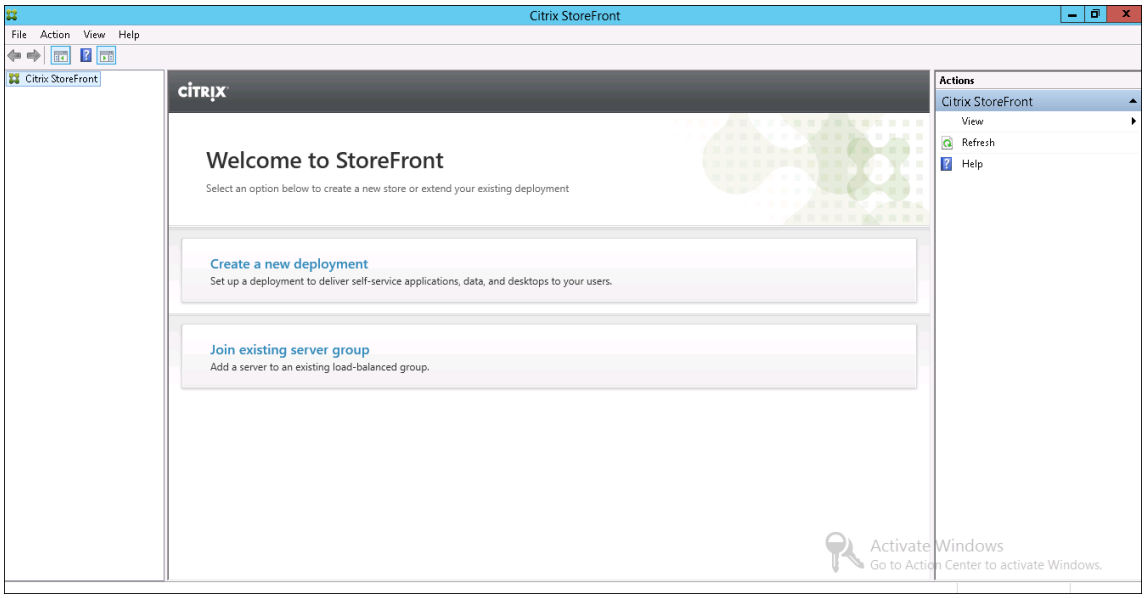
```
1 Import-Module citrix.storefront -verbose
```

5. Führen Sie nach dem Importieren des Moduls den Befehl **Clear-STFDeployment** aus, um den StoreFront-Server auf die Standardeinstellungen zurückzusetzen:

```
1 Clear-STFDeployment -Confirm $False
```

6. Wenn der Befehl erfolgreich ausgeführt wurde, öffnen Sie die StoreFront-Verwaltungskonsole, und stellen Sie sicher, dass alle Einstellungen zurückgesetzt wurden. Die Optionen **Neue Bereitstellung erstellen** bzw. **Vorhandener Servergruppe beitreten** stehen zur Verfügung.



Migrieren von Webinterface-Features nach StoreFront

January 6, 2020

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 kompletten Grafikinhalt, Auswahl durch Benutzer	Nicht verfügbar StoreFront erkennt automatisch den Gerätebildschirm und passt die Benutzeroberfläche entsprechend an.

Webinterface-Funktion	StoreFront-Äquivalent
Suche aktivieren, Suche deaktivieren	Die Suche ist standardmäßig aktiviert. **Zum Ausblenden der Suchfelder auf der Desktop-/Webbenutzeroberfläche** fügen Sie der Datei style.css folgenden Stil hinzu: `.search-container { display: none; } .` **Zum Ausblenden der Suchfelder auf der Telefonbenutzeroberfläche** fügen Sie der Datei style.css folgenden Stil hinzu: `## searchBtnPhone { display: none; } .`
Aktualisierung	Standardmäßig aktiviert (Browseraktualisierung).

Webinterface-Funktion	StoreFront-Äquivalent
Rückkehr zum letzten Ordner	Nicht standardmäßig aktiviert. Zum Speichern des aktuellen Ordners und Zurückkehren zu diesem Ordner 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 der Citrix Workspace-App gibt es nur sehr wenige QuickInfos, da sie für Geräte mit und ohne Touchscreen vorgesehen ist. Sie können QuickInfos über ein benutzerdefiniertes Skript hinzufügen.

Webinterface-Funktion	StoreFront-Äquivalent
Symbolansicht, Baumstrukturansicht, Detailansicht, Listenansicht, Gruppenansicht, Standardansicht festlegen, (niedrige Grafik) Symbolansicht, (niedrige Grafik) Listenansicht, (niedrige Grafik) Standardansicht	Die Citrix Workspace-App hat eine andere Benutzeroberfläche, daher gelten diese Optionen nicht. Sie können mit der StoreFront-Verwaltungskonsole Ansichten konfigurieren. Weitere Informationen, siehe Angeben anderer Ansichten für Desktops und Anwendungen.
Benutzeroberfläche auf einer einzelnen Registerkarte, Benutzeroberfläche auf Registerkarten (Registerkarte “App”, Registerkarte “Desktop”, Registerkarte “Inhalt”, (Tabulatorreihenfolge))	Die Benutzeroberfläche der Citrix Workspace-App 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, Kopfzeilenhintergrundfarbe, Kopfzeilenhintergrundbild	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'); }`

Webinterface-Funktion	StoreFront-Äquivalent
Begrüßungsnachricht vor der Anmeldung (Pre-locale) (Titel, Text, Hyperlink, Schaltflächenbeschriftung)	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: ”Welcome!”, messageText: ”Only for \<a href=” http://www.WWc.com” target=”_blank ”\>WWCo Employees”, okButtonText: ” Accept”, okAction: callback }); } ; // Before main screen (for native clients)CTXS.Extensions. beforeDisplayHomeScreen = function (callback){ if (!doneClickThrough){ CTXS.ExtensionAPI.showMessage({ messageTitle: ”Welcome!”, messageText: ”Only for WWCo Employees”, okButtonText: ”Accept”, okAction: callback }); } else { callback(); } } ;`

Webinterface-Funktion	StoreFront-Äquivalent
Anmeldebildschirmtitel, Anmeldebildschirmnachricht, Anmeldebildschirmsystemmeldung	Es gibt vier Bereiche für Anpassungen auf dem Anmeldebildschirm bzw. den Anmeldebildschirmen: Bereich oben 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 Neuladen der Benutzeroberfläche auf allen Clients erzwingen. Fügen Sie dynamische Inhalte im Verzeichnis **customweb** ein.
Anwendungsbildschirmbegrüßungsnachricht, Anwendungsbildschirmsystemnachricht	Siehe Beispiele für **CustomAuth**-Begrüßungsbildschirm oben. Sie 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; } ** Example static content using a script: **\$('\##customBottom').html("Welcome to ACME");`

Webinterface-Funktion	StoreFront-Äquivalent
Features ohne direkte Entsprechung	
Anmeldebildschirm ohne Kopfzeilen, Anmeldebildschirm mit Kopfzeilen (einschließlich Nachrichten)	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. Siehe 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

January 6, 2020

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.

Bevor ein entfernter StoreFront-Server wieder zur gleichen oder einer anderen Servergruppe hinzugefügt werden kann, müssen Sie ihn auf die werkseitigen Standardeinstellungen zurücksetzen. Siehe Zurücksetzen eines Servers auf die Werkseinstellungen

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. Die Verteilung von Konfigurationsinformationen wird manuell initiiert, sodass Sie die Kontrolle darüber behalten, ob und wann die Server in der Gruppe mit Konfigurationsänderungen aktualisiert werden. Beachten Sie bei dieser Aufgabe, dass Sie erst dann weitere Änderungen machen, wenn alle Server in der Gruppe aktualisiert wurden.

> **Wichtig:**
>
> Alle Änderungen, die auf anderen Servern in der Gruppe vorgenommen wurden, werden bei der Verteilung verworfen. Wenn Sie die Konfiguration eines Servers aktualisieren, verteilen Sie die Änderungen auf die anderen Server in der Gruppe, um zu vermeiden, dass die Änderungen verloren gehen, falls Sie anschließend Änderungen von einem anderen Server in der Bereitstellung übernehmen.

Die Informationen, die zwischen Servern in der Gruppe übertragen werden, umfassen Folgendes:

- Inhalt aller web.config-Dateien, die die StoreFront Konfiguration enthalten
- Inhalt von `C:\Program Files\Citrix\Receiver StoreFront\Receiver Clients`, z. B. `C:\Program Files\Citrix\Receiver StoreFront\Receiver Clients\Windows\CitrixWorkspaceAppWeb.exe` und `C:\Program Files\Citrix\Receiver StoreFront\Receiver Clients\MAC\CitrixWorkspaceAppWeb.dmg`
- Inhalt von `C:\inetpub\wwwroot\Citrix\StoreWeb\Custom\contrib`
- Inhalt von `C:\inetpub\wwwroot\Citrix\StoreWeb\Custom\custom folder`, z. B. kopierte Bilder und benutzerdefinierte JS-Dateien
- Inhalt des Citrix Delivery Services-Zertifikatspeichers, ausgenommen manuell importierte Zertifikatsperrlisten. (Weitere Informationen zum Verteilen lokaler Zertifikatsperrlisten finden Sie unter Überprüfung von Zertifikatsperrlisten.)

> **Hinweis:**
>
> Abonnementdaten werden unabhängig vom Mechanismus “Änderungen verteilen” mit den anderen Servern synchronisiert. Dies geschieht automatisch, ohne dass der Task “Änderungen verteilen” gestartet wird.

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 und Sie der Standardwebsite eine HTTPS-Bindung hinzufügen. Weitere Informationen finden Sie unter Sichern der StoreFront-Bereitstellung.

Konfigurieren der Serverumgehung

Zur Verbesserung der Leistung bei Ausfall eines Servers, auf dem Ressourcen bereitgestellt werden, umgeht StoreFront vorübergehend Server, die nicht antworten. Bei einer Serverumgehung ignoriert

StoreFront den Server und greift nicht auf dessen Ressourcen zu. 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 der "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 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. Navigieren Sie auf der Windows-**Startseite** oder auf der **Apps**-Seite zur Kachel **Citrix StoreFront**.
2. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores** und klicken Sie auf **Delivery Controller verwalten** im Bereich **Aktionen**.
3. Wählen Sie einen Controller aus, klicken Sie auf **Bearbeiten** und dann auf **Einstellungen** auf dem Bildschirm **Delivery Controller bearbeiten**.
4. Klicken Sie unter "Erweiterte Einstellungen" auf **Einstellungen**.

5. Gehen Sie im Dialogfeld “Erweiterte Einstellungen” vor:
   a) Klicken Sie in der Zeile **Umgehungsdauer bei Ausfall aller Server** in die zweite Spalte und geben Sie eine Zeit in Minuten ein, für die ein Delivery Controller als offline betrachtet wird, nachdem alle seine Server nicht geantwortet haben.
   b) Klicken Sie in der Zeile **Umgehungsdauer** in die zweite Spalte und geben Sie eine Zeit in Minuten ein, für die ein einzelner Server als offline betrachtet wird, wenn er nicht antwortet.

Konfigurieren von Authentifizierung und Delegierung

January 6, 2020

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

Methode	Detail
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 Citrix Virtual Apps and Desktops ist und keine Active Directory-Vertrauensstellungen eingerichtet werden können, können Sie StoreFront zur Verwendung des XML-Diensts von Citrix Virtual Apps and Desktops 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.

Methode	Detail
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.

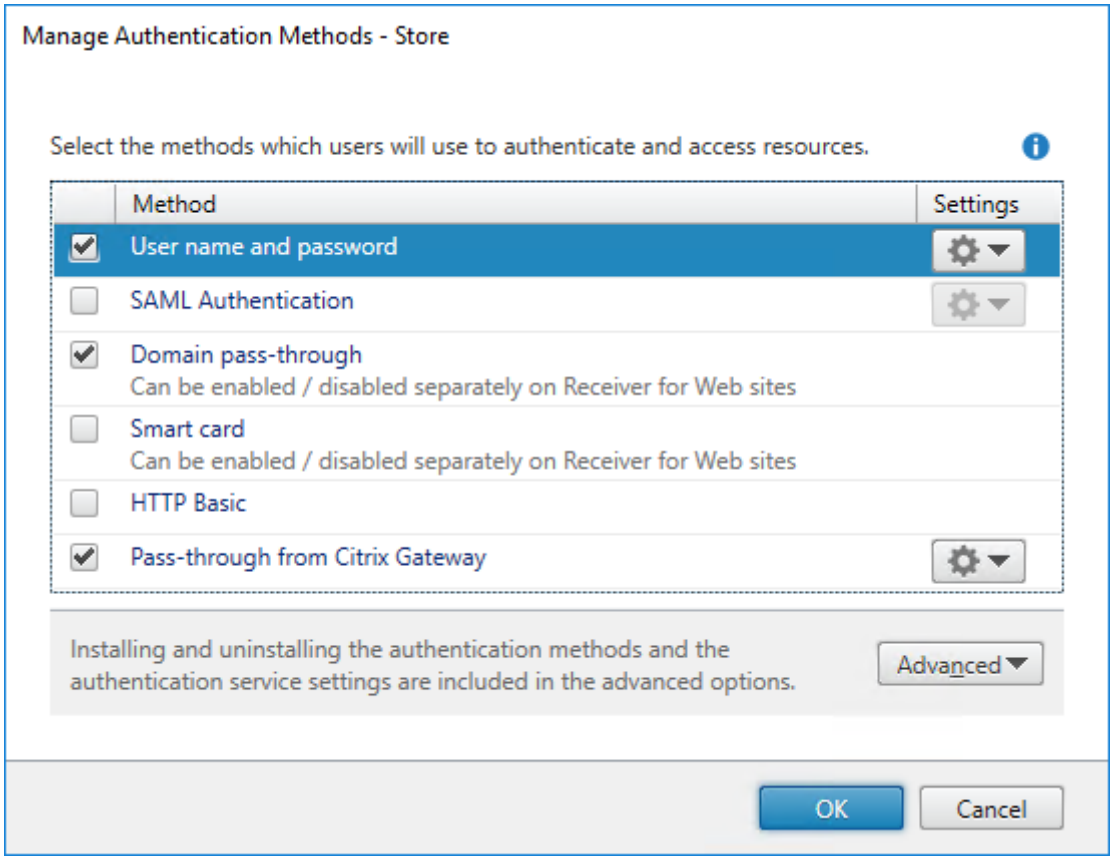
Konfigurieren des Authentifizierungsdiensts

April 1, 2020

Authentifizierungsmethoden verwalten

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 dem Windows-Bildschirm “Start” oder “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 **Authentifizierungsmethoden verwalten**.
3. Geben Sie an, welche Zugriffsmethoden für die Benutzer aktiviert werden sollen.



- Aktivieren Sie 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 **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 bzw. die Citrix Workspace-App auf den Benutzergeräten installiert ist.
- Aktivieren Sie **Smartcard**, um die Smartcardauthentifizierung zu aktivieren. Benutzer authentifizieren sich mit Smartcards und PINs beim Zugriff auf ihre Stores.

- Aktivieren Sie **HTTP Basic**, um die HTTP Basic-Authentifizierung zu aktivieren. Benutzer authentifizieren sich über den IIS-Webserver des StoreFront-Servers.
- Aktivieren Sie **Passthrough-Authentifizierung von Citrix Gateway** zum Aktivieren der Passthrough-Authentifizierung von Citrix Gateway. Die Benutzer authentifizieren sich bei Citrix Gateway und werden beim Zugriff auf ihre Stores automatisch angemeldet.

Zum Aktivieren der Passthrough-Authentifizierung für Smartcardbenutzer, die auf Stores über Citrix 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 Citrix Gateway anmelden.

1. Navigieren Sie auf der Windows-Startseite oder auf der Apps-Seite zur 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 > Einstellungen** die Option **Vertrauenswürdige Domänen konfigurieren** aus.
4. Wählen Sie **Nur vertrauenswürdige Domänen** aus 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**. Um den Zugriff auf Stores für Benutzerkonten in der Domäne zu entfernen, wählen Sie eine Domäne in der Liste aus und klicken Sie auf **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 der Citrix Workspace-App und von Receiver für Web, die sich mit Domänenanmeldeinformationen anmelden, ihre Kennwörter ändern. Beim Erstellen des Authentifizierungsdiensts verhindert die Standardkonfiguration, dass Benutzer der Citrix Workspace-App und von Citrix Receiver für Web 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 Desktopversionen der Citrix Workspace-App unterstützen die Kennwortänderung über Citrix Gateway nur bei Kennwortablauf. Navigieren Sie auf der Windows-Startseite oder auf der Apps-Seite zur 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, 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 ihre Kennwörter nur ändern können, wenn sie abgelaufen sind, wählen Sie **Nach Ablauf**. Benutzer, die sich nicht anmelden können, weil das Kennwort abgelaufen ist, werden an das Dialogfeld Kennwort ändern weitergeleitet. Dies wird für die Citrix Workspace-App und für Citrix Receiver für Web unterstützt.

> Hinweis:
>
> Stellen Sie sicher, dass auf den StoreFront-Servern ausreichend Speicherplatz zum Speichern aller Benutzerprofile vorhanden ist. 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.

- Um zu verhindern, dass Benutzer ihre Kennwörter ändern, wählen Sie die Option **Benutzern erlauben, Passwörter zu ändern** nicht aus. Wenn Sie diese Option nicht auswählen, müssen Sie Benutzern unterstützen, die keinen Zugriff auf ihre Desktops und Anwendungen haben, weil das Kennwort abgelaufen ist.
- Um zu verhindern, dass Benutzer ihre Kennwörter ändern, wählen Sie die Option **Benutzern erlauben, Passwörter zu ändern** nicht aus. Wenn Sie diese Option nicht auswählen, müssen Sie Benutzern unterstützen, die keinen Zugriff auf ihre Desktops und Anwendungen haben, weil das Kennwort abgelaufen ist.

Citrix Workspace-App	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-Site	Ja	Ja	Ja

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.

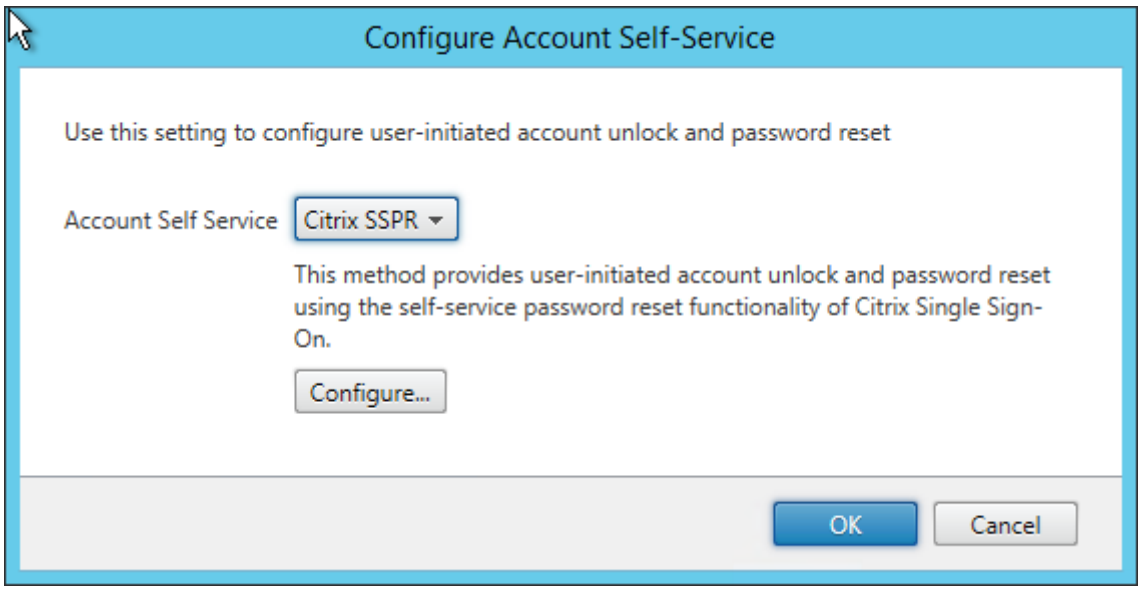
Self-Service-Kennwortzurücksetzung unterstützt keine UPN-Anmeldungen, wie `username@domain.com`.

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

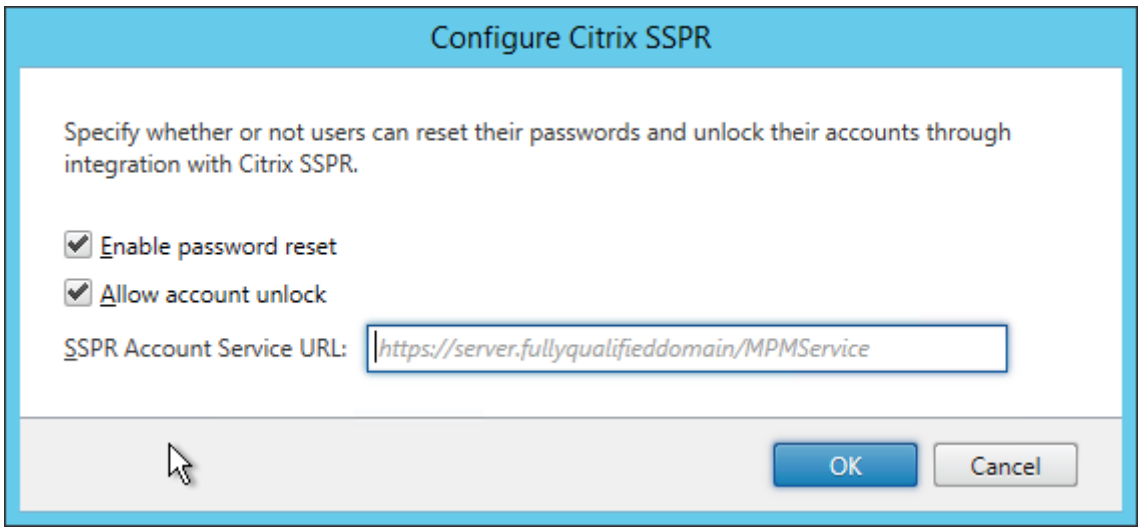
- Der Store ist für die Authentifizierung mit Benutzernamen und Kennwort konfiguriert.
- Der Store ist für die Verwendung von nur einer Self-Service-Kennwortzurücksetzung konfiguriert. Wenn StoreFront zur Verwendung mehrerer Farmen in derselben Domäne oder in vertrauenswürdigen Domänen konfiguriert ist, 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 zuordnen.

Zur Verwendung der Self-Service-Kennwortzurücksetzung müssen Sie diese installieren und konfigurieren. Sie befindet sich auf dem Medium mit Citrix Virtual Apps and Desktops. Informationen hierzu finden Sie unter Self-Service-Kennwortzurücksetzung.

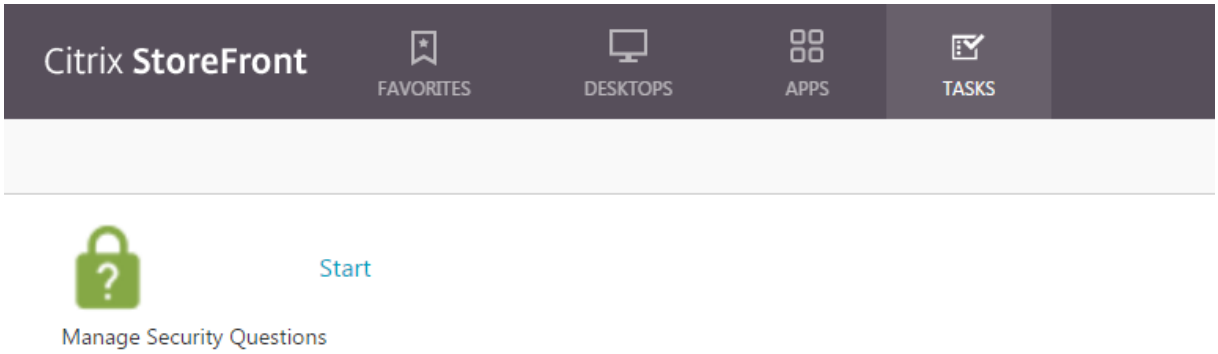
1. Wählen Sie zum Aktivieren der Unterstützung der Self-Service-Kennwortzurücksetzung im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores** aus, klicken Sie im Bereich **Aktionen** auf **Authentifizierungsmethoden verwalten > Benutzername und Kennwort** und wählen Sie im Dropdownmenü **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 noch einmal 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.



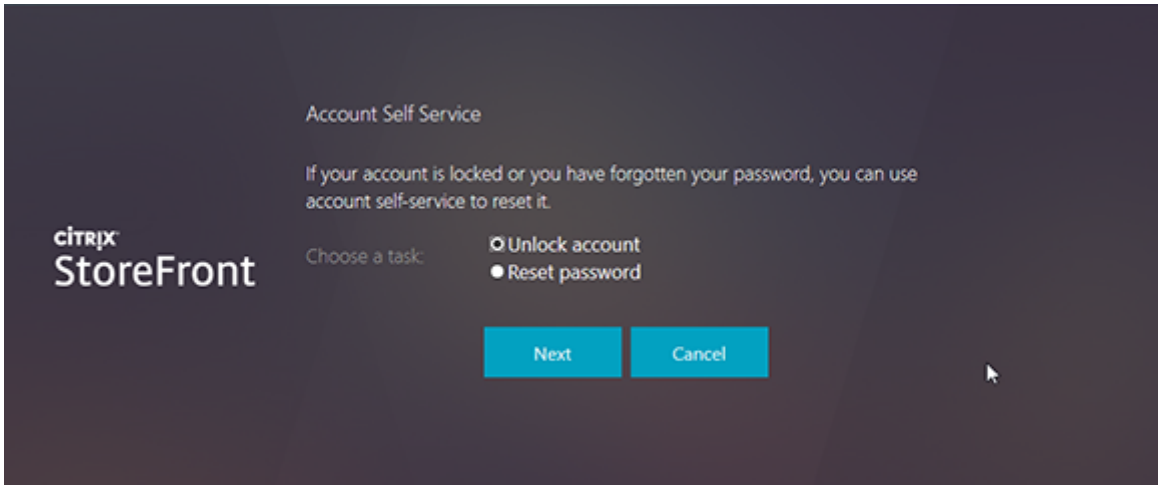
Das nächste Mal, wenn ein Benutzer sich an der Citrix Workspace-App oder Citrix Receiver für Web anmeldet, ist die Registrierung für Sicherheitszwecke verfügbar. Nachdem der Benutzer auf **Start** geklickt hat, werden Fragen angezeigt, die er beantworten muss.



Nach der Konfiguration in StoreFront sehen Benutzer den Link **Konto-Self-Service** im Citrix Receiver für Web-Anmeldebildschirm (wird in der Citrix Workspace-App als Schaltfläche angezeigt).

Durch Klicken auf diesen Link werden Benutzer durch eine Reihe von Formularen geführt. Zunächst wählen sie zwischen **Konto entsperren** und **Kennwort zurücksetzen** (wenn beide verfügbar sind).

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 `username@domain.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. Navigieren Sie auf der Windows-**Startseite** oder auf der **Apps**-Seite zur 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 **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 funktionalen Unterschied zwischen einem gemeinsam genutzten und einem dedizierten Authentifizierungsdienst. 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 Anmeldeinformationsvalidierung an Citrix Gateway

Zum Aktivieren der Passthrough-Authentifizierung für Smartcardbenutzer, die auf Stores über Citrix Gateway zugreifen, verwenden Sie die Aufgabe “Delegierte Authentifizierung konfigurieren”. Diese Aufgabe ist nur verfügbar, wenn Passthrough-Authentifizierung von Citrix Gateway aktiviert und im Ergebnisbereich ausgewählt ist.

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

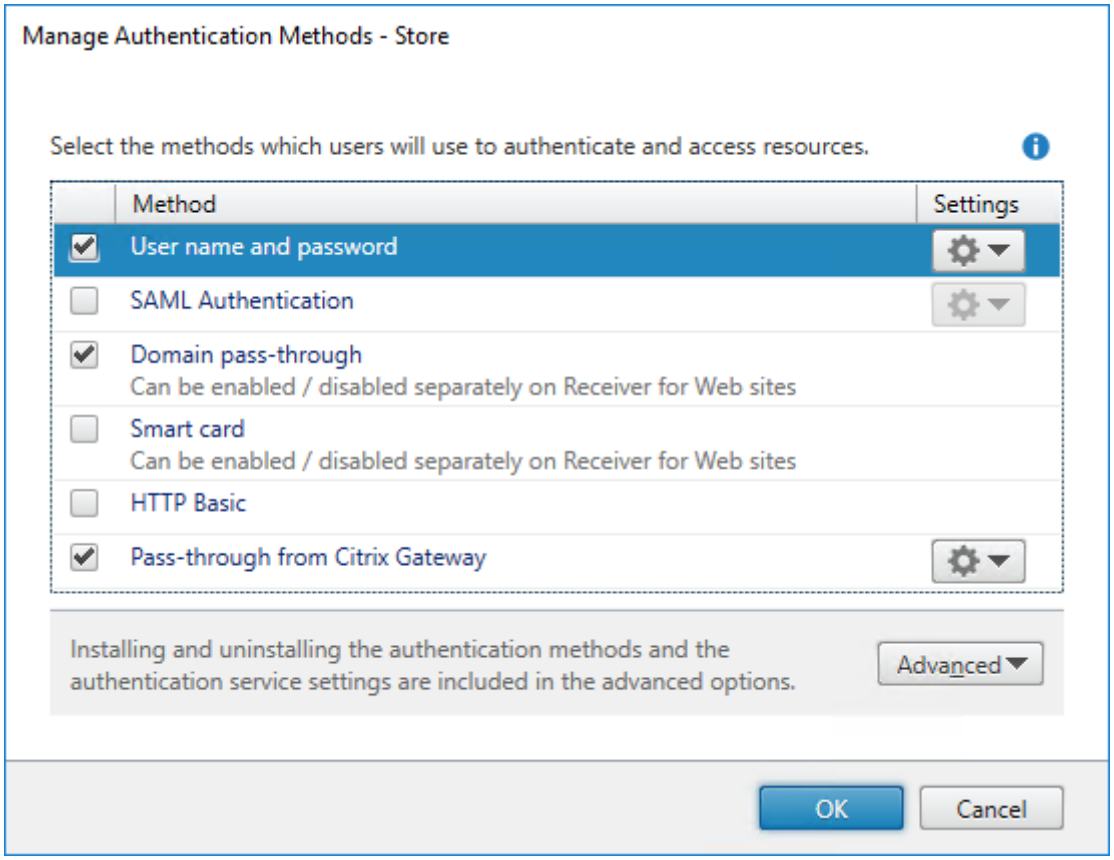
Authentifizierung auf Basis des XML-Diensts

April 1, 2020

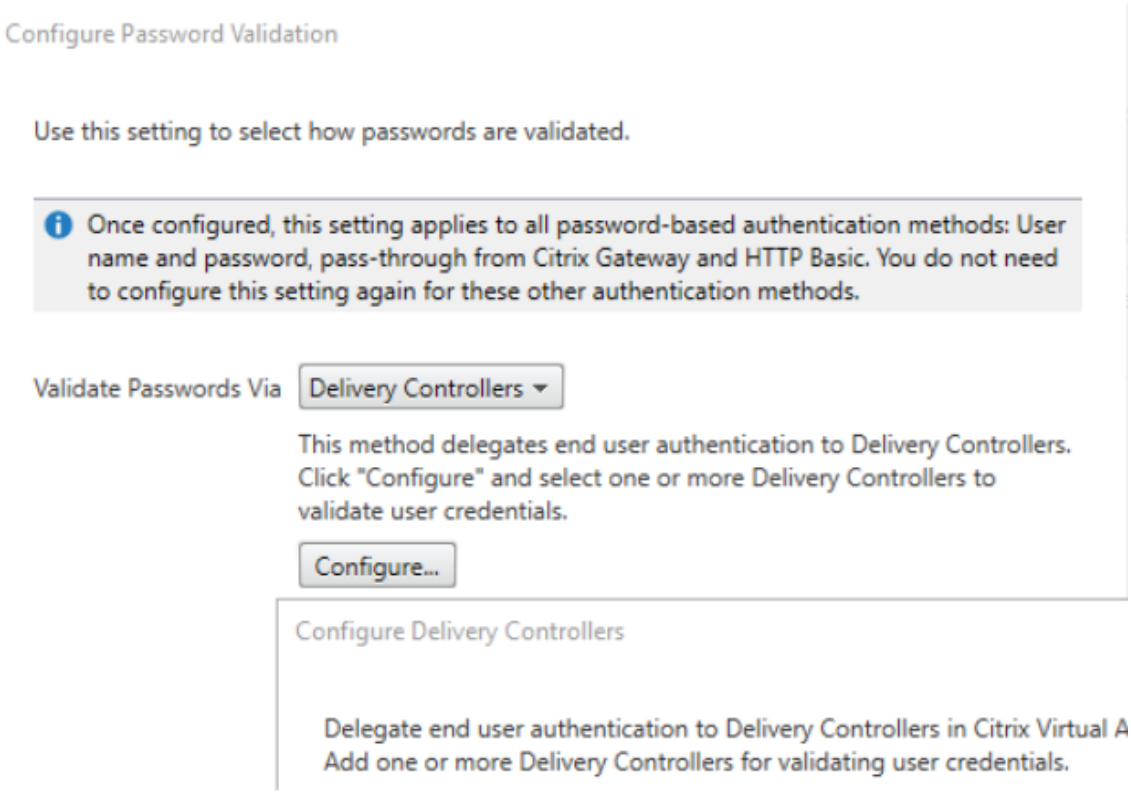
Wenn StoreFront nicht in der gleichen Domäne wie Citrix Virtual Apps and Desktops ist und keine Active Directory-Vertrauensstellungen eingerichtet werden können, können Sie StoreFront zur Verwendung des XML-Diensts von Citrix Virtual Apps and Desktops für die Authentifizierung der Anmeldeinformationen konfigurieren.

Aktivieren der Authentifizierung auf Basis des XML-Diensts

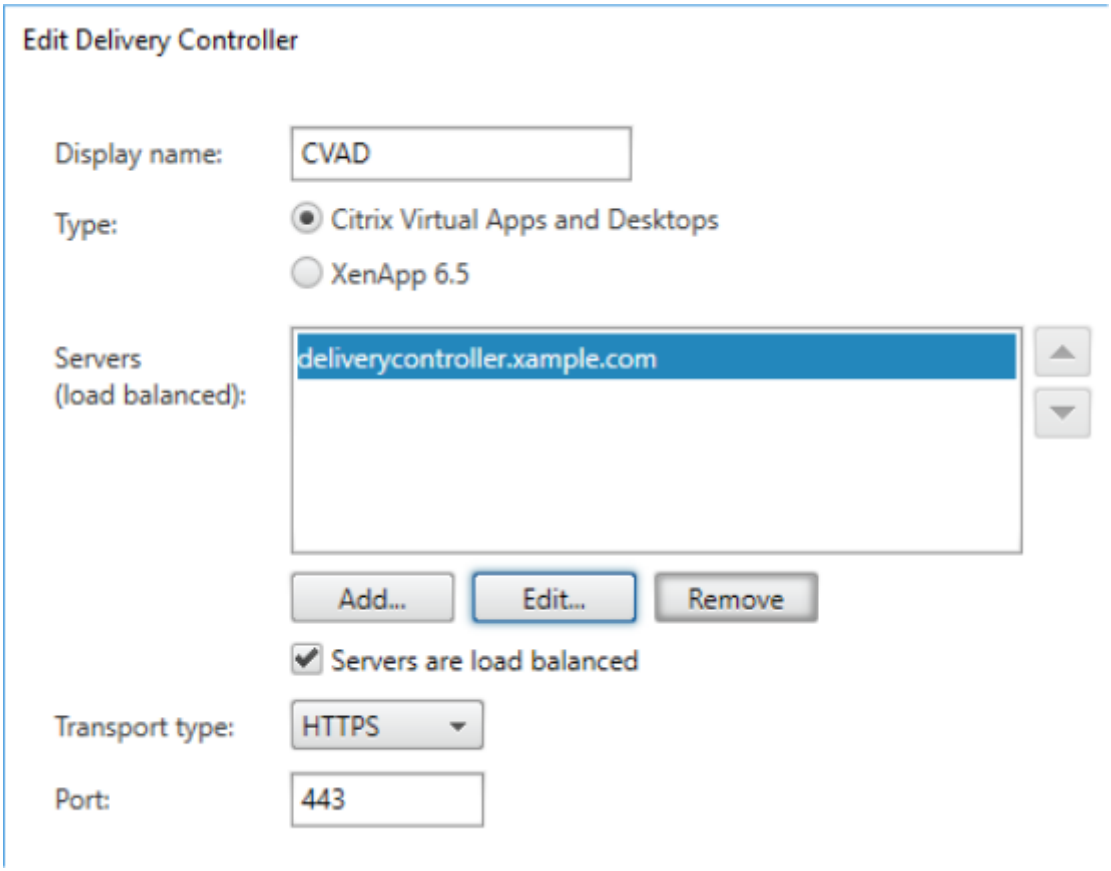
1. Klicken Sie auf dem Windows-Bildschirm **Start** oder **Apps** auf die Kachel “Citrix StoreFront”.
2. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores** und klicken Sie im Aktionsbereich auf **Authentifizierungsmethoden verwalten**.
3. Wählen Sie auf der Seite **Authentifizierungsmethoden verwalten** im Dropdownmenü **Benutzername und Kennwort > Einstellungen** die Option **Kennwortvalidierung konfigurieren**.



4. Wählen Sie in der Liste **Kennwörter validieren mit** die Option **Delivery Controller** und klicken Sie auf **Konfigurieren**.



5. Folgen Sie den Anweisungen auf den Seiten **Delivery Controller konfigurieren**, um mindestens einen **Delivery Controller** zum Validieren der Benutzeranmeldeinformationen hinzuzufügen und klicken Sie auf **OK**.



Deaktivieren der Authentifizierung auf Basis des XML-Diensts

1. Klicken Sie auf dem Windows-Bildschirm **Start** oder **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. Wählen Sie auf der Seite **Authentifizierungsmethoden verwalten** in der Liste **Benutzername und Kennwort** > **Einstellungen** die Option **Kennwortvalidierung konfigurieren**.
4. Wählen Sie im Dropdownmenü **Kennwörter validieren mit** die Option **Active Directory** und klicken Sie auf **Konfigurieren**.

Konfigurieren der eingeschränkten Kerberos-Delegierung für XenApp 6.5

March 3, 2020

> Hinweis:
>
> XenApp 6.5 hat das Ende des Lebenszyklus (EOL) erreicht und wird jetzt vom Extended Support-Programm abgedeckt.

Verwenden Sie die Aufgabe **Storeeinstellungen konfigurieren** > **Kerberos-Delegierung** 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. Zum Abschluss übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden.

1. Navigieren Sie auf der Windows-Startseite oder auf der Apps-Seite zur 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 “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 Citrix Virtual Apps 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 **Aktionen** 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 XML-Dienst von Citrix Virtual Apps and Desktops 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 Citrix Virtual Apps-Servers für die Delegierung

Konfigurieren Sie die vertrauenswürdige Active Directory-Delegierung für jeden Citrix Virtual Apps-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 XML-Dienst von Citrix Virtual Apps and Desktops aus, mit dem StoreFront eine Verbindung herstellen soll.
3. Klicken Sie im Bereich **Aktionen** 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 XML-Dienst von Citrix Virtual Apps and Desktops 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 Überlegungen

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.
- Citrix 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 Citrix 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 Citrix 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 Citrix Gateway-Server ohne Authentifizierung zu leiten.

- Citrix Receiver für Windows bzw. Citrix Workspace-App 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 bzw. Citrix Workspace-App 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 ein Backup der Registrierung, bevor Sie sie bearbeiten.

    32-Bit-Maschinen: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\AuthManagerProtocols\integratedwindo
    Name: SSONCheckEnabled
    Type: REG_SZ
    Wert: true oder false
    64-Bit-Maschinen: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\AuthManagerProtocols\
    Name: SSONCheckEnabled
    Type: REG_SZ
    Wert: true oder false

Konfigurieren der Smartcardauthentifizierung

December 23, 2019

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.

Unter Smartcard-Konfiguration für Citrix Umgebungen wird beschrieben, wie eine Citrix-Bereitstellung für eine bestimmte Art von Smartcards konfiguriert wird. Bei Smartcards anderer Hersteller sind die Arbeitsschritte ähnlich.

> Hinweis:
>
> In diesem Artikel gelten die Erläuterungen zur Citrix Workspace-App, sofern nicht anders angegeben, auch für die unterstützten Versionen von Citrix Receiver.

Voraussetzungen

- 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 Citrix Virtual Desktops 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.

Konfigurieren von Citrix Gateway

- Installieren Sie auf dem Citrix Gateway-Gerät ein signiertes Serverzertifikat von einer Zertifizierungsstelle. Weitere Informationen finden Sie unter Installieren und Verwalten von Zertifikaten.

- Installieren Sie auf dem Citrix Gateway-Gerät das Stammzertifikat der Zertifizierungsstelle, die die Smartcardbenutzerzertifikate ausstellt. Weitere Informationen finden Sie unter To install a root certificate on Citrix 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 Konfigurieren und Binden einer Richtlinie für die Clientzertifikatauthentifizierung.
- 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 Configuring smart card authentication.

  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 Citrix 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 Citrix Gateway zu StoreFront und binden Sie diese an den geeigneten virtuellen Server. Weitere Informationen finden Sie unter Access to StoreFront Through Citrix 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 Citrix 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.

Konfigurieren von StoreFront

- 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 https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831637(v=ws.11)#create-certificate-wizard. Weitere Hinweise zum Hinzufügen einer HTTPS-Bindung zu einer IIS-Site finden Sie unter https://docs.microsoft.com/en-us/previous-versions/orphan-topics/ws.11/hh831632(v=ws.11).
- 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, mit den entsprechenden Windows-Richtlinieneinstellungen, damit Benutzer 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 Citrix 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 Citrix 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 Citrix Gateway zugreifen, aktivieren Sie die Passthrough-Authentifizierung mit Citrix Gateway und stellen Sie sicher, dass StoreFront so konfiguriert ist, dass die Überprüfung der Anmeldeinformationen an Citrix Gateway delegiert wird. Wenn Sie beabsichtigen, die Passthrough-Authentifizierung zu aktivieren, wenn Sie Citrix

Receiver für Windows bzw. die Citrix Workspace-App 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 bzw. die Citrix Workspace-App für Windows auf domänengebundenen Benutzergeräten installieren, bearbeiten Sie die Datei default.ica für den Store, um 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 bzw. die Citrix Workspace-App für Windows.
- Wenn Sie einen zusätzlichen virtuellen Server für Citrix Gateway erstellt haben, der ausschließlich für Verbindungen zu Ressourcen verwendet werden soll, konfigurieren Sie das optimale Citrix 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 von 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.

Konfigurieren von Benutzergeräten

- Stellen Sie sicher, dass die Smartcard-Middleware des Herstellers auf allen Benutzergeräten installiert ist.
- Installieren Sie 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 am 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 der Citrix Workspace-App auf dem Benutzergerät. Zum Aktivieren von Passthrough der Smartcardanmeldeinformationen

zu Citrix Virtual Apps and Desktops für Benutzer domänengebundener Geräte verwenden Sie ein Konto mit Administratorrechten für die Installation der Citrix Workspace-App für Windows an einer Eingabeaufforderung mit der Option **/includeSSON**. Weitere Informationen finden Sie unter Verwenden von Befehlszeilenparametern.

Stellen Sie sicher, dass die Citrix Workspace-App 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 für Citrix Workspace-App für Windows, icaclient.adm, auf dem Domänencontroller für die 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 Smartcard.

Aktivieren Sie die Richtlinie Smartcardauthentifizierung. Zum Gestatten von Passthrough der Smartcardanmeldeinformationen wählen Sie Use pass-through authentication for PIN. Damit die Smartcardanmeldeinformationen an Citrix Virtual Apps and Desktops weitergeleitet werden, aktivieren Sie dann die Richtlinie “Lokaler Benutzername und Kennwort” und wählen Sie die Option “Passthrough-Authentifizierung für alle ICA-Verbindungen zulassen”. Weitere Informationen finden Sie unter Referenz für ICA-Einstellungen.

Wenn Sie Passthrough von Smartcardanmeldeinformationen an Citrix Virtual Apps and Desktops 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 Citrix Gateway-Gerät (Remotebenutzer) mit einer entsprechenden Methode zur Verfügung. Weitere Informationen über die Bereitstellung von Konfigurationsinformationen für die Benutzer finden Sie unter Referenz für ICA-Einstellungen.

Aktivieren von Passthrough mit Smartcardauthentifizierung für Citrix Receiver für Windows bzw. die Citrix Workspace-App für Windows

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 Citrix Virtual Apps and Desktops 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 Texteditor. 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. Für Passthrough von Smartcardanmeldeinformationen für Benutzer, die ohne Citrix Gateway auf Stores zugreifen, fügen Sie die folgende Einstellung im Bereich [Anwendung] 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. Für Passthrough von Smartcardanmeldeinformationen für Benutzer, die mit Citrix Gateway auf Stores zugreifen, fügen Sie die folgende Einstellung im Bereich [Anwendung] 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

April 1, 2020

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 dem Windows-Bildschirm **Start** oder **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. 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

January 6, 2020

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

Aufgabe	Detail
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 Citrix Gateway-Bereitstellungen und Beacons, die für Stores konfiguriert wurden.

Aufgabe	Detail
Ausblenden und Ankündigen von Stores für Benutzer	Verhindern Sie, dass Stores den Benutzern zum Hinzufügen zu ihrem Konto angezeigt werden, wenn diese die Citrix Workspace-App 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 Citrix Gateway	Konfigurieren Sie den Zugriff auf Stores über Citrix Gateway für Benutzer in öffentlichen Netzwerken.
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

April 1, 2020

Verwenden Sie die Aufgabe **Store erstellen**, um zusätzliche Stores zu konfigurieren. Sie können beliebig viele Stores erstellen. Beispielsweise kann es empfehlenswert sein, einen Store für eine bestimmte Benutzergruppe zu erstellen oder bestimmte Ressourcen zusammenzufassen.

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 Citrix Gateway.

Wenn Sie auf der Seite “Storename” die Option **Nur nicht authentifizierte (anonyme) Benutzer dürfen auf diesen Store zugreifen** wählen, können Sie einen Store ohne Authentifizierung erstellen. Wenn Sie einen Store ohne Authentifizierung erstellen, sind die Seiten **Authentifizierungsmethoden** und **Remotezugriff** nicht verfügbar und der **Servergruppenknoten** links und der Bereich “Aktion” wird durch **Basis-URL ändern** ersetzt. (Es ist nur diese Option verfügbar, weil Servergruppen für Server, die nicht in einer Domäne sind, nicht zur Verfügung stehen.)

> 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.

Hinzufügen von Desktops und Anwendungen zu einem Store

1. Klicken Sie auf dem Windows-Bildschirm “Start” oder “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 **Store erstellen**.
3. Geben Sie auf der Seite **Storename** einen Namen für den Store an und klicken Sie auf **Weiter**.

   Storenamen erscheinen in der Citrix Workspace-App unter den Konten der Benutzer. Wählen Sie daher einen Namen, anhand dessen die 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 Anzeigenamen an, anhand dessen Sie die Bereitstellung identifizieren können. Geben Sie unter **Typ** an, wie die Ressourcen im Store bereitgestellt werden. Der Typ ist standardmäßig auf Citrix Virtual Apps and Desktops festgelegt. XenApp 6.5 steht als Typ zur Auswahl, hat jedoch im Juni 2018 das Ende des Lebenszyklus erreicht und wird jetzt vom Extended Support-Programm abgedeckt.
6. Um Desktops und Anwendungen, die von Citrix Virtual Apps and Desktops und XenApp 6.5 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 Citrix Virtual Apps and Desktops-Sites Details der Delivery Controller an. Listen Sie für XenApp 6.5-Farmen Server auf, auf denen der Citrix XML-Dienst ausgeführt wird.
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 TLS (Transport Layer Security) zu senden. Wenn Sie diese Option für Citrix Virtual Apps and Desktops-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 6.5-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 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 dem Server verwenden soll. Der Standardport ist 80 für Verbindungen über HTTP und SSL-Relay bzw. 443 für HTTPS-Verbindungen. Bei Citrix Virtual Apps and Desktops-Servern muss der angegebene Port dem vom Citrix XML-Dienst verwendeten Port entsprechen.
9. Wenn Sie SSL-Relay verwenden, um Verbindungen zwischen StoreFront und dem XenApp 6.5-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.
10. Klicken Sie auf **OK**. Sie können Stores konfigurieren, die Ressourcen aus einer beliebigen Zusammenstellung von Citrix Virtual Apps and Desktops-Bereitstellungen bieten. Wiederholen Sie erforderlichenfalls die Schritte 4 bis 10, um weitere Bereitstellungen von Ressourcen für den Store aufzulisten. Wenn Sie alle erforderlichen Ressourcen hinzugefügt haben, klicken Sie auf **Weiter**.
11. Geben Sie auf der Seite **Remotezugriff** an, ob und wie Benutzer, die eine Verbindung aus einem öffentlichen Netzwerk herstellen, über Citrix Gateway auf den Store zugreifen können:
    - Soll der Store Benutzern in öffentlichen Netzwerken nicht zur Verfügung stehen, deaktivieren Sie die Option **Remotezugriff aktivieren**. 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 Citrix Gateway verfügbar machen möchten, wählen Sie **Kein VPN-Tunnel** aus. Die Benutzer melden sich entweder über ICAProxy oder ein clientloses VPN (CVPN) bei Citrix Gateway an und benötigen das Citrix Gateway-Plug-In nicht für ein vollständiges VPN.
      - 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. Die Benutzer benötigen das Citrix Gateway-Plug-In für das Erstellen des VPN-Tunnels.

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

12. Wenn Sie den Remotezugriff aktiviert haben, wählen Sie in der Liste der **Citrix Gateway-Geräte** ein Gerät (Bereitstellung) aus, über das die Benutzer auf den Store zugreifen können. Die Liste enthält alle Bereitstellungen, die zuvor für diesen und andere Stores konfiguriert wurden. Wenn Sie Zugriff über mehrere Geräte aktivieren, indem Sie mehr als einen Eintrag in der Liste auswählen, geben Sie das **Standardgerät** für den Zugriff auf den Store an. Um weitere Geräte zur Liste hinzuzufügen, führen Sie die unter Konfigurieren des Remotezugriffs auf den Store über Citrix Gateway beschriebenen Schritte aus.
13. Wählen Sie auf der Seite **Authentifizierungsmethoden** die Methoden, die Benutzer zum Authentifizieren und Zugreifen auf den Store verwenden, 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 einem Identitätsanbieter und werden beim Zugriff auf ihre Stores automatisch angemeldet.
    - **Domänen-Passthrough-Authentifizierung**: Die 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.
    - **HTTP Basic**: Benutzer authentifizieren sich über den IIS-Webserver des StoreFront-Servers.
    - **Passthrough-Authentifizierung von Citrix Gateway**: Die Benutzer authentifizieren sich bei Citrix Gateway und werden beim Zugriff auf ihre Stores automatisch angemeldet. Diese Option wird automatisch aktiviert, wenn Remotezugriff aktiviert wird.1. Wählen Sie auf der Seite **Kennwortvalidierung konfigurieren** die Delivery Controller, die die Kennwortvalidierung bereitstellen, und klicken Sie auf **Weiter**.
14. 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**.
15. Nach dem Erstellen des Stores klicken Sie auf **Fertig stellen**.

Zugriff auf den Store

Der Store steht jetzt für den Zugriff durch Benutzer über die Citrix Workspace-App 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 von 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.

Konfigurieren des Remotezugriffs auf den Store über Citrix Gateway

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

1. Klicken Sie auf der Seite **Remotezugriff** des **Assistenten zum Erstellen von Stores** auf **Hinzufügen**.
2. Geben im Dialogfeld **Citrix Gateway-Gerät hinzufügen** auf der Seite **Allgemeine Einstellungen** einen **Anzeigenamen** für das Citrix Gateway-Gerät an, über den die Benutzer dieses identifizieren können.

   Den Benutzern wird der Anzeigename angezeigt, den Sie in der Citrix Workspace-App angegeben haben. Nehmen Sie deshalb relevante Informationen in den Namen auf, damit die Benutzer leichter entscheiden können, ob sie das Gateway verwenden möchten. Beispielsweise können Sie den geographischen Standort in die Anzeigenamen der Citrix Gateway-Bereitstellungen einfügen, damit Benutzer problemlos das nächstgelegene Gateway für ihren Standort identifizieren können.
3. Geben Sie für **Citrix Gateway-URL** die URL:Port-Kombination des virtuellen Citrix Gateway-Servers Ihrer Bereitstellung ein. Wird kein Port angegeben, wird der Standard-`https://`-Port 443 verwendet. Port 443 muss in der URL nicht angegeben werden.

Der vollqualifizierte Domänenname (FQDN) für die StoreFront-Bereitstellung muss eindeutig sein und darf nicht dem vollqualifizierten Domänennamen des virtuellen Citrix Gateway-Servers entsprechen. Das Verwenden desselben FQDN für StoreFront und den virtuellen Citrix Gateway-Server wird nicht unterstützt.

4. Wählen Sie aus den verfügbaren Optionen die **Verwendung oder Rolle** des Citrix Gateways aus.
   - **Authentifizierung und HDX-Routing:** Das Citrix Gateway wird für die Authentifizierung und das Routing von HDX-Sitzungen verwendet.
   - **Nur Authentifizierung:** Das Citrix Gateway wird nur für die Authentifizierung, jedoch nicht für das HDX-Sitzungsrouting verwendet.
   - **Nur HDX-Routing:** Das Citrix Gateway wird für das HDX-Routing, nicht aber für die Authentifizierung verwendet.
5. Liste Sie für alle Bereitstellungen, in denen Sie Ressourcen von Citrix Virtual Apps and Desktops oder XenApp 6.5 im Store verfügbar machen, auf der Seite **Secure Ticket Authority (STA)** alle 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 Citrix Virtual Apps and Desktops- bzw. XenApp 6.5-Servern gehostet und gibt Sitzungstickets als Reaktion auf Verbindungsanforderungen aus. Auf diesen Sitzungstickets basiert die Authentifizierung und Autorisierung für den Zugriff auf Citrix Virtual Apps and Desktops- bzw. XenApp 6.5-Ressourcen. Verwenden Sie die richtige STA URL (`HTTPS://` oder `HTTP://`) je nachdem, wie Ihre Delivery Controller konfiguriert sind. Die STA URL muss mit der in Citrix Gateway auf dem virtuellen Server konfigurierten URL identisch sein.
6. Wählen Sie für die STA Load Balancing aus. Sie können auch ein Zeitintervall festlegen, nach dem STAs, die nicht antworten, umgangen werden.
7. Um sicherzustellen, dass Citrix Virtual Apps and Desktops bzw. XenApp 6.5 getrennte Sitzungen aufrechterhält, während die Citrix Workspace-App eine automatische Wiederverbindung versucht, wählen Sie **Sitzungszuverlässigkeit aktivieren**.
8. Aktivieren Sie **Tickets von zwei Secure Ticket Authoritys anfordern (falls verfügbar)**, wenn Sie mehrere STAs konfigurieren und sicherstellen möchten, dass Sitzungszuverlässigkeit immer gegeben ist. StoreFront ruft dann Tickets von zwei verschiedenen Secure Ticket Authoritys ab und Benutzersitzungen werden nicht unterbrochen, 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. Geben Sie auf der Seite **Authentifizierungseinstellungen** die **vServer-IP-Adresse** (VIP) des Citrix Gateway-Geräts ein.

Verwenden Sie die private IP-Adresse des virtuellen Citrix Gateway-Servers und nicht die öffentliche, die der privaten per Netzwerkadressübersetzung zugeordnet ist. Gateways werden von StoreFront normalerweise über ihre URL identifiziert. Wenn Sie Global Server Load Balancing (GSLB) verwenden, müssen Sie die VIP jedem Gateway hinzufügen. Dadurch kann StoreFront mehrere Gateways identifizieren, die alle dieselbe URL (GSLB-Domänennamen) als separate Gateways verwenden. Beispielsweise können für den Store drei Gateways mit der URL `https://gslb.domain.com` konfiguriert werden, jedes hat jedoch eine eindeutige VIP (z. B. 10.0.0.1, 10.0.0.2 und 10.0.0.3).

10. Wenn Sie ein Gerät mit Citrix Gateway hinzufügen, wählen Sie aus der Liste **Anmeldetyp** die Authentifizierungsmethode aus, die Sie auf dem Gerät für Benutzer der Citrix Workspace-App konfiguriert haben.

    - 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** 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**.

11. Wenn Sie StoreFront für Citrix Gateway konfigurieren und SmartAccess verwenden möchten, müssen Sie eine **Callback-URL** eingeben. StoreFront fügt automatisch den Standardteil der URL an. Geben Sie die intern zugängliche URL des Geräts ein. StoreFront kontaktiert den Citrix Gateway-Authentifizierungsdienst, um zu überprüfen, ob von Citrix Gateway empfangene Anforderungen auch tatsächlich von diesem Gerät ausgehen.

    Bei Verwendung von GSLB empfiehlt es sich, eine eindeutige Callback-URL für jedes GSLB-Gateway zu konfigurieren. StoreFront muss jede eindeutige Callback-URL in die private VIP auflösen können, die für den jeweiligen virtuellen GSLB-Gateway-Server konfiguriert ist. Beispielsweise müssen `emeagateway.domain.com`, `usgateway.domain.com` und `apacgateway.domain.com` in die korrekte Gateway-VIP aufgelöst werden.

12. Klicken Sie auf **Erstellen**, um das Citrix Gateway-Gerät der Liste im Dialogfeld **Remotezugriffeinstellungen** hinzuzufügen.

    Die Informationen zur Konfiguration von Citrix Gateway-Geräten werden der CR-Provisioningdatei

für den Store hinzugefügt. Dadurch kann die Citrix Workspace-App die richtige Verbindungsanforderung senden, wenn ein Gerät zum ersten Mal kontaktiert wird.

Store entfernen

Mit der Aufgabe Store entfernen können Sie einen Store löschen. Wenn Sie einen Store entfernen, werden alle diesem zugeordneten Receiver für Web-Sites 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

March 3, 2020

Verwenden Sie die Aufgabe “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 Citrix 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.

Hinzufügen von Desktops und Anwendungen zu einem Store

1. Navigieren Sie auf der Windows-Startseite oder auf der Apps-Seite zur 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 **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 Citrix Virtual Apps and Desktops bzw. XenApp 6.5 bereitgestellt werden. (XenApp 6.5 hat das Ende des Lebenszyklus (EOL) erreicht und wird jetzt vom Extended Support-Programm abgedeckt.) Stellen Sie beim Zuweisen von Delivery 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.

   Um Desktops und Anwendungen, die von XenApp 6.5-Farmen bereitgestellt werden, im Store verfügbar zu machen, fügen Sie die Namen aller Server in der Farm 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 Citrix Virtual Desktops-Sites Details der Delivery Controller an. Listen Sie für XenApp 6.5-Farmen Server auf, auf denen der Citrix XML-Dienst ausgeführt wird.
6. 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 Citrix Virtual Apps and Desktops-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.

7. Geben Sie den Port an, den StoreFront für Verbindungen mit dem Server verwenden soll. Der Standardport ist 80 für Verbindungen mit HTTP und 443 für HTTPS-Verbindungen. Bei Citrix Virtual Apps and Desktops-Servern muss der angegebene Port dem vom Citrix XML-Dienst verwendeten Port entsprechen.
8. Klicken Sie auf **OK**. Sie können Stores konfigurieren, die Ressourcen aus einer beliebigen Zusammenstellung von Citrix Virtual Apps and Desktops-Bereitstellungen bieten. Wiederholen Sie erforderlichenfalls die Schritte 4 bis 9, um weitere Bereitstellungen von Ressourcen für den Store aufzulisten. Wenn Sie 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 die Citrix Workspace-App 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 Information 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. Standardmäßig werden 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 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.

> 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 beim Erstellen festgelegt wurde. Damit diese Sitzungen richtig beendet werden, muss auf dem von diesem Store verwendeten XenApp-Server die Option “XML-Anforderungen vertrauen” aktiviert sein (siehe Konfigurieren von Ports und Vertrauenseinstellungen für den Citrix XML-Service).

Exportieren von Store-Provisioningdateien für Benutzer

March 3, 2020

Mit den Aufgaben **Multistore-Provisioningdatei exportieren** und **Provisioningdatei exportieren** können Sie Dateien mit Verbindungsinformationen für Stores generieren, z. B. für Citrix Gateway-Bereitstellungen und Beacons, die für Stores konfiguriert wurden. Stellen Sie diese Dateien Benutzern zur Verfügung, damit diese die Citrix Workspace-App automatisch mit den Details der Stores konfigurieren können. Benutzer können auch Citrix Workspace-App-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. Navigieren Sie auf der Windows-Startseite oder auf der Apps-Seite zur Kachel Citrix StoreFront. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten Stores.
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

December 23, 2019

Verhindern Sie mit der Aufgabe “Store ausblenden”, dass Stores den Benutzern zum Hinzufügen zu ihrem Konto angezeigt werden, wenn diese die Citrix Workspace-App 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 die Benutzer müssen die Citrix Workspace-App 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. Navigieren Sie auf der Windows-**Startseite** oder auf der **Apps**-Seite zur 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**.

Verwalten der durch Stores zur Verfügung gestellten Ressourcen

April 1, 2020

Mit der Aufgabe **Manage Delivery Controllers** können Sie Ressourcen, die durch Citrix Virtual Apps and Desktops 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. Navigieren Sie auf der Windows-Startseite oder auf der Apps-Seite zur 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. Gehen Sie im Dialogfeld “Delivery Controller verwalten” folgendermaßen vor:
   a) Klicken Sie auf **Hinzufügen**, um Desktops und Apps aus einer anderen Citrix Virtual Apps and Desktops-Bereitstellung in den Store aufzunehmen.
   b) Klicken Sie auf **Bearbeiten**, um die Einstellungen für eine Bereitstellung zu ändern.
   c) Wählen Sie einen Eintrag in der Liste der Delivery Controller aus und klicken Sie auf **Entfernen**, um die Verfügbarkeit der Ressourcen der Bereitstellung im Store zu beenden.
4. Geben Sie im Dialogfeld “Delivery Controller hinzufügen” bzw. “Delivery Controller bearbeiten” einen **Anzeigenamen** an, anhand dessen Sie die Bereitstellung identifizieren können.
5. Um Desktops und Anwendungen, die von Citrix Virtual Apps and Desktops 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 Citrix Virtual Desktops-Sites die Details der Delivery Controller an. Listen Sie für Citrix Virtual Apps-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.
6. Es wird empfohlen, die Option **Server verwenden Lastausgleich** auszuwählen, damit die Last auf alle Delivery Controller in der Citrix Virtual Apps and Desktops-Site verteilt wird. StoreFront wählt bei jedem Start zufällig einen Delivery Controller aus der Serverliste und verteilt die Last auf alle Server der Citrix Virtual Apps and Desktops-Site. Wenn diese Option nicht ausgewählt ist, wird die Serverliste wie eine Failoverliste mit Prioritätsreihenfolge behandelt. In diesem Fall erfolgen 100 % der Starts auf dem ersten Delivery Controller in der Liste. Wenn dieser Server offline geht, werden 100 % der Starts mit dem zweiten Server in der Liste ausgeführt usw.
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 Citrix Virtual Apps and Desktops-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 Citrix Virtual Apps-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 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 dem Server verwenden soll. Der Standardport ist 80 für Verbindungen über HTTP und SSL-Relay bzw. 443 für HTTPS-Verbindungen. Bei Citrix Virtual Apps and Desktops-Servern muss der angegebene Port dem vom Citrix XML-Dienst verwendeten Port entsprechen.
9. Wenn Sie SSL-Relay verwenden, um Verbindungen zwischen StoreFront und Citrix Virtual Apps-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 Citrix Virtual Apps and Desktops-Bereitstellungen bieten. Wiederholen Sie erforderlichenfalls die Schritte 3 bis 9 zum Hinzufügen oder Ändern weiterer Bereitstellungen unter Delivery Controller.

Verwalten des Remotezugriffs auf Stores über Citrix Gateway

April 1, 2020

Mit der Aufgabe "Remotezugriffeinstellungen" können Sie den Zugriff auf Stores über Citrix Gateway für Benutzer in öffentlichen Netzwerken konfigurieren. Remotezugriff über Citrix 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. Navigieren Sie auf der Windows-Startseite oder auf der Apps-Seite zur Kachel Citrix StoreFront.

2. Wählen Sie im rechten 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 Citrix Gateway auf den Store zugreifen können.
   - Soll der Store Benutzern in öffentlichen Netzwerken nicht zur Verfügung stehen, deaktivieren Sie die Option **Remotezugriff aktivieren**. Nur lokale Benutzer im internen Netzwerk können dann auf den Store zugreifen.
   - Um den Remotezugriff zu ermöglichen, aktivieren Sie **Remotezugriff aktivieren**.
     - Wenn Sie Ressourcen, die über den Store angeboten werden, über Citrix Gateway verfügbar machen möchten, wählen Sie **Kein VPN-Tunnel** aus. Die Benutzer melden sich entweder über ICAProxy oder ein clientloses VPN (CVPN) bei Citrix Gateway an und benötigen das Citrix Gateway-Plug-In nicht für ein vollständiges VPN.
     - 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. Die Benutzer benötigen das Citrix Gateway-Plug-In für das Erstellen des VPN-Tunnels.

     Wenn Sie Remotezugriff auf den Store konfigurieren, wird automatisch die **Passthrough-Authentifizierung von Citrix Gateway** aktiviert. Die Benutzer authentifizieren sich bei Citrix Gateway und werden beim Zugriff auf ihre Stores automatisch angemeldet.
4. Wenn Sie Remotezugriff aktiviert haben, wählen Sie in der Liste **Citrix Gateway-Geräte** die Bereitstellungen aus, über die 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 14 fort.
5. Geben Sie auf der Seite “Allgemeine Einstellungen” einen **Anzeigenamen** für das Citrix Gateway-Gerät an, anhand dessen die Benutzer dieses erkennen können.

   Den Benutzern wird der Anzeigename angezeigt, den Sie in der Citrix Workspace-App angegeben haben. Nehmen Sie deshalb relevante Informationen in den Namen auf, damit die Benutzer leichter entscheiden können, ob sie das Gateway verwenden möchten. Beispielsweise können Sie den geographischen Standort in die Anzeigenamen der Citrix Gateway-Bereitstellungen einfügen, damit Benutzer problemlos das nächstgelegene Gateway für ihren Standort identifizieren können.
6. Geben Sie für **Citrix Gateway-URL** die URL:Port-Kombination des virtuellen Citrix Gateway-Servers Ihrer Bereitstellung ein. Wird kein Port angegeben, wird der Standard-`https://`-Port 443 verwendet. Port 443 muss in der URL nicht angegeben werden.

7. Wählen Sie aus den verfügbaren Optionen die Verwendung des Citrix Gateways aus.
   - **Authentifizierung und HDX-Routing:** Das Citrix Gateway wird für die Authentifizierung und das Routing von HDX-Sitzungen verwendet.
   - **Nur Authentifizierung:** Das Citrix Gateway wird nur für die Authentifizierung, jedoch nicht für das HDX-Sitzungsrouting verwendet.
   - **Nur HDX-Routing:** Das Citrix Gateway wird für das HDX-Routing, nicht aber für die Authentifizierung verwendet.
8. Liste Sie für alle Bereitstellungen, in denen Sie Ressourcen von Citrix Virtual Apps and Desktops oder XenApp 6.5 im Store verfügbar machen, auf der Seite **Secure Ticket Authority** (STA) alle 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 Citrix Virtual Apps and Desktops- bzw. XenApp 6.5-Servern gehostet und gibt Sitzungstickets als Reaktion auf Verbindungsanforderungen aus. Auf diesen Sitzungstickets basiert die Authentifizierung und Autorisierung für den Zugriff auf Citrix Virtual Apps and Desktops- bzw. XenApp 6.5-Ressourcen. Verwenden Sie die richtige STA URL (`HTTPS://` oder `HTTP://`) je nachdem, wie Ihre Delivery Controller konfiguriert sind. Die STA URL muss mit der in Citrix Gateway auf dem virtuellen Server konfigurierten URL identisch sein.
9. Wählen Sie für die STA Load Balancing aus. Sie können auch ein Zeitintervall festlegen, nach dem STAs, die nicht antworten, umgangen werden.
10. Um sicherzustellen, dass Citrix Virtual Apps and Desktops bzw. XenApp 6.5 getrennte Sitzungen aufrechterhält, während die Citrix Workspace-App eine automatische Wiederverbindung versucht, wählen Sie **Sitzungszuverlässigkeit aktivieren**.
11. Aktivieren Sie **Tickets von zwei Secure Ticket Authoritys anfordern (falls verfügbar)**, wenn Sie mehrere STAs konfigurieren und sicherstellen möchten, dass Sitzungszuverlässigkeit immer gegeben ist. StoreFront ruft dann Tickets von zwei verschiedenen Secure Ticket Authoritys ab und Benutzersitzungen werden nicht unterbrochen, 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.
12. Geben Sie auf der Seite **Authentifizierungseinstellungen** die **vServer-IP-Adresse** (VIP) des Citrix Gateway-Geräts ein.

    Verwenden Sie die private IP-Adresse des virtuellen Citrix Gateway-Servers und nicht die öffentliche, die der privaten per Netzwerkadressübersetzung zugeordnet ist. Gateways werden von StoreFront normalerweise über ihre URL identifiziert. Wenn Sie Global Server Load Balancing (GSLB) verwenden, müssen Sie die VIP jedem Gateway hinzufügen. Dadurch kann StoreFront mehrere Gateways identifizieren, die alle dieselbe URL (GSLB-Domänennamen) als sep-

arate Gateways verwenden. Beispielsweise können für den Store drei Gateways mit der URL `https://gslb.domain.com` konfiguriert werden, jedes hat jedoch eine eindeutige VIP (z. B. 10.0.0.1, 10.0.0.2 und 10.0.0.3).

13. Wenn Sie ein Gerät mit Citrix Gateway hinzufügen, wählen Sie aus der Liste **Anmeldetyp** die Authentifizierungsmethode aus, die Sie auf dem Gerät für Benutzer der Citrix Workspace-App konfiguriert haben.

    - 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** 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**.

14. Wenn Sie StoreFront für Citrix Gateway konfigurieren und SmartAccess verwenden möchten, müssen Sie eine **Callback-URL** eingeben. StoreFront fügt automatisch den Standardteil der URL an. Geben Sie die intern zugängliche URL des Geräts ein. StoreFront kontaktiert den Citrix Gateway-Authentifizierungsdienst, um zu überprüfen, ob von Citrix Gateway empfangene Anforderungen auch tatsächlich von diesem Gerät ausgehen.

    Bei Verwendung von GSLB empfiehlt es sich, eine eindeutige Callback-URL für jedes GSLB-Gateway zu konfigurieren. StoreFront muss jede eindeutige Callback-URL in die private VIP auflösen können, die für den jeweiligen virtuellen GSLB-Gateway-Server konfiguriert ist. Beispielsweise müssen `emeagateway.domain.com`, `usgateway.domain.com` und `apacgateway.domain.com` in die korrekte Gateway-VIP aufgelöst werden.

15. Klicken Sie auf **Erstellen**, um das Citrix Gateway-Gerät der Liste im Dialogfeld **Remotezugriffeinstellungen** hinzuzufügen.

    Die Informationen zur Konfiguration von Citrix Gateway-Geräten werden der CR-Provisioningdatei für den Store hinzugefügt. Dadurch kann die Citrix Workspace-App die richtige Verbindungsanforderung senden, wenn ein Gerät zum ersten Mal kontaktiert wird.

16. Wiederholen Sie erforderlichenfalls die Schritte 4 bis 13 zum Hinzufügen weiterer Citrix Gateway-Geräte zu der Liste. Wenn Sie Zugriff über mehrere Geräte aktivieren, indem Sie mehr als einen Eintrag in der Liste auswählen, geben Sie das **Standardgerät** für den Zugriff auf den Store an.

17. Klicken Sie auf **OK**, um die Konfiguration zu speichern und das Dialogfeld “Remotezugriff konfigurieren” zu schließen.

Überprüfung von Zertifikatsperrlisten

April 1, 2020

Einführung

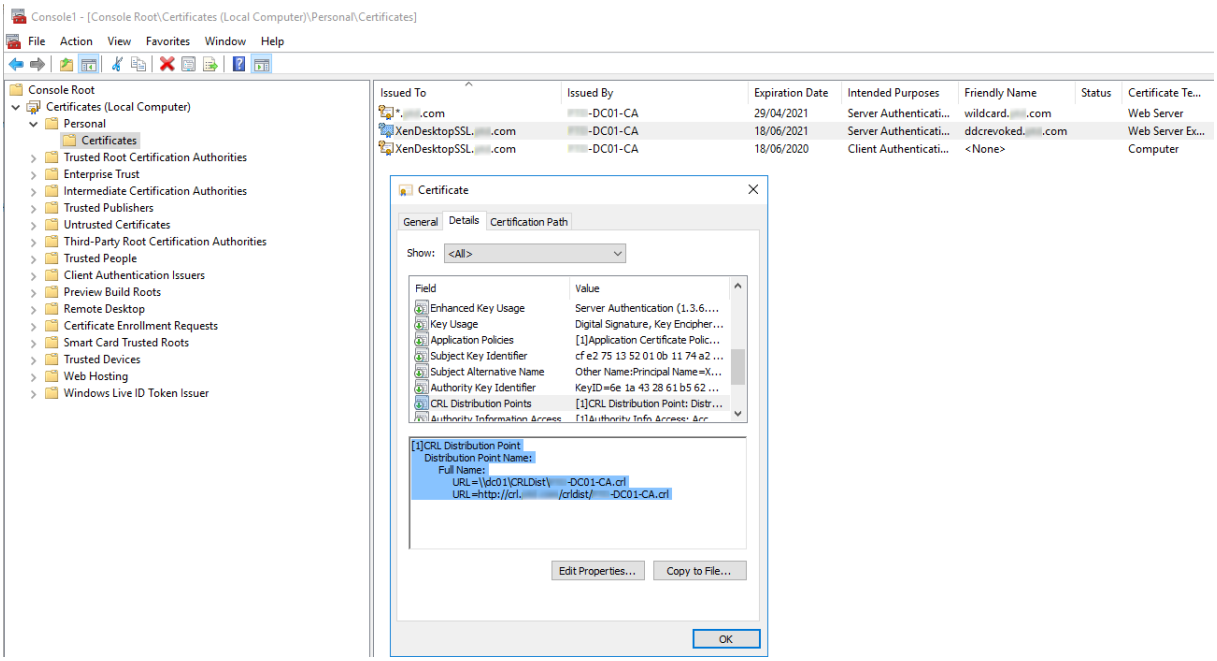
Sie können StoreFront so konfigurieren, dass der Status der von
Citrix Virtual Apps and Desktops-Delivery Controllern verwendeten TLS-Zertifikate anhand einer veröffentlichten Zertifikatssperrliste überprüft wird.
Sie müssen ggf. den Zugriff auf ein Zertifikat aus folgenden Gründen widerrufen:

- Sie vermuten, dass der private Schlüssel kompromittiert wurde.
- Die Zertifizierungsstelle wurde kompromittiert.
- Die Zugehörigkeit hat sich geändert.
- Das Zertifikat wurde ersetzt.

> **Hinweis:**
>
> Dieses Thema ist nur relevant, wenn zwischen StoreFront und
> Citrix Virtual Apps and Desktops-Delivery Controllern HTTPS-Verbindungen verwendet werden. HTTP-Verbindungen
> zu Delivery Controllern erfordern kein Zertifikat. Daher hat die hier beschriebene Einstellung -CertRevocationPolicy für den Store keine Auswirkungen.
>
> StoreFront unterstützt die Zertifikatsperrprüfung mithilfe von CDP-Erweiterungen und lokal installierten
> Zertifikatsperrlisten. StoreFront unterstützt keine Delta-Sperrlisten, sondern nur vollständige Zertifikatsperrlisten.

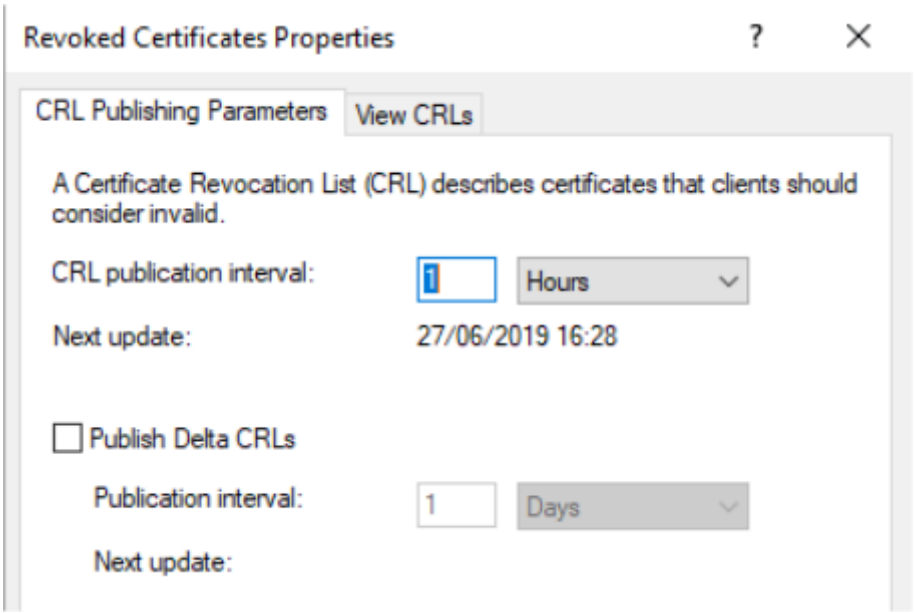
CDP-Erweiterungen

StoreFront listet keine Ressourcen von Citrix Virtual Apps and Desktops-
Delivery Controllern auf, die gesperrte Zertifikate verwenden, deren Seriennummern in der veröffentlichten Zertifikatsperrliste aufgeführt
sind. Um zu erkennen, welche Zertifikate gesperrt wurden, muss
StoreFront über eine der in den CDP-Zertifikaterweiterungen
definierten URLs auf die veröffentlichte Zertifikatsperrliste zugreifen können.



Zertifikatsperrlisten-Veröffentlichungsintervall

Damit StoreFront gesperrte Zertifikate auf Delivery Controllern schneller erkennt, verringern Sie das Intervall der Veröffentlichung der Zertifizierungsstelle. Legen Sie in den Eigenschaften der CDP-Erweiterung einen niedrigeren , für Ihre PKI geeigneten Wert für das Zertifikatsperrlisten-Veröffentlichungsintervall fest.



Caching der Zertifikatsperrliste auf Clients

Der Windows-PKI-Client speichert Zertifikatsperrlisten lokal zwischen. Eine neue Zertifikatsperrliste wird erst heruntergeladen, wenn die lokal zwischengespeicherte abgelaufen ist.

StoreFront-Zugriff auf Zertifikatsperrlisten

Zur Überprüfung auf Zertifikatsperrungen muss StoreFront auf Zertifikatsperrlisten zugreifen können. Überlegen Sie, wie StoreFront den Webserver oder die Zertifizierungsstelle, die die Zertifikatsperrliste veröffentlicht, kontaktieren soll und wie StoreFront Zertifikatsperrlistenupdates erhalten soll.

Interne Unternehmenszertifizierungsstellen und private Zertifikate auf Delivery Controllern

Zur Verwendung privater Zertifizierungsstellen und Zertifikate benötigt StoreFront eine ordnungsgemäß konfigurierte Unternehmenszertifizierungsstelle und eine veröffentlichte Zertifikatsperrliste, auf die es innerhalb der Organisation im internen Netzwerk zugreifen kann. Informationen zum Konfigurieren einer Unternehmenszertifizierungsstelle zum Veröffentlichen von CDP-Erweiterungen finden Sie in der Microsoft-Dokumentation. Zertifikate auf Delivery Controllern, die vorhanden waren, bevor die Zertifizierungsstelle für CDP-Erweiterungen konfiguriert wurde, müssen möglicherweise neu ausgestellt werden.

StoreFront- und Citrix Virtual Apps and Desktops-Server sind normalerweise in isolierten privaten Netzwerken ohne Zugriff auf das Internet. In einem solchen Szenario sollten private Zertifizierungsstellen verwendet werden.

Externe öffentliche Zertifizierungsstellen und öffentliche Zertifikate auf Delivery Controllern

StoreFront-Server und Citrix Virtual Apps and Desktops-Delivery Controller können Zertifikate verwenden, die von öffentlichen Zertifizierungsstellen ausgestellt wurden. StoreFront muss Zugang zu dem Webserver der öffentlichen Zertifizierungsstelle über das Internet unter Verwendung der in den CDP-Erweiterungen referenzierten URLs haben. Wenn StoreFront keine Kopie der Zertifikatsperrliste anhand einer CDP-URL herunterladen kann, nachdem ein öffentliches Zertifikat gesperrt wurde, kann StoreFront die Zertifikatsperrprüfung nicht durchführen.

Einstellungen der Richtlinie “Zertifikatsperrüberprüfung”

Verwenden Sie die Citrix StoreFront-PowerShell-Cmdlets **Get-STFStoreFarmConfiguration** und **Set-STFStoreFarmConfiguration** zum Festlegen der Richtlinie “Zertifikatsperrüberprüfung” für einen Store. Mit **Get-Help Set-STFStoreFarmConfiguration -detailed** werden die PowerShell-Hilfe und Beispiele mit der Option -CertRevocationPolicy angezeigt. Weitere Informationen zu den StoreFront-PowerShell-Cmdlets finden Sie unter Citrix StoreFront SDK PowerShell Modules.

Die Option **-CertRevocationPolicy** kann auf die folgenden Werte eingestellt werden:

Einstellung	Beschreibung
NoCheck	StoreFront überprüft das Zertifikat auf dem Delivery Controller nicht auf seinen Sperrstatus. StoreFront listet weiterhin Ressourcen von Delivery Controllern auf, die gesperrte Zertifikate verwenden. Dies ist die Standardeinstellung.
MustCheck	Dies ist die sicherste Option. StoreFront versucht, eine Zertifikatsperrliste abzurufen, indem es die URLs aufruft, auf die in den CDP-Erweiterungen des Zertifikats auf dem Delivery Controller verwiesen wird. StoreFront kann nichts von dem Delivery Controller auflisten, wenn die Zertifikatsperrliste nicht verfügbar ist oder das auf dem Delivery Controller verwendete Zertifikat gesperrt ist. Die URL kann auf einen internen Webserver verweisen, wenn das Zertifikat privat ist, oder auf einen öffentlichen Internet-Webserver, wenn das Zertifikat von einer öffentlichen Zertifizierungsstelle ausgestellt wurde.

Einstellung	Beschreibung
FullCheck	StoreFront versucht die URLs aufzurufen, die in den CDP-Erweiterungen des Zertifikats auf dem Delivery Controller veröffentlicht sind. Kann StoreFront keine Kopie der Zertifikatsperrliste von den URLs abrufen, gestattet es weiterhin die Auflistung der Ressourcen von dem Delivery Controller. Ruft StoreFront die Zertifikatsperrliste erfolgreich ab und wurde das Zertifikat des Delivery Controllers gesperrt, listet StoreFront keine Ressourcen auf. Die URL kann auf einen internen Webserver verweisen, wenn das Zertifikat privat ist, oder auf einen öffentlichen Internet-Webserver, wenn das Zertifikat von einer öffentlichen Zertifizierungsstelle ausgestellt wurde.
NoNetworkAccess	Es werden nur Zertifikatsperrlisten geprüft, die lokal in den Citrix Delivery Controller-Zertifikatspeicher auf dem StoreFront-Server importiert wurden. StoreFront versucht nicht, die in den CDP-Erweiterungen angegebenen URLs aufzurufen. Kann StoreFront keine lokale Kopie der Zertifikatsperrliste abrufen, gestattet es weiterhin die Auflistung der Ressourcen von dem Delivery Controller. Ruft StoreFront die lokale Zertifikatsperrliste erfolgreich aus dem Citrix Delivery Controller-Zertifikatspeicher ab und wurde das Zertifikat des Delivery Controllers gesperrt, listet StoreFront keine Ressourcen auf.

Konfigurieren eines Stores für die Überprüfung der Zertifikatsperrlisten

Um die Richtlinie “Zertifikatsperrüberprüfung” für einen Store festzulegen, öffnen Sie die PowerShell ISE

mit dem Befehl **Als Administrator ausführen** und führen Sie dann die folgenden PowerShell-Cmdlets aus. Wenn Sie
mehrere Stores haben, wiederholen Sie diesen Vorgang für alle. -CertRevocationPolicy ist eine Einstellung
auf Storeebene, die sich auf alle Delivery Controller auswirkt, die für den in $StoreVirtualPath angegebenen
Store konfiguriert wurden.

```
$SiteID = 1
$StoreVirtualPath = "/Citrix/Store"
$StoreObject = Get-STFStoreService -SiteId $SiteID -VirtualPath
$StoreVirtualPath
Set-STFStoreFarmConfiguration -StoreService $StoreObject -
    CertRevocationPolicy
"MustCheck"
```

Führen Sie folgenden Befehl aus, um zu überprüfen, ob die Einstellung richtig angewendet wurde oder um die aktuelle
-CertRevocationPolicy-Konfiguration anzuzeigen:

```
(Get-STFStoreFarmConfiguration -StoreService $StoreObject).
    CertRevocationPolicy
```

Verwenden lokal importierter Zertifikatsperrlisten auf dem StoreFront-Server

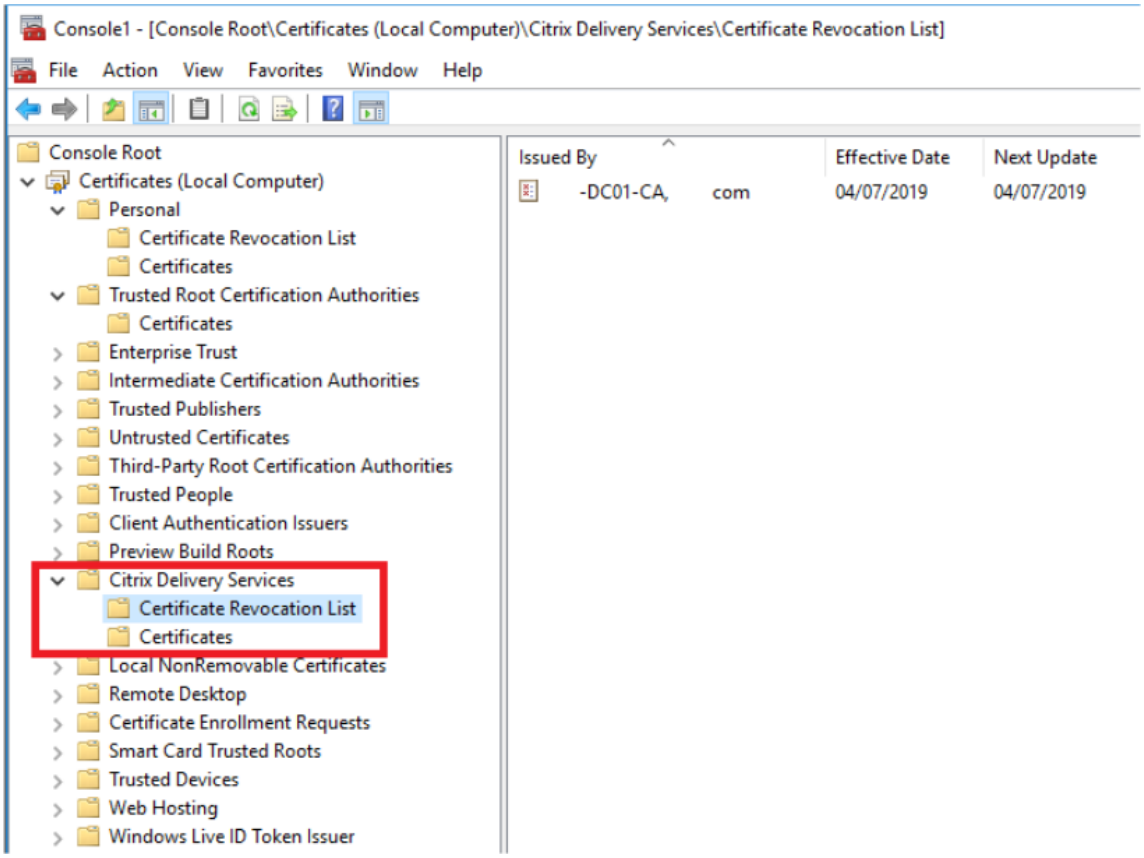
Die Verwendung lokal importierter Zertifikatsperrlisten wird unterstützt, von Citrix jedoch aus folgenden
Gründen nicht empfohlen:

- Die Verwaltung und Aktualisierung ist in großen Bereitstellungen schwierig, in denen möglicherweise mehrere StoreFront-Servergruppen vorliegen.
- Das manuelle Aktualisieren von Zertifikatsperrlisten auf jedem StoreFront-Server bei jeder Sperrung eines Zertifikats
  ist viel weniger effizient als die Verwendung von CDP-Erweiterungen und veröffentlichten Zertifikatsperrlisten in der gesamten Active Directory-Domäne.

Lokal installierte oder aktualisierte Zertifikatsperrlisten können verwendet werden, wenn -CertRevocationPolicy auf "NoNetworkAccess"
festgelegt ist und Sie die Zertifikatsperrliste
effizient an alle StoreFront-Server verteilen können.

Verwenden lokal importierter Zertifikatsperrlisten

1. Kopieren Sie die Zertifikatsperrliste auf den Desktop des StoreFront-Servers. Wenn der StoreFront-Server
   Teil einer Servergruppe ist, kopieren Sie sie auf alle Server in der Gruppe.
2. Öffnen Sie das MMC-Snap-In und wählen Sie **Datei > Snap-In hinzufügen/entfernen > Zertifikate > Computerkonto > Citrix Delivery Services certificate store**.
3. Klicken Sie mit der rechten Maustaste und wählen Sie **Alle Tasks > Importieren**, navigieren Sie zur Zertifikatsperrlistendatei
   und wählen Sie **Alle Dateien auswählen > Öffnen > Alle Zertifikate in folgendem Speicher speichern > Citrix Delivery Services**.



Hinzufügen der Zertifikatsperrliste zum Citrix Delivery Services-Zertifikatspeicher per PowerShell oder Befehlszeile

1. Melden Sie sich bei StoreFront an und kopieren Sie die Zertifikatsperrlistendatei auf den Desktop des aktuellen
   Benutzers.

2. Öffnen Sie die PowerShell ISE und wählen Sie **Als Administrator ausführen**.
3. Führen Sie folgenden Befehl aus:

```
certutil -addstore "Citrix Delivery Services" "$env:UserProfile\
    Desktop\Example-DC01-CA.crl"
```

Bei Erfolg wird Folgendes zurückgegeben:

```
Citrix Delivery Services
CRL "CN=Example-DC01-CA, DC=example, DC=com" added to store.
CertUtil: -addstore command completed successfully.
```

Sie können diesen Befehl als Grundlage verwenden, um die Zertifikatsperrliste automatisch per Skript an alle
StoreFront-Server in Ihrer Bereitstellung zu verteilen.

XML-Authentifizierung mit Delivery Controllern

Sie können StoreFront so konfigurieren, dass die Benutzerauthentifizierung an Citrix Virtual Apps and Desktops-Delivery Controller delegiert wird. Die Benutzer werden daran gehindert, sich bei StoreFront anzumelden, wenn das Zertifikat auf dem Delivery Controller gesperrt wurde. Dieses Verhalten ist wünschenswert, da Active Directory-Benutzer sich nicht bei StoreFront anmelden können sollten, wenn das Zertifikat auf dem Citrix Virtual Apps and Desktops-Delivery Controller, das für ihre Authentifizierung verantwortlich ist, gesperrt wurde.

Delegieren der Benutzerauthentifizierung an Delivery Controller

1. Konfigurieren Sie den Store für die Zertifikatsperrung wie im vorherigen Abschnitt Konfigurieren eines Stores für die Überprüfung der Zertifikatsperrlisten beschrieben.
2. Konfigurieren Sie den Delivery Controller für die Verwendung von HTTPS (Verfahren siehe Authentifizierung auf Basis des XML-Diensts).

Konfigurieren des XML-Authentifizierungsdiensts für die Überprüfung der Zertifikatsperrlisten

Diese Schritte sind nur erforderlich, wenn Sie XML-Authentifizierung in Ihrer Bereitstellung verwenden.

> **Hinweis:**
>
> StoreFront unterstützt zwei Modelle zum Zuordnen von Stores zu einem Authentifizierungsdienst. Der empfohlene Ansatz ist die Eins-zu-Eins-Zuordnung zwischen Store und Authentifizierungsdienst. In diesem Fall müssen Sie die Schritte in diesem Abschnitt für alle Stores und zugehörigen Authentifizierungsdienste ausführen.
>
> Stellen Sie sicher, dass Sie den Zertifikatsperrmodus für Store und Authentifizierungsdienst auf denselben Wert festlegen. Ist die Authentifizierungskonfiguration für alle Stores identisch, können mehrere Stores zur gemeinsamen Verwendung eines einzelnen Authentifizierungsdiensts konfiguriert werden.

Die PowerShell-Cmdlets für Authentifizierungsdienste besitzen kein Äquivalent zu **Set-STFStoreFarmConfiguration**. Daher ist ein etwas anderer PowerShell-Ansatz erforderlich. Verwenden Sie die gleichen, im vorherigen Abschnitt beschriebenen Einstellungen der Richtlinie "Zertifikatsperrüberprüfung".

1. Öffnen Sie die PowerShell ISE und wählen Sie **Als Administrator ausführen**.

```
$SiteID = 1
$StoreVirtualPath = "/Citrix/Store"
$AuthVirtualPath = "/Citrix/StoreAuth"
```

2. Wählen Sie den Storedienst, den Authentifizierungsdienst und den Delivery Controller für die XML-Authentifizierung aus. Stellen Sie sicher, dass der Delivery Controller bereits für den Store konfiguriert ist.

```
$StoreObject = Get-STFStoreService -SiteId $SiteID -VirtualPath
    $StoreVirtualPath
$FarmObject = Get-STFStoreFarm -StoreService $StoreObject -
    FarmName "CVAD"
$AuthObject = Get-STFAuthenticationService -SiteID $SiteID -
    VirtualPath $AuthVirtualPath
```

3. Ändern Sie direkt die CertRevocationPolicy-Eigenschaft des Authentifizierungsdiensts.

```
$AuthObject.FarmsConfiguration.CertRevocationPolicy = "FullCheck"
$AuthObject.Save()
Enable-STFXmlServiceAuthentication -AuthenticationService
    $AuthObject -Farm $FarmObject
```

4. Prüfen Sie, ob Sie den richtigen Zertifikatsperrmodus festgelegt haben.


```
$AuthObject = Get-STFAuthenticationService -SiteID 1 -VirtualPath
    $AuthVirtualPath
$AuthObject.FarmsConfiguration.CertRevocationPolicy
```

Erwartungsgemäße Fehler in der Windows-Ereignisanzeige

Wenn die Zertifikatsperrlisten-Überprüfung aktiviert ist, werden Fehler in der Windows-Ereignisanzeige auf
dem StoreFront-Server gemeldet.

Öffnen der Ereignisanzeige:

- Geben Sie auf dem StoreFront-Server **run** ein.
- Geben Sie **eventvwr** ein und drücken Sie die Eingabetaste.
- Suchen Sie unter “Anwendungen und Dienste” nach Citrix Delivery Services-Ereignissen.

Beispiel: Store cannot contact a delivery controller with a revoked certificate

```
An SSL connection could not be established: An error occurred during
    SSL
crytography: Access is denied.

This message was reported from the Citrix XML Service at address
https://deliverycontrollerTLS.domain.com/scripts/wpnbr.dll.

The specified Citrix XML Service could not be contacted and has been
    temporarily
removed from the list of active services.
```

Beispiel für einen Fehler von Receiver für Web, wenn sich ein Benutzer aufgrund fehlgeschlagener XML-Authentifizierung nicht anmelden kann

```
An unexpected response was received during the authentication process.

Citrix.DeliveryServicesClients.Authentication.Exceptions.
    ExplicitAuthenticationFailure,
Citrix.DeliveryServicesClients.Authentication, Version=3.20.0.0,
Culture=neutral, PublicKeyToken=null

General Authentication Failure

```



```
ExplicitResult.State: 5

AuthenticationControllerRequestUrl:
https://storefront.example.com/Citrix/StoreWeb/ExplicitAuth/
   LoginAttempt

ActionType: LoginAttempt

at
Citrix.Web.AuthControllers.Controllers.ExplicitAuthController.
   GetExplicitAuthResult(ActionType
type, Dictionary‘2 postParams)
```

Konfigurieren zweier StoreFront-Stores zur gemeinsamen Nutzung eines Abonnementdatenspeichers

April 1, 2020

Bei der StoreFront-Installation wird lokal auf jedem StoreFront-Server ein Windows-Datenspeicher für die Abonnementdaten 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 erstellt StoreFront einen Datenspeicher für jeden Store. 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 Citrix 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 den entsprechenden Abonnementdatenspeichern muss ein Benutzer dieselbe 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.

```
<clientEndpoint uri=”net.pipe://localhost/Citrix/Subscriptions/1__Citrix_<
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 Citrix Virtual Apps and Desktops-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:

```
1 <subscriptionsStoreClient enabled=”true”>
2 <clientEndpoint uri=”net.pipe://localhost/Citrix/Subscriptions/1
     __Citrix_External” authenticationMode=”windows” transferMode=”
     Streamed”>
3 <clientCertificate thumbprint=”0” />
4 </clientEndpoint>
5 </subscriptionsStoreClient>
```

2. Ändern Sie extern so, dass es dem internen Storeendpunkt entspricht:

```
1 <subscriptionsStoreClient enabled=”true”>
2 <clientEndpoint uri=”net.pipe://localhost/Citrix/Subscriptions/1
     __Citrix_Internal” authenticationMode=”windows” transferMode=”
     Streamed”>
3 <clientCertificate thumbprint=”0” />
4 </clientEndpoint>
5 </subscriptionsStoreClient>
```

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.

Verwalten von Abonnementdaten für einen Store

April 1, 2020

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. Citrix empfiehlt 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 jedem StoreFront-Server zum Abonementstoreordner: `C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\SubscriptionsStore\1__Citrix_<StoreName>`
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.

```
function Remove-SubscriptionData

{

        [CmdletBinding()]

```



```
7           [Parameter(Mandatory=$False)][String]$Store = "Store"
8
9           $SubsService = "Citrix Subscriptions Store"
10
11          # Path to Subscription Data in StoreFront version 2.6 or later
12
13          $SubsPath = "C:\Windows\ServiceProfiles\NetworkService\AppData\
                Roaming\Citrix\SubscriptionsStore\1__Citrix_$Store*"
14
15          Stop-Service -displayname $SubsService
16
17          Remove-Item $SubsPath -Force -Verbose
18
19          Start-Service -displayname $SubsService
20
21          Get-Service -displayname $SubsService
22  }
23
24
25      Remove-SubscriptionData -Store "YourStore"
```

Exportieren von Abonnementdaten

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

```
1 $StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/citrix/<
      yourstore>"
2
3 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 wiederher-

stellen, die Sie zuvor mit Export-STFStoreSubscriptions erstellt haben.

```
1 $StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/citrix/<
     yourstore>"
2
3 Restore-STFStoreSubscriptions -StoreService $StoreObject -FilePath "
     $env:USERPROFILE\Desktop\Subscriptions.txt"
```

Weitere Informationen zu Restore-STFStoreSubscriptions finden Sie unter https://developer-docs.citrix.com/projects/storefront-powershell-sdk/en/latest/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.

```
1 $StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/citrix/<
    yourstore>"
2
3 Import-STFStoreSubscriptions -StoreService $StoreObject -FilePath "$env
    :USERPROFILE\Desktop\Subscriptions.txt"
```

Weitere Informationen zu Import-STFStoreSubscriptions finden Sie unter https://developer-docs.citrix.com/projects/storefront-powershell-sdk/en/latest/Import-STFStoreSubscriptions/

Details in der Abonnementdatendatei

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

`<user-identifier> <resource-id> <subscription-id> <subscription-status> <property-name> <property-value> <property-name> <property-value> ...`

Wobei:

- `<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 property-name-/property-value-Wertepaare. Diese repräsentieren Eigenschaften eines Abonnements durch einen StoreFront-Client (normalerweise eine Citrix Workspace-App). 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 den 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

Leistungsindikatoren für Storeabonnements

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

```
1 Get-Counter -Counter ”\Citrix Subscription Store(1__citrix_store)\
     Subscription Entries Count (including unpurged deleted records)”
2
3 Get-Counter -Counter ”\Citrix Subscription Store Synchronization\
     Subscriptions Store Synchronizing”
4
5 Get-Counter -Counter ”\Citrix Subscription Store Synchronization\Number
      Subscriptions Synchronized”
6
7 Get-Counter -Counter ”\Citrix Subscription Store Synchronization\Number
      Subscriptions Transferred”
```


Speichern von Abonnementdaten mit Microsoft SQL Server

April 1, 2020

> **Hinweis:**
>
> Dieses Dokument setzt Grundkenntnisse in MS SQL Server und T-SQL-Abfragen voraus. Administratoren müssen mit der Konfiguration, Verwendung und Verwaltung von SQL Server vertraut sein, bevor sie die Informationen dieses Dokuments nutzen.

Einführung

ESENT ist eine einbettbare transaktionale Datenbankengine, die von Windows verwendet werden kann. Alle Versionen von StoreFront unterstützen standardmäßig die Verwendung einer integrierten ESENT-Datenbank. Sie können auch eine Verbindung zu einer Microsoft SQL Server-Instanz herstellen, wenn der Store zur Verwendung einer SQL-Verbindungszeichenfolge konfiguriert ist.

Der Hauptvorteil des Umstiegs von ESENT auf SQL in StoreFront besteht darin, dass Abonnementdatensätze mit T-SQL-Update-Anweisungen verwaltet, geändert und gelöscht werden können. Wenn Sie SQL verwenden, müssen Sie für geringfügige Änderungen an den Abonnementdaten nicht die gesamten ESENT-Abonnementdaten exportieren, ändern und wieder importieren.

Um Abonnementdaten von ESENT nach Microsoft SQL Server zu migrieren, müssen die aus StoreFront exportierten ESENT-Flat-Daten in ein SQL-freundliches Format für den Massenimport umgewandelt werden. Bei neuen Bereitstellungen ohne neue Abonnementdaten ist dieser Schritt nicht erforderlich. Die Datentransformation ist nur einmal erforderlich. In diesem Artikel wird die für StoreFront-Versionen ab Version 3.5 (mit der das hier genannte PowerShell-SDK -STF eingeführt wurde) unterstützte Konfiguration beschrieben.

> **Hinweis:**
>
> Fehler beim Herstellen der Verbindung mit der zum Speichern der Abonnementdaten verwendeten SQL Server-Instanz aufgrund von Netzwerkausfällen machen die StoreFront-Bereitstellung nicht unbrauchbar. Ausfälle führen lediglich zu einer vorübergehend verschlechterten Benutzererfahrung: Die Benutzer können keine bevorzugten Ressourcen hinzufügen, entfernen oder anzeigen, bis die Verbindung zu SQL Server wiederhergestellt wurde. Ressourcen können während eines Ausfalls weiterhin angezeigt und gestartet werden. Das erwartete Verhalten ist mit dem identisch, wenn bei Verwendung von ESENT der Citrix Subscription Store-Dienst beendet wird.
>
> **Tipp:**
>
> Mit KEYWORDS:Auto oder KEYWORDS:Mandatory konfigurierte Ressourcen verhalten sich bei

> Verwendung von ESENT und SQL gleich. Neue SQL-Abonnementdatensätze werden automatisch erstellt, wenn sich ein Benutzer zum ersten Mal anmeldet, wenn ein KEYWORD in den Ressourcen des Benutzers enthalten ist.

Vorteile von ESENT und SQL Server

ESENT	SQL
Standard, erfordert keine zusätzliche Konfiguration zur direkten Verwendung von StoreFront.	Wesentlich besser verwaltbar, Abonnementdaten können mühelos mit T-SQL-Abfragen bearbeitet oder aktualisiert werden. Ermöglicht das Löschen oder Aktualisieren von Datensätzen pro Benutzer. Ermöglicht das einfache Zählen von Datensätzen pro Anwendung, Delivery Controller oder Benutzer. Bietet einfaches Verfahren zum Löschen unnötiger Benutzerdaten, wenn Benutzer das Unternehmen verlassen. Einfache Möglichkeit zur Aktualisierung von Delivery Controller-Referenzen, z. B. wenn der Administrator auf Aggregation umstellt oder neue Delivery Controller bereitgestellt werden.
Einfachere Konfiguration der Replikation zwischen verschiedenen Servergruppen mithilfe von Abonnement-Synchronisierungs- und Pull-Zeitplänen. Siehe Konfigurieren der Abonnementsynchronisierung	Von StoreFront entkoppelt, sodass kein Backup der Abonnementdaten vor StoreFront-Upgrades erforderlich ist, da die Daten auf einem separaten SQL Server-Rechner verwaltet werden. Abonnementbackups sind unabhängig von StoreFront und verwenden SQL-Backupstrategien und -mechanismen.
SQL ist nicht nötig, wenn keine Abonnementverwaltung erforderlich ist. Wenn die Abonnementdaten nie aktualisiert werden müssen, erfüllt ESENT wahrscheinlich die Kundenanforderungen.	Eine Kopie der Abonnementdaten wird von allen Mitgliedern der Servergruppe gemeinsam genutzt, sodass die Wahrscheinlichkeit von Unterschieden bei Daten auf den Servern und von Synchronisierungsproblemen geringer ist.

Nachteile von ESENT und SQL Server

ESENT	SQL
Keine einfache Möglichkeit, Abonnementdaten detailliert zu verwalten. Bearbeitung der Abonnementdaten in exportierten TXT-Dateien erforderlich. Die gesamte Abonnementdatenbank muss exportiert und wieder importiert werden. Möglicherweise müssen Tausende von Datensätzen per Suche und Ersetzen geändert werden, was arbeitsintensiv und fehleranfällig ist.	Erfordert grundlegende SQL-Kenntnis und -Infrastruktur. Erfordert evtl. den Erwerb einer SQL-Lizenz, was die Gesamtbetriebskosten für die StoreFront Bereitstellung erhöht. Allerdings kann eine Citrix Virtual Apps and Desktops Datenbankinstanz auch für StoreFront verwendet werden, um Kosten zu senken.
Eine Kopie der ESENT-Datenbank muss auf jedem StoreFront-Server einer Servergruppe verwaltet werden. In seltenen Fällen kann diese Datenbank innerhalb einer Servergruppe oder zwischen verschiedenen Servergruppen asynchron werden.	Das Replizieren von Abonnementdaten zwischen Servergruppen ist eine nicht ganz einfache Bereitstellungsaufgabe. Es erfordert pro Datencenter mehrere SQL-Instanzen und die Transaktionsreplikation zwischen diesen. Hierfür ist MS SQL-Fachwissen erforderlich.
	Datenmigration aus ESENT und Umwandlung in SQL-freundliches Format erforderlich. Dieser Vorgang ist nur einmal erforderlich.
	Zusätzliche Windows-Server und -Lizenzen möglicherweise erforderlich.
	Zusätzliche Schritte zum Bereitstellen von StoreFront.

Bereitstellungsszenarios

> **Hinweis:**
>
> Jeder in StoreFront konfigurierte Store erfordert entweder eine ESENT-Datenbank oder eine Microsoft SQL-Datenbank, wenn Sie Benutzerabonnements unterstützen möchten. Die Methode zum Speichern der Abonnementdaten wird in StoreFront auf Store-Ebene festgelegt.

Citrix empfiehlt, alle Store-Datenbanken in derselben Microsoft SQL Server-Instanz zu führen, um die Verwaltung zu vereinfachen und das Potenzial von Fehlkonfigurationen zu verringern.

Stores können dieselbe Datenbank gemeinsam nutzen, vorausgesetzt, sie sind zur Verwendung derselben Verbindungszeichenfolge konfiguriert. Es spielt keine Rolle, ob sie unterschiedliche Delivery Controller verwenden. Der Nachteil der Verwendung einer Datenbank durch mehrere Stores besteht darin, dass nicht erkennbar ist, welchem Store die einzelnen Abonnementdatensätze entsprechen.

Eine Kombination beider Datenspeichermethoden in einer einzelnen StoreFront-Bereitstellung mit mehreren Stores ist technisch möglich. Ein Speicher kann für ESENT und ein zweiter für SQL konfiguriert werden. Das wird aufgrund der komplexeren Verwaltung und des Potenzials für Fehlkonfigurationen nicht empfohlen.

Zum Speichern von Abonnementdaten in SQL
Server gibt es vier Szenarien:

Szenario 1: Einzelner StoreFront -Server oder Servergruppe mit ESENT (Standard)

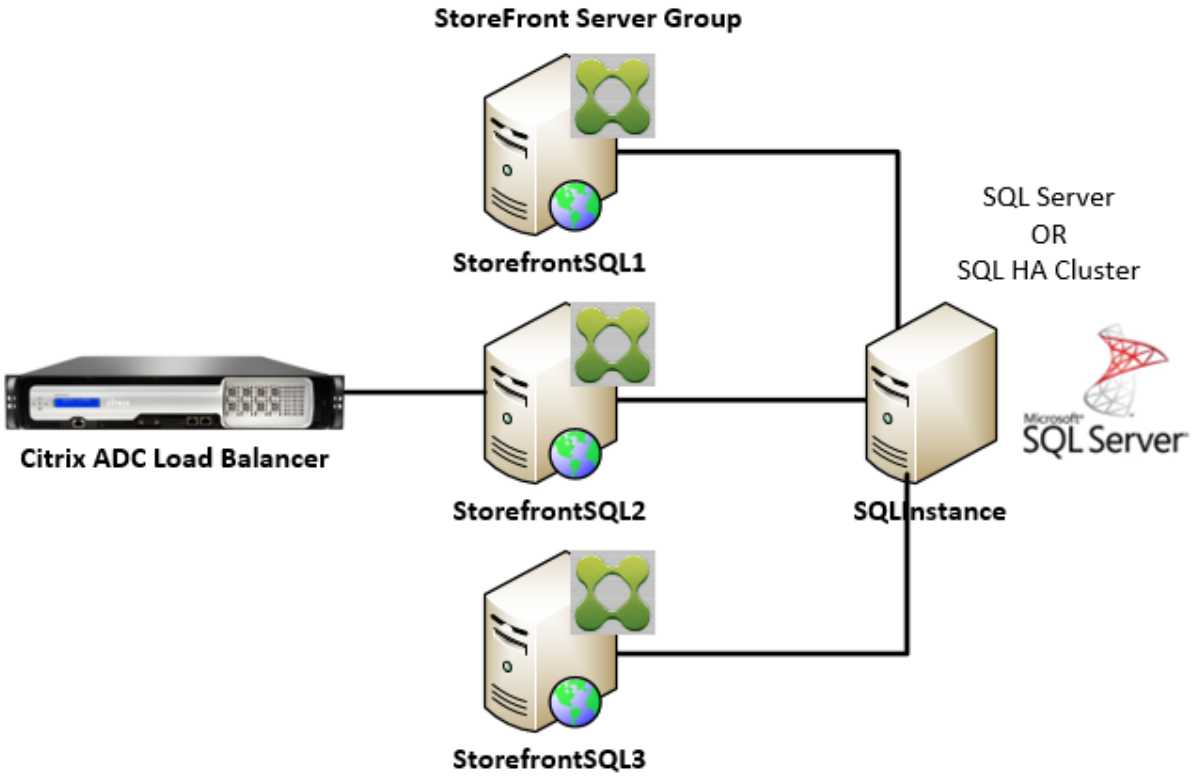
Standardmäßig verwenden alle Versionen von StoreFront ab 2.0 eine ESENT-Flat-Datenbank, um Abonnementdaten einer Servergruppe zu speichern und zu replizieren. Auf jedem Mitglied der Servergruppe wird eine identische Kopie der Abonnementdatenbank geführt und mit allen anderen Mitgliedern der Servergruppe synchronisiert. Dieses Szenario erfordert keine zusätzliche Konfiguration. Das Szenario eignet sich für die meisten Kunden, bei denen keine häufigen Änderungen an Delivery Controller-Namen und keine häufigen Verwaltungsaufgaben an Abonnementdaten (Entfernen oder Aktualisieren alter Benutzerabonnements) zu erwarten sind.

Szenario 2: Einzelner StoreFront-Server und lokal installierte Microsoft SQL Server-Instanz

StoreFront verwendet eine lokal installierte SQL Server-Instanz und beide Komponenten befinden sich auf demselben Server. Dieses Szenario eignet sich für eine einfache StoreFront-Bereitstellung, bei der häufig Änderungen an Delivery Controller-Namen oder Verwaltungsschritte wie Entfernen oder Aktualisieren von Abonnementdaten nötig sind, jedoch keine hohe Verfügbarkeit der StoreFront-Bereitstellung erforderlich ist. Citrix empfiehlt dieses Szenario nicht für Servergruppen, da damit ein zentraler Ausfallpunkt auf dem Servergruppenmitglied entsteht, das die Microsoft SQL-Datenbankinstanz hostet. Das Szenario ist nicht für große Enterprise-Bereitstellungen geeignet.

Szenario 3: StoreFront-Servergruppe und eine dedizierte, für hohe Verfügbarkeit konfigurierte Microsoft SQL Server-Instanz (empfohlen)

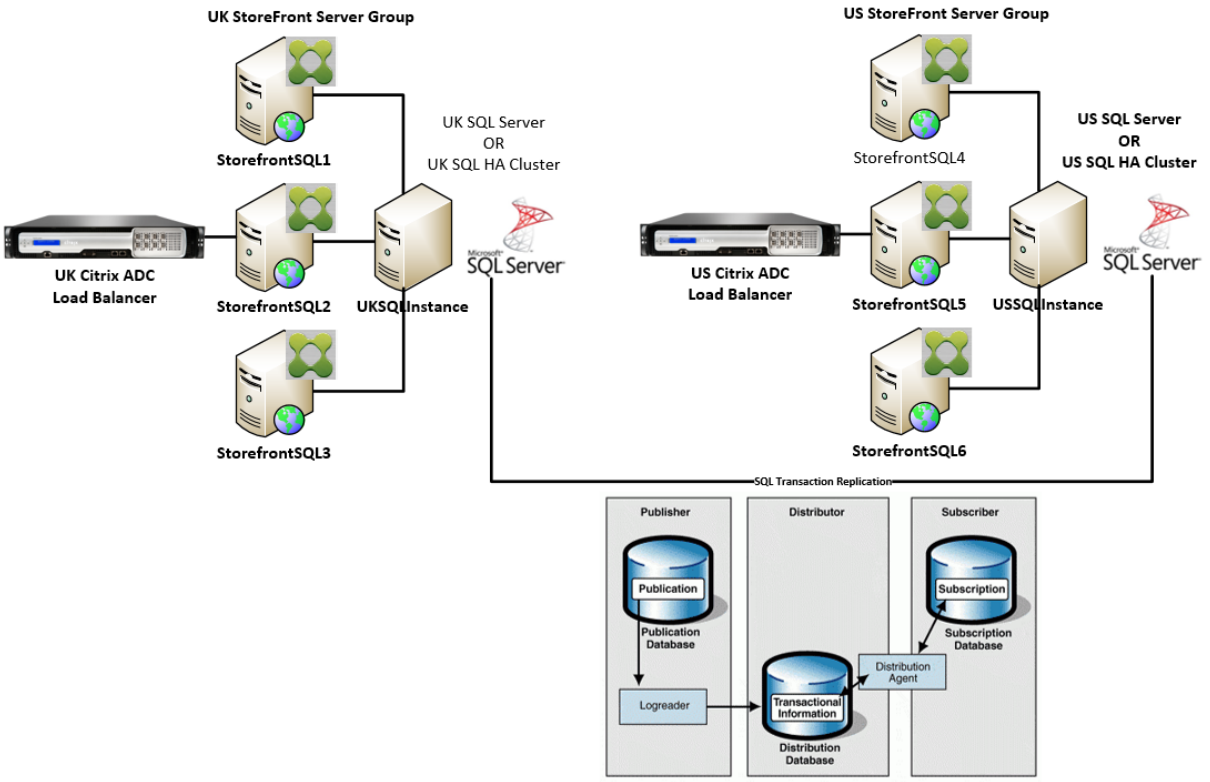
Alle Mitglieder der StoreFront-Servergruppe stellen eine Verbindung mit derselben dedizierten Microsoft SQL Server-Instanz bzw. einem SQL-Failovercluster her. Dies ist das am besten geeignete Modell für große Enterprise-Bereitstellungen, in denen Citrix Administratoren häufig Änderungen an Delivery Controller-Namen vornehmen oder häufig Verwaltungsaufgaben an Abonnementdaten ausgeführt werden (z. B. Entfernen oder Aktualisieren) und die hohe Verfügbarkeit erfordern.



Szenario 4: Mehrere StoreFront-Servergruppen und eine dedizierte Microsoft SQL Server-Instanz für jede Servergruppe in jedem Datencenter

> **Hinweis:**
>
> Dies ist eine fortgeschrittene Konfiguration. Sie sollte nur von erfahrenen SQL Server-Administratoren erstellt werden, die mit der Transaktionsreplikation vertraut sind und über die erforderlichen Kenntnisse verfügen.

Das Szenario ähnelt Szenario 3, erweitert auf Umgebungen, in denen mehrere StoreFront-Servergruppen in verschiedenen Datencentern erforderlich sind. Citrix Administratoren können die Abonnementdaten zwischen verschiedenen Servergruppen in denselben oder verschiedenen Datencentern synchronisieren. Für Redundanz- und Failoverzwecke und eine hohe Leistung stellt jede Servergruppe im Datencenter eine Verbindung zu einer dedizierten Microsoft SQL Server-Instanz her. Das Szenario erfordert eine erhebliche zusätzliche Microsoft SQL Server-Konfiguration und -Infrastruktur. Sie nutzt für die Replikation von Abonnementdaten und für SQL-Transaktionen ausschließlich Microsoft SQL-Technologie.



Ressourcen

Sie können die folgenden hilfreichen Skripts von https://github.com/citrix/sample-scripts/tree/master/storefront herunterladen:

Konfigurationsskripts

- **Set-STFDatabase.ps1** – Legt die MS SQL-Verbindungszeichenfolge für jeden Store fest. Führen Sie das Skript auf dem StoreFront-Server aus.
- **Add-LocalAppPoolAccounts.ps1** – Gewährt den App-Pools des lokalen StoreFront-Servers Lese- und Schreibzugriff auf die SQL-Datenbank. Führen Sie das Skript für Szenario 2 auf dem SQL-Server aus.
- **Add-RemoteSFAccounts.ps1** – Gewährt allen StoreFront-Servern in einer Servergruppe Lese- und Schreibzugriff auf die SQL-Datenbank. Führen Sie das Skript für Szenario 3 auf dem SQL-Server aus.
- **Create-StoreSubscriptionsDB-2016.sql** – Erstellt die SQL-Datenbank und das Schema. Führen Sie das Skript auf dem SQL-Server aus.

Skripts für Datentransformation und Import

- **Transform-SubscriptionDataForStore.ps1** – Exportiert Abonnementdaten aus ESENT und wandelt sie in ein SQL-freundliches Format für den Import um.
- **Create-ImportSubscriptionDatasp.sql** – Erstellt eine gespeicherte Prozedur zum Importieren der von Transform-SubscriptionDataForStore.ps1 umgewandelten Daten. Führen Sie das Skript einmal auf dem SQL-Server aus, nachdem Sie das Datenbankschema mit Create-StoreSubscriptionsDB-2016.sql erstellt haben.

Konfigurieren der lokalen Sicherheitsgruppe des StoreFront-Servers auf dem SQL-Server

Szenario 2: Einzelner StoreFront-Server und lokal installierte Microsoft SQL Server-Instanz

Erstellen Sie eine lokale Sicherheitsgruppe unter dem Namen `<SQLServer>\StoreFrontServers` auf dem Microsoft SQL-Server und fügen Sie die virtuellen Konten für `IIS APPPOOL\DefaultAppPool` und `IIS APPPOOL\Citrix Receiver for Web` hinzu, damit das lokal installierte StoreFront Lese- und Schreibvorgänge an SQL ausführen kann. Auf diese Sicherheitsgruppe wird in dem SQL-Skript verwiesen, das das Schema für die Store-Abonnementdatenbank erstellt. Stellen Sie daher sicher, dass die Gruppennamen übereinstimmen.

Sie können hierfür das Skript Add-LocalAppPoolAccounts.ps1 herunterladen.

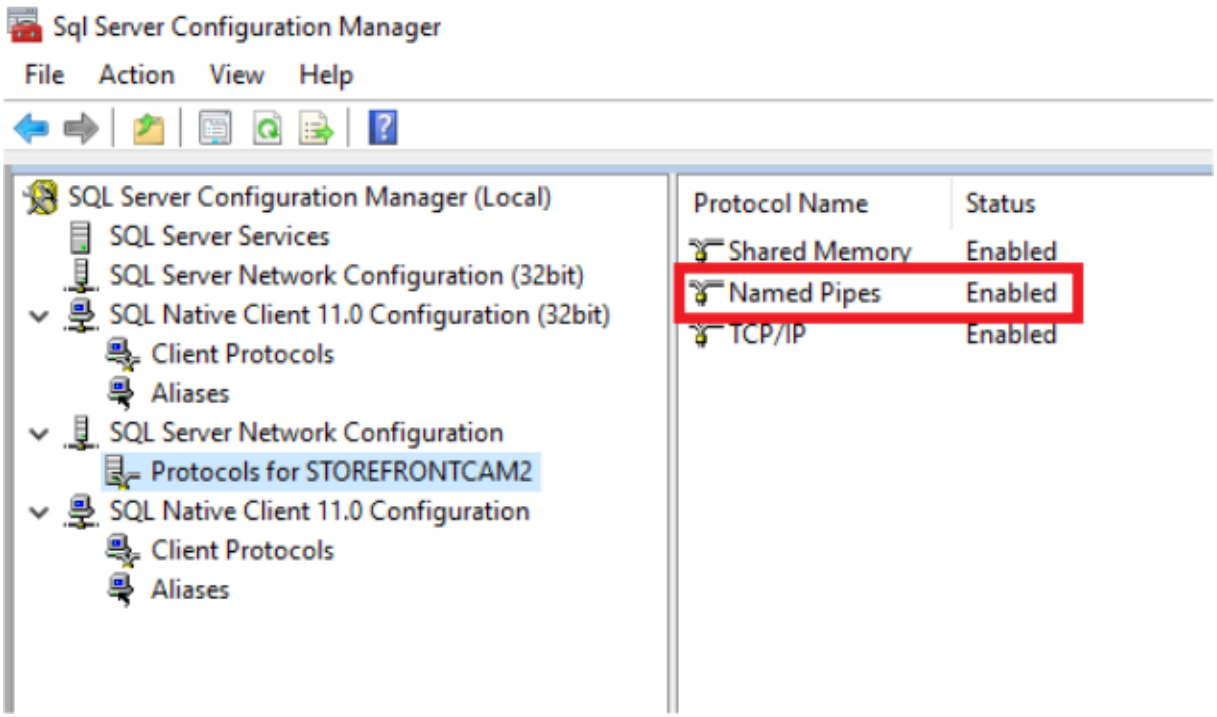
Installieren Sie StoreFront, bevor Sie das Skript *Add-LocalAppPoolAccounts.ps1* ausführen. Das Skript erfordert, dass das virtuelle IIS-Konto von `IIS APPPOOL\Citrix Receiver for Web` gefunden werden kann, welches erst nach der Installation und Konfiguration von StoreFront vorhanden ist. `IIS APPPOOL\DefaultAppPool` wird automatisch durch die Installation der IIS-Webserverrolle erstellt.

```
1  # Create Local Group for StoreFront servers on DB Server
2  $LocalGroupName = "StoreFrontServers"
3  $Description = "Contains StoreFront Server Machine Accounts or
       StoreFront AppPool Virtual Accounts"
4
5  # Check whether the Local Group Exists
6  if ([ADSI]::Exists("WinNT://$env:ComputerName/$LocalGroupName"))
7  {
8
9      Write-Host "$LocalGroupName already exists!" -ForegroundColor "
           Yellow"
10  }
11
12 else
13 {
14
```



```
15 Write-Host ”Creating $LocalGroupName local security group” -
       ForegroundColor ”Yellow”
16
17 # Create Local User Group
18 $Computer = [ADSI]”WinNT://$env:ComputerName,Computer”
19 $LocalGroup = $Computer.Create(”group”,$LocalGroupName)
20 $LocalGroup.setinfo()
21 $LocalGroup.description = $Description
22 $Localgroup.SetInfo()
23 Write-Host ”$LocalGroupName local security group created” -
       ForegroundColor ”Green”
24  }
25
26 $Group = [ADSI]”WinNT://$env:ComputerName/$LocalGroupName,group”
27
28 # Add IIS APPPOOL\DefaultAppPool
29 $objAccount = New-Object System.Security.Principal.NTAccount(”IIS
       APPPOOL\DefaultAppPool”)
30 $StrSID = $objAccount.Translate([System.Security.Principal.
       SecurityIdentifier])
31 $DefaultSID = $StrSID.Value
32
33 $Account = [ADSI]”WinNT://$DefaultSID”
34 $Group.Add($Account.Path)
35
36 # Add IIS APPPOOL\Citrix Receiver for Web
37 $objAccount = New-Object System.Security.Principal.NTAccount(”IIS
       APPPOOL\Citrix Receiver for Web”)
38 $StrSID = $objAccount.Translate([System.Security.Principal.
       SecurityIdentifier])
39 $WebRSID = $StrSID.Value
40
41 $Account = [ADSI]”WinNT://$WebRSID”
42 $Group.Add($Account.Path)
43
44 Write-Host ”AppPools added to $LocalGroupName local group” -
       ForegroundColor ”Green”
```

Aktivieren Sie mithilfe von SQL Server-Konfigurations-Manager Named Pipes in Ihrer lokalen SQL-Instanz. Named Pipes sind für die Kommunikation zwischen StoreFront- und SQL Server-Prozessen erforderlich.

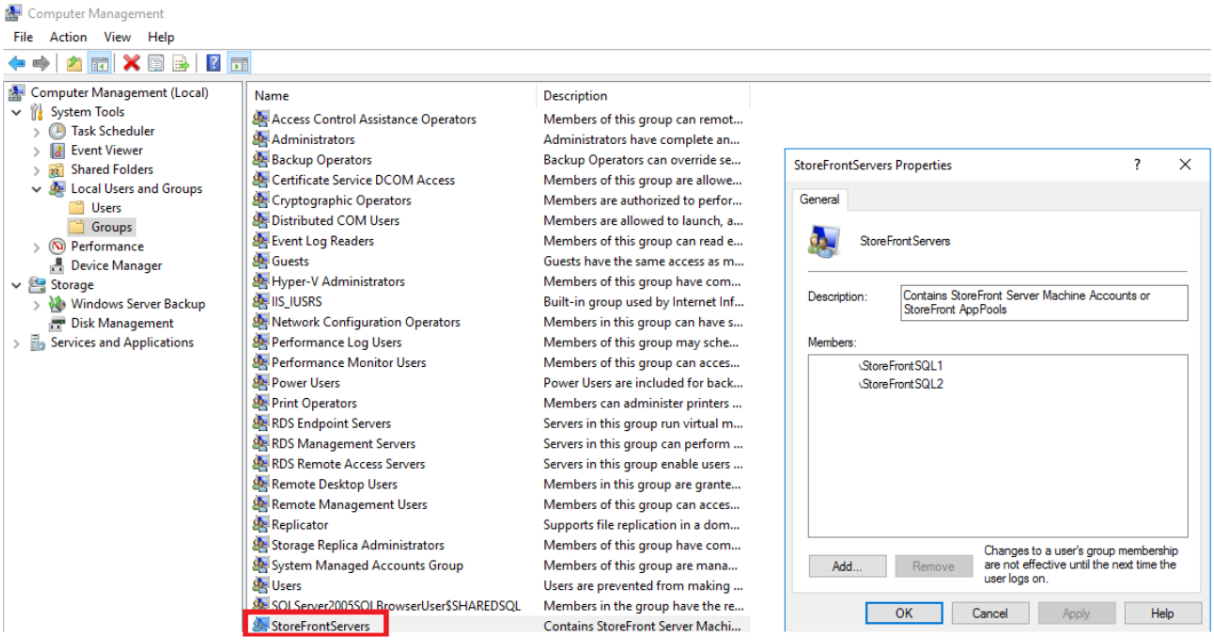


Stellen Sie sicher, dass die Windows-Firewallregeln korrekt konfiguriert sind, sodass SQL Server-Verbindungen über einen bestimmten Port oder dynamische Ports zugelassen sind. Spezifische Informationen hierzu für Ihre Umgebung finden Sie in der Microsoft-Dokumentation.

> **Tipp:**
>
> Wenn die Verbindung zur lokalen SQL-Instanz fehlschlägt, überprüfen Sie, ob localhost bzw. die Angabe <hostname> in der Verbindungszeichenfolge in die richtige IPv4-Adresse aufgelöst wird. Windows versucht möglicherweise, IPv6 anstelle von IPv4 zu verwenden, und die DNS-Auflösung von localhost kann ::1 anstelle der richtigen IPv4-Adresse des StoreFront- und SQL-Servers zurückgeben. Möglicherweise ist das vollständige Deaktivieren des IPv6-Netzwerkstapels auf dem Hostserver erforderlich, um dieses Problem zu beheben.

Szenario 3: StoreFront-Servergruppe und eine dedizierte Microsoft SQL Server-Instanz

Erstellen Sie eine lokale Sicherheitsgruppe unter dem Namen <SQLServer>\StoreFrontServers auf dem Microsoft SQL-Server und fügen Sie alle Mitglieder der StoreFront-Servergruppe hinzu. Auf diese Sicherheitsgruppe wird später im Skript **Create-StoreSubscriptionsDB-2016.SQL** verwiesen, das das Schema der Abonnementdatenbank in SQL erstellt.



Fügen Sie der Gruppe alle Domänencomputerkonten der StoreFront-Servergruppe `<SQLServer>\StoreFrontServers` hinzu. Nur in der Gruppe aufgelistete StoreFront-Server-Domänenkonten können Abonnementdatensätze in SQL lesen und schreiben, wenn die Windows-Authentifizierung von SQL Server verwendet wird. Die folgende PowerShell-Funktion in Skript Add-RemoteSFAccounts.ps1 erstellt die lokale Sicherheitsgruppe und fügt ihr zwei StoreFront-Server mit dem Namen “StoreFrontSQL1” und “StoreFrontSQL2” hinzu.

```
function Add-RemoteSTFMachineAccounts
{

[CmdletBinding()]
param([Parameter(Mandatory=$True)][string]$Domain,
[Parameter(Mandatory=$True)][array]$StoreFrontServers)

# Create Local Group for StoreFront servers on DB Server
$LocalGroupName = ”StoreFrontServers”
$Description = ”Contains StoreFront Server Machine Accounts or
    StoreFront AppPool virtual accounts”

# Check whether the Local Security Group already exists
if ([ADSI]::Exists(”WinNT://$env:ComputerName/$LocalGroupName”))
{

    Write-Host ”$LocalGroupName already exists!” -ForegroundColor ”
        Yellow”
 }

```



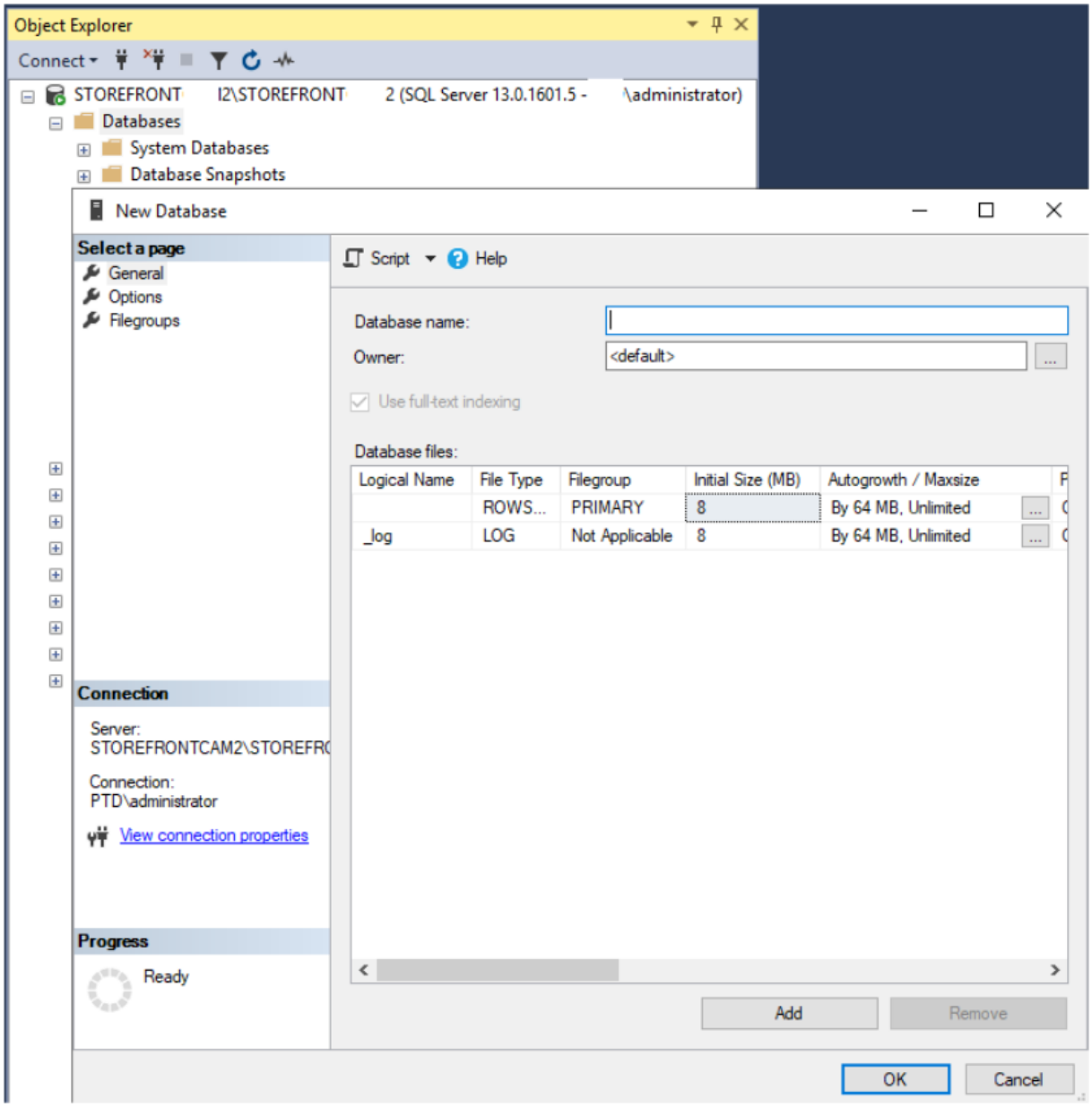
```
19 else
20 {
21
22     Write-Host ”Creating $LocalGroupName local group” -ForegroundColor
       ”Yellow”
23
24     # Create Local Security Group
25     $Computer = [ADSI]”WinNT://$env:ComputerName,Computer”
26     $LocalGroup = $Computer.Create(”group”,$LocalGroupName)
27     $LocalGroup.setinfo()
28     $LocalGroup.description = $Description
29     $Localgroup.SetInfo()
30 Write-Host ”$LocalGroupName local group created” -ForegroundColor ”
       Green”
31  }
32
33 Write-Host ”Adding $StoreFrontServers to $LocalGroupName local group” -
       ForegroundColor ”Yellow”
34
35 foreach ($StoreFrontServer in $StoreFrontServers)
36 {
37
38     $Group = [ADSI]”WinNT://$env:ComputerName/$LocalGroupName,group”
39     $Computer = [ADSI]”WinNT://$Domain/$StoreFrontServer$”
40     $Group.Add($Computer.Path)
41  }
42
43 Write-Host ”$StoreFrontServers added to $LocalGroupName” -
       ForegroundColor ”Green”
44  }
45
46 Add-RemoteSTFMachineAccounts -Domain ”example” -StoreFrontServers @(”
       StoreFrontSQL1”,”StoreFrontSQL2”)
```

Konfigurieren des Abonnementdatenbankschemas in Microsoft SQL Server für jeden Store

Erstellen Sie eine benannte Instanz auf Ihrem Microsoft SQL-Server zur Verwendung durch StoreFront. Legen Sie den Pfad innerhalb des .SQL-Skripts auf den Installationsort der SQL-Version oder den Speicherort der Datenbankdateien fest. Das Beispielskript Create-StoreSubscriptionsDB-2016.sqlverwendet SQL Server 2016 Enterprise.

Erstellen Sie mit SQL Server Management Studio (SSMS) eine leere Datenbank, indem Sie mit der

rechten Maustaste auf **Datenbanken** klicken und **Neue Datenbank** auswählen.



Geben Sie einen **Datenbanknamen** ein, der Ihrem Store entspricht, oder wählen Sie einen anderen Namen, etwa *STFSubscriptions*.

Ändern Sie vor dem Ausführen des Skripts für jeden Store in Ihrer StoreFront Bereitstellung die Verweise im Beispielskript so, dass sie Ihren StoreFront- und SQL-Bereitstellungen entsprechen. Beispiel:

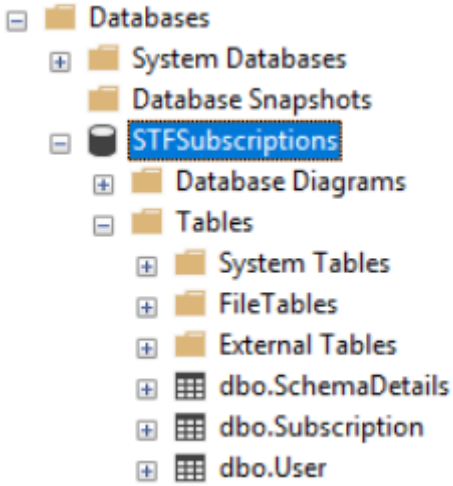
- Benennen Sie jede von Ihnen erstellte Datenbank so, dass sie mit dem Storenamen in StoreFront unter `USE [STFSubscriptions]` übereinstimmt.
- Legen Sie den Pfad der MDF- und LDF-Datenbankdateien auf den Pfad fest, an dem die Datenbank gespeichert werden soll.


```
C:\Program Files\Microsoft SQL Server\MSSQL13.SQL2016\MSSQL\DATA\
STFSubscriptions.mdf

C:\Program Files\Microsoft SQL Server\MSSQL13.SQL2016\MSSQL\DATA\
STFSubscriptions.ldf
```

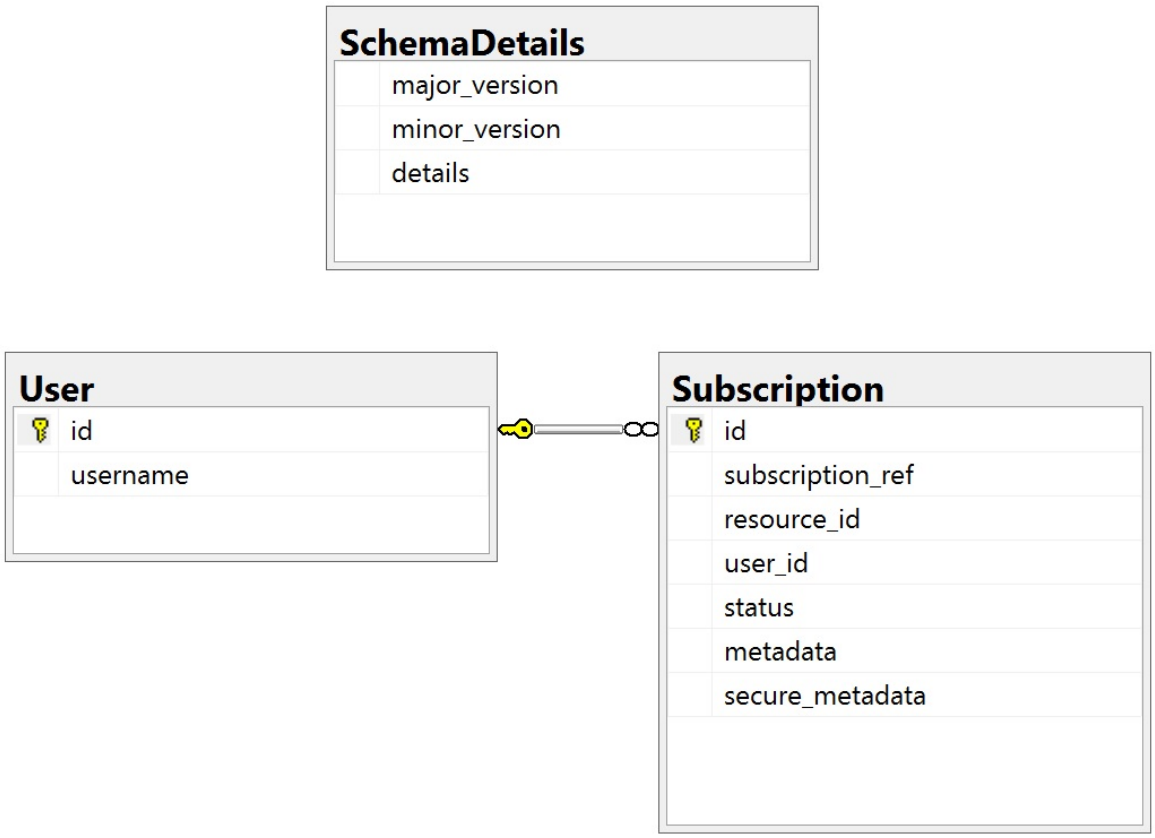
- Legen Sie den Verweis auf den Namen Ihres SQL-Servers innerhalb des Skripts fest:

```
CREATE LOGIN [SQL2016\StoreFrontServers] FROM WINDOWS;

ALTER LOGIN [SQL2016\StoreFrontServers]
```

Führen Sie das Skript aus. Nach erfolgreicher Konfiguration des Schemas werden drei Datenbanktabellen erstellt: *SchemaDetails*, *Subscription* und *User*.



Die folgende Abbildung zeigt das Schema der mit dem Skript *Create-StoreSubscriptionsDB-2016.SQL* erstellten Abonnementdatenbank:



Konfigurieren der SQL Server-Verbindungszeichenfolge für jeden StoreFront-Store

Szenario 1

> **Tipp:**
>
> Die auf der Festplatte gespeicherten ursprünglichen Abonnementdaten der ESENT-Datenbank werden nicht gelöscht. Wenn Sie von Microsoft SQL Server wieder auf ESENT umsteigen möchten, können Sie die Store-Verbindungszeichenfolge entfernen und einfach wieder die ursprünglichen Daten verwenden. Abonnements, die während der Verwendung von SQL für den Store erstellt wurden, sind in ESENT nicht vorhanden und die Benutzer sehen diese neuen Abonnementdatensätze nicht. Alle ursprünglichen Abonnementdatensätze sind weiterhin vorhanden.

Erneutes Aktivieren von ESENT-Abonnements in einem Store

Öffnen Sie PowerShell ISE, und wählen Sie **Als Administrator ausführen**.

Verwenden Sie die Option **-UseLocalStorage**, um den Store anzugeben, für den Sie ESENT-Abonnements erneut aktivieren möchten:


```
$SiteID = 1
$StoreVirtualPath = ”/Citrix/Store1”

# Sets SQL DB Connection String
$StoreObject = Get-STFStoreService -SiteID $SiteID -VirtualPath
    $StoreVirtualPath

# Removes the SQL DB Connection string and reverts back to using ESENT
Set-STFStoreSubscriptionsDatabase -StoreService $StoreObject -
    UseLocalStorage
Get-STFStoreSubscriptionsDatabase -StoreService $StoreObject
```

Szenarios 2, 3 und 4

Öffnen Sie PowerShell ISE, und wählen Sie **Als Administrator ausführen**.

Geben Sie mit **$storeVirtualPath** den Store an, für den Sie eine Verbindungszeichenfolge festlegen möchten.

```
$SiteID = 1
$VirtualPath= ”/Citrix/Store1”
$DBName = ”Store1”
$DBServer = ”SQL2016Ent”
$DBLocalServer = ”localhost”
$DBInstance = ”StoreFrontInstance”

# For a remote database instance
$ConnectionString = ”Server=$DBServer$SQLInstance;Database=$DBName;
    Trusted_Connection=True;” Database=$DBName;Trusted_Connection=True;”
```

ODER

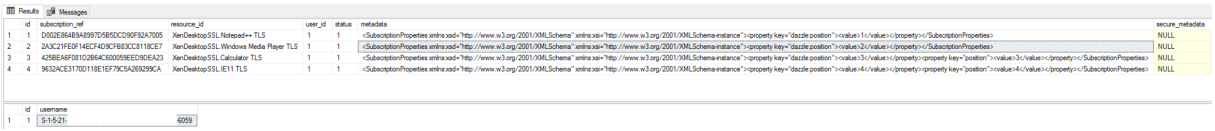
```
# For a locally installed database instance
$ConnectionString = ”$DBLocalServer$SQLInstance;Database=$DBName;
    Trusted_Connection=True;”

# Sets SQL DB Connection String
$StoreObject = Get-STFStoreService -SiteID $SiteID -VirtualPath ”/
    Citrix/Store”
Set-STFStoreSubscriptionsDatabase -StoreService $StoreObject -
    ConnectionString $ConnectionString
Get-STFStoreSubscriptionsDatabase -StoreService $StoreObject
```


Wiederholen Sie den Vorgang für jeden Store in der Bereitstellung, wenn Sie alle Stores für die Verwendung einer SQL-Verbindungszeichenfolge konfigurieren möchten.

Migrieren von Daten von ESENT nach Microsoft SQL Server

Zur Migration vorhandener ESENT-Daten nach SQL ist ein zweistufiger Datentransformationsprozess erforderlich. Zwei Skripts stehen zur Verfügung, die bei der Ausführung dieser einmaligen Operation helfen. Wenn die Verbindungszeichenfolge in StoreFront und der SQL-Instanz korrekt konfiguriert ist, werden alle neuen Abonnements automatisch in SQL im richtigen Format erstellt. Nach der Migration werden die ESENT-Abonnementdaten in ein SQL-Format umgewandelt und die Benutzer sehen auch ihre zuvor abonnierten Ressourcen.

Beispiel: vier SQL-Abonnements für einen Domänenbenutzer



Schritt 1: Konvertieren der ESENT-Daten in ein SQL-Format für den Massenimport mit Transform-SubscriptionDataForStore.ps1

Melden Sie sich bei dem StoreFront-Server an, dessen ESENT-Daten Sie umwandeln möchten.

Jedes Mitglied einer Servergruppe ist geeignet, sofern alle die gleiche Anzahl Abonnementdatensätze enthalten.

Öffnen Sie PowerShell ISE, und wählen Sie **Als Administrator ausführen**.

Führen Sie das Skript Transform-SubscriptionDataForStore.ps1 aus, das eine `<StoreName>.txt`-Datei aus der ESENT-Datenbank auf den Desktop des aktuellen Benutzers exportiert.

Das PowerShell-Skript bietet ausführliches Feedback zu jeder verarbeiteten Abonnementzeile, um das Debuggen und die Prüfung des Erfolgs des Vorgangs zu unterstützen. Die Verarbeitung kann lange dauern.

Die umgewandelten Daten werden nach Abschluss des Skripts in die Datei `<StoreName>SQL.txt` auf dem Desktop des aktuellen Benutzers geschrieben. Das Skript fasst die Anzahl der eindeutigen Benutzerdatensätze und die Gesamtzahl der verarbeiteten Abonnements zusammen.

Wiederholen Sie diesen Vorgang für jeden Store, den Sie nach SQL Server migrieren möchten.

Schritt 2: Massenimport der umgewandelten Daten mit einer gespeicherten T-SQL-Prozedur

Die Daten müssen für jeden Stores gesondert importiert werden.

Kopieren Sie die in Schritt 1 erstellte Datei `<StoreName>SQL.txt` vom Desktop des StoreFront-Servers`C:\` auf den Computer mit Microsoft SQL Server und benennen Sie sie in SubscriptionsSQL.txt um.

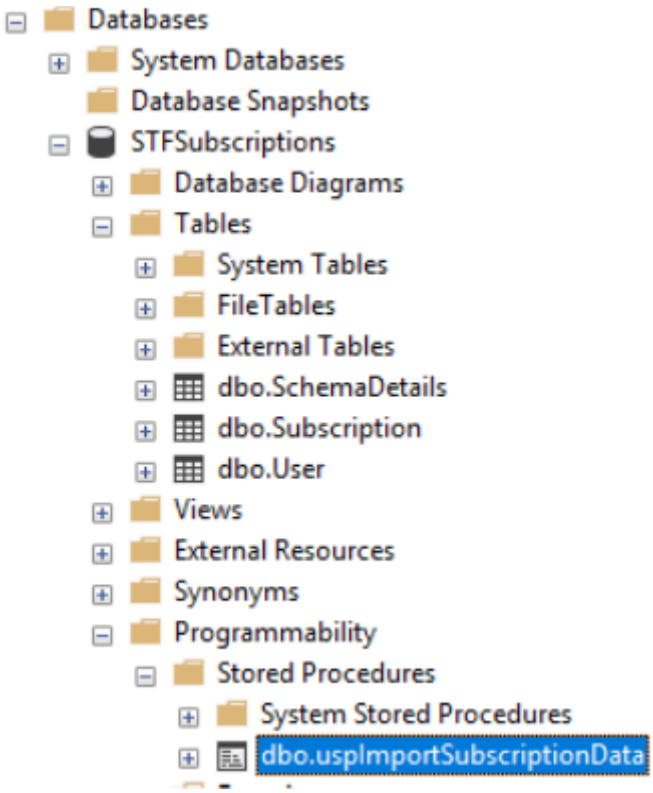
Das Skript Create-ImportSubscriptionDataSP.sql erstellt eine gespeicherte T-SQL-Prozedur zum Massenimport der Abonnementdaten. Es entfernt doppelte Einträge für eindeutige Benutzer, sodass die resultierenden SQL-Daten korrekt normalisiert und in die richtigen Tabellen aufgeteilt werden.

Bevor Sie *Create-ImportSubscriptionDatasp.sql* ausführen, ändern Sie `USE [STFSubscriptions]` auf die Datenbank, in der Sie die gespeicherte Prozedur erstellen möchten.

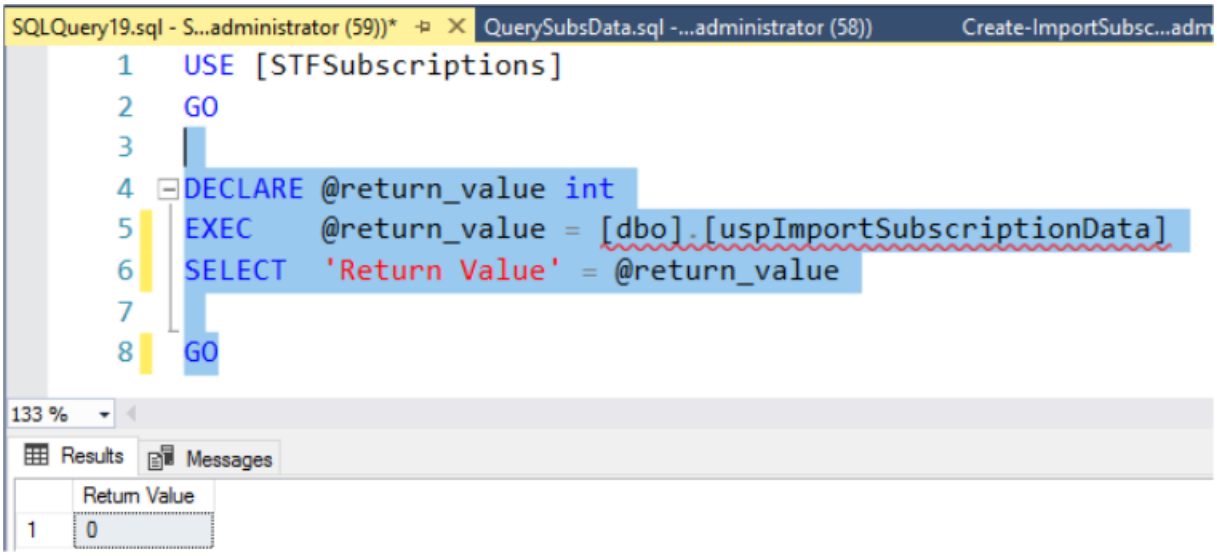
Öffnen Sie die Datei *Create-ImportSubscriptionDatasp.sql* mit SQL Server Management Studio und führen Sie den enthaltenen Code aus. Das Skript fügt der zuvor erstellten Datenbank die gespeicherte Prozedur *ImportSubscriptionDatasp* hinzu.

Nach Erstellung der gespeicherten Prozedur wird in der SQL-Konsole die folgende Meldung angezeigt und die gespeicherte Prozedur ImportSubscriptionDatasp wird der Datenbank hinzugefügt:

```
Commands completed successfully.
```



Führen Sie die gespeicherte Prozedur aus, indem Sie mit der rechten Maustaste darauf klicken, **Gespeicherte Prozedur ausführen** wählen und auf **OK** klicken.



Der Rückgabewert 0 zeigt an, dass alle Daten erfolgreich importiert wurden. Jegliche Probleme beim Import werden in der SQL-Konsole protokolliert. Nach dem erfolgreichen Ausführen der gespeicherten Prozedur vergleichen Sie die von Transform-SubscriptionDataForStore.ps1 zurückgegebene Gesamtzahl der Abonnementdatensätze und eindeutigen Benutzer mit dem Ergebnis der beiden SQL-Abfragen unten. Die beiden Summen müssen übereinstimmen.

Die Gesamtanzahl der Abonnements aus dem Transformationsskript muss mit der Gesamtzahl übereinstimmen, die von folgender SQL-Abfrage zurückgegeben wird:

```
SELECT COUNT(*) AS TotalSubscriptions
FROM [Subscription]
```

Die Anzahl der eindeutigen Benutzer aus dem Transformationsskript muss mit der Anzahl übereinstimmen, die von folgender SQL-Abfrage aus der Tabelle “User” zurückgegeben wird:

```
SELECT COUNT(*) AS TotalUsers
FROM [User]
```

Wenn das Transformationsskript 100 eindeutige Benutzer und 1000 Abonnementdatensätze insgesamt anzeigt, muss SQL nach erfolgreicher Migration dieselben Zahlen anzeigen.

Melden Sie sich bei StoreFront an, um zu überprüfen, ob bestehende Benutzer ihre Abonnementdaten sehen können. Bestehende Abonnementdatensätze werden in SQL aktualisiert, wenn Benutzer Ressourcen abonnieren oder abbestellen. Neue Benutzer- und Abonnementdatensätze werden ebenfalls in SQL erstellt.

Schritt 3: Ausführen der T-SQL-Abfragen an importierten Daten

> **Hinweis:**
>
> Bei allen Delivery Controller-Namen wird zwischen Groß- und Kleinschreibung unterschieden. Die Schreibung muss mit der in StoreFront verwendeten Groß- und Kleinschreibung übereinstimmen.

```
-- Get all SQL subscription records
Use [STFSubscriptions]
SELECT * FROM [Subscription]
SELECT * FROM [User]
```

```
-- Get all subscription records for a particular user SID
Use [STFSubscriptions]
SELECT * FROM [Subscription]
INNER JOIN [User]
ON [Subscription].[user_id] = [User].[id]
WHERE [User].[username] = 'S-1-5-21-xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxxx-
    xxxx'

-- Get total number of Subscription records for a particular user SID
Use [STFSubscriptions]
SELECT COUNT(Subscription.id)
FROM [Subscription]
INNER JOIN [User]
ON [Subscription].[user_id] = [User].[id]
WHERE [User].[username] = 'S-1-5-21-xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxxx-
    xxxx'
```

```
-- Get all subscription records for a particular delivery controller
Use [STFSubscriptions]
SELECT * FROM [Subscription]
WHERE [resource_id] LIKE 'DeliveryController.%'

-- OR for aggregated resources use the name of the aggregation group
Use [STFSubscriptions]
SELECT * FROM [Subscription]
WHERE [resource_id] LIKE 'DefaultAggregationGroup.%'

-- Get all subscription records for a particular application
Use [STFSubscriptions]
SELECT * FROM [Subscription]
WHERE [resource_id] = ' DeliveryController.Application'
```


Aktualisieren oder Löschen von Abonnementdatensätzen mit T-SQL

> **Haftungsausschluss:**
>
> Sie verwenden alle SQL-Anweisungen zum Aktualisieren und Löschen ausschließlich auf eigenes Risiko. Citrix ist nicht haftbar bei einem Verlust oder einer versehentlichen Änderung Ihrer Abonnementdaten durch die falsche Anwendung der angegebenen Beispiele. Die folgenden T-SQL-Anweisungen sollen als Leitfaden für einfache Aktualisierungen dienen. Führen Sie für alle Abonnementdaten in der SQL-Datenbank ein vollständiges Backup aus, bevor Sie versuchen, Abonnements zu aktualisieren oder veraltete Datensätze zu entfernen. Wenn Sie diese erforderlichen Backups nicht ausführen, kann dies zu Datenverlust oder -beschädigung führen. Bevor Sie eigene T-SQL-UPDATE- oder DELETE-Anweisungen an der Produktionsdatenbank ausführen, testen Sie diese an Testdaten oder einer redundanten Kopie der Produktionsdaten außerhalb der Live-Produktionsdatenbank.
>
> **Hinweis:**
>
> Bei allen Delivery Controller-Namen wird zwischen Groß- und Kleinschreibung unterschieden. Die Schreibung muss mit der in StoreFront verwendeten Groß- und Kleinschreibung übereinstimmen.

```
-- Update the delivery controller used in all subscriptions.
Use [STFSubscriptions]
UPDATE [Subscription]
SET [resource_id] = REPLACE(resource_id,'OldDeliveryController.','
   NewDeliveryController.')
WHERE [resource_id] LIKE 'OldDeliveryController.%'

-- OR for aggregated resources use the name of the aggregation group
Use [STFSubscriptions]
UPDATE [Subscription]
SET [resource_id] = REPLACE(resource_id,'OldDeliveryController.','
   DefaultAggregationGroup.')
WHERE [resource_id] LIKE 'OldDeliveryController.%'
```

```
-- Delete all subscription records for a particular Delivery Controller
Use [STFSubscriptions]
DELETE FROM [Subscription]
WHERE [resource_id] LIKE 'DeliveryController.%'

-- OR for aggregated resources use the name of the aggregation group
Use [STFSubscriptions]
DELETE FROM [Subscription]
FROM [Subscription]
WHERE [resource_id] LIKE 'DefaultAggregationGroup.%'
```

```
11
12 -- Delete all subscription records for a particular application
13 Use [STFSubscriptions]
14 DELETE FROM [Subscription]
15 FROM [Subscription]
16 WHERE [resource_id] LIKE '%.Application'
17
18 -- Delete all subscription records for an application published via a
       specific delivery controller
19 Use [STFSubscriptions]
20 DELETE FROM [Subscription]
21 FROM [Subscription]
22 WHERE [resource_id] = 'DeliveryController.Application'
```

```
1  -- Delete all subscription records for a particular user SID
2  Use [STFSubscriptions]
3  DELETE FROM [Subscription]
4  INNER JOIN [User]
5  ON [Subscription].[user_id] = [User].[id]
6  WHERE [User].[username] = 'S-1-5-21-xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxxx-
       xxxx'
7
8  Use [STFSubscriptions]
9  DELETE FROM [User]
10 WHERE [User].[username] = 'S-1-5-21-xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxxx-
       xxxx'
```

```
1  -- Delete ALL subscription data from a particular database and reset
       the primary key clustered index to start numbering from 0.
2  -- USE WITH EXTREME CARE AND NOT ON LIVE PRODUCTION DATABASES.
3  -- Can be useful whilst debugging data import issues to start with a
       clean database.
4
5  Use [STFSubscriptions]
6  DELETE FROM [Subscription]
7  DBCC CHECKIDENT ([Subscription], RESEED, 0)
8  DELETE FROM [User]
9  DBCC CHECKIDENT ([User], RESEED, 0)
```

Erweiterte Storeeinstellungen

April 1, 2020

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

> **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. Navigieren Sie auf der Windows-Startseite oder auf der Apps-Seite zur 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**.

Adressauflösungstyp

Auf der Seite **Erweiterte Einstellungen** geben Sie den Adresstyp an, der vom Server angefordert werden soll. Der Standardwert ist “DnsPort”. Wählen Sie im Dropdownmenü **Adressauflösungstyp** unter **Erweiterte Einstellungen** eine der folgenden Optionen:

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

Schriftartenglättung zulassen

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

Wählen Sie über die Aufgabe **Erweiterte Einstellungen** die Option **Schriftglättung zulassen** und klicken Sie auf **OK**.

Sitzungswiederverbindung zulassen

Sie können festlegen, ob HDX-Sitzungen wieder verbunden werden sollen. Die Standardeinstellung ist “Ein”.

Wählen Sie in der Aufgabe **Erweiterte Einstellungen** die Option **Sitzungswiederverbindung zulassen** und klicken Sie auf **OK**, um die Sitzungswiederverbindung zu aktivieren.

Umleitung spezieller Ordner zulassen

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 **Erweiterte Einstellungen** die Option **Umleitung spezieller Ordner zulassen** und klicken Sie auf **OK**.

Intervall für Hintergrundsystemdiagnose

StoreFront führt regelmäßig Systemdiagnosen an jedem Citrix Virtual Desktops-Broker und Citrix Virtual Apps-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.

Kommunikationstimeoutdauer

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 1 Kommunikationsversuch gescheitert ist. Wählen Sie die Aufgabe **Erweiterte Einstellungen**, ändern Sie die Standardzeit nach Bedarf und klicken Sie auf **OK**.

Verbindungstimeout

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

Geben Sie mit der Aufgabe **Erweiterte Einstellungen** die Sekunden ein, die beim Herstellen der ersten Verbindung gewartet werden soll, und klicken Sie auf **OK**.

Erweiterte Enumeration aktivieren

Diese Option steuert, ob StoreFront die Delivery Controller gleichzeitig oder sequentiell abfragt, wenn Apps und Desktops über mehrere Citrix Virtual Apps and Desktops-Sites hinweg enumeriert werden. Die gleichzeitige Enumerierung bietet schnellere Antworten auf Benutzerabfragen, wenn Ressourcen über mehrere Sites hinweg aggregiert werden. Wenn diese Option ausgewählt ist (Standardeinstellung), sendet StoreFront gleichzeitig Enumerierungsanforderungen an alle Delivery Controller und aggregiert Antworten, wenn sie alle geantwortet haben. Sie können die Optionen **Maximum gleichzeitiger Enumerationen** und **Minimum Farmen für gleichzeitige Enumeration** verwenden, um dieses Verhalten zu optimieren.

Aktivieren oder Deaktivieren Sie in der Aufgabe **Erweiterte Einstellungen** die Option **Erweiterte Enumeration aktivieren** und klicken Sie auf **OK**.

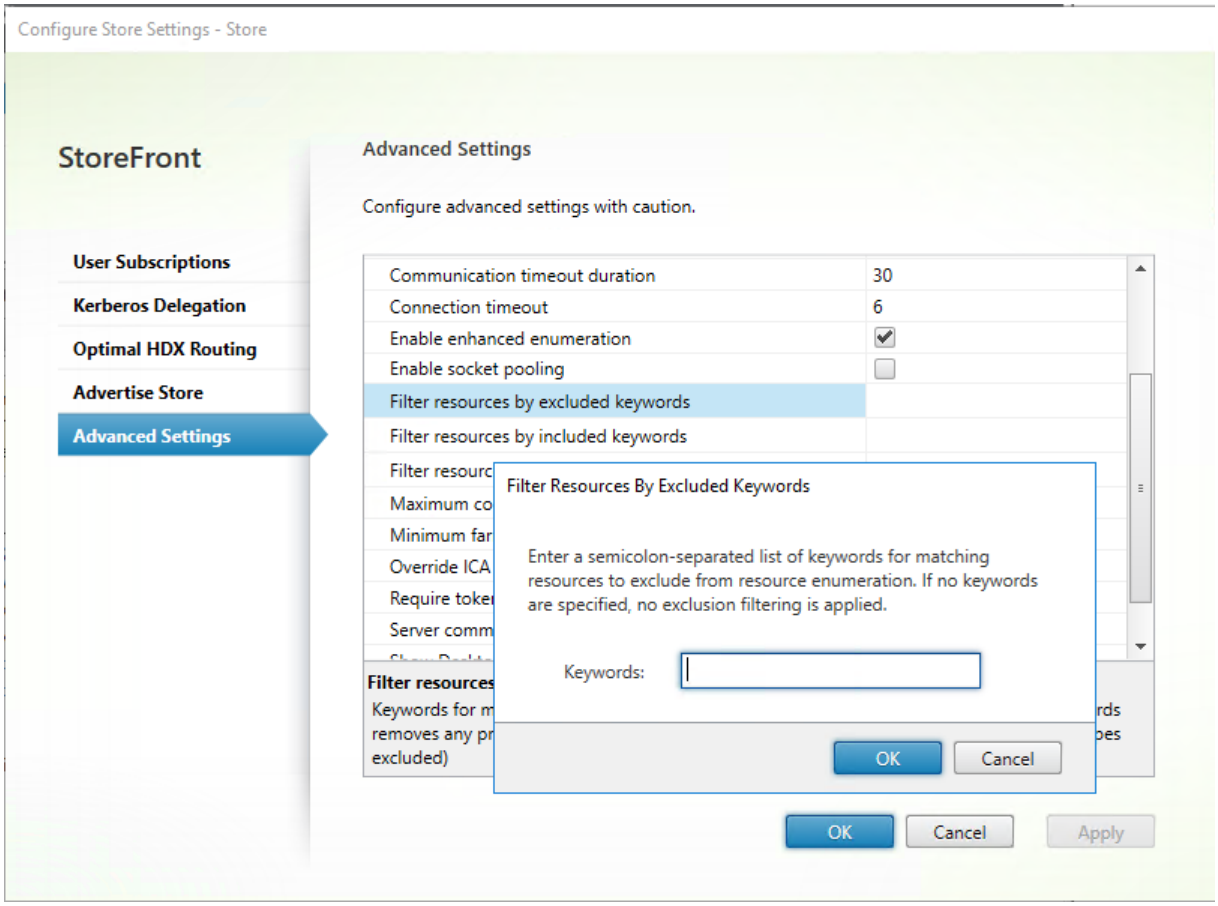
Socketpooling aktivieren

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** die Option **Socketpooling aktivieren** und klicken Sie auf **OK**.

Ressourcen nach Ausschlussschlüsselwörtern filtern

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**.



Ressourcen nach Einschlussschlüsselwörtern filtern

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**.

Ressourcen nach Typ filtern

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**.

Maximum gleichzeitiger Enumerationen

Legen Sie fest, wie viele Anforderungen gleichzeitig an alle Delivery Controller gesendet werden sollen. Diese Option wird wirksam, wenn die Option **Erweiterte Enumeration aktivieren** aktiviert ist. 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**.

Minimum Farmen für gleichzeitige Enumeration

Geben Sie die Mindestanzahl von Delivery Controllern an, die erforderlich sind, um die gleichzeitige Enumeration auszulösen. Diese Option wird wirksam, wenn die Option **Erweiterte Enumeration aktivieren** aktiviert ist. Die Standardeinstellung ist 3.

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

ICA-Clientnamen überschreiben

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 der Citrix Workspace-App festgelegt. Die Standardeinstellung ist “Aus”.

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

Tokenkonsistenz erforderlich

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** die Option **Tokenkonsistenz erforderlich** und klicken Sie auf **OK**.

Serverkommunikationsversuche

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

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

Desktop Viewer für Legacyclients anzeigen

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

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

Verwalten einer Citrix Receiver für Web-Site

January 6, 2020

Eine *Citrix Receiver für Web*-Site ist eine Website, die als App-Store verwendet wird. Die Benutzer können die Site in einem Browser öffnen und sicher auf Anwendungen, Daten und Desktops zugreifen, die für sie über Citrix Virtual Apps and Desktops veröffentlicht wurden.

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

Aufgabe	Detail
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.
Einheitliche Benutzeroberfläche	StoreFront unterstützt 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.

Aufgabe	Detail
Konfigurieren der Verwendung der Browserregisterkarten für die Citrix Workspace-App für HTML5	Zum Festlegen, ob der Desktop bzw. die Anwendung beim Start von Ressourcen über Verknüpfungen mit Citrix Receiver bzw. der Citrix Workspace-App 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 Citrix 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

January 30, 2020

Bei der Erstellung eines neuen Stores wird standardmäßig eine Citrix Receiver für Web-Site für den Store erstellt. Sie können vorhandenen Stores zusätzliche Citrix Receiver für Web-Sites hinzufügen.

> 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. Navigieren Sie auf der Windows-Startseite oder auf der Apps-Seite zur Kachel Citrix StoreFront.
2. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten “Store”, wählen Sie im Bereich “Aktionen” 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 den gewünschten **Websitepfad** ein, und klicken Sie auf **Weiter**.

4. Wählen Sie die Citrix Receiver-Benutzeroberfläche und klicken Sie auf **Weiter**.
5. Wählen Sie Authentifizierungsmethoden, 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 die Citrix Workspace-App auf dem Benutzergerät installiert ist, wenn ein Benutzer über einen Computer unter Windows oder Mac OS X auf Receiver für Web-Sites zugreift. Wenn die Citrix Workspace-App nicht erkannt wird, wird der Benutzer aufgefordert, die App von der Citrix Website herunterzuladen und zu installieren. Weitere Informationen zum Ändern dieses Verhaltens finden Sie unter Konfigurieren der Site-Funktionsweise für Benutzer ohne Citrix Workspace-App.

Die Standardkonfiguration für Receiver für Web-Sites erfordert, dass Benutzer eine kompatible Version der Citrix Workspace-App installieren, um auf ihre Desktops und Anwendungen zuzugreifen. Sie können jedoch die Citrix Workspace-App für HTML5 auf den Receiver für Web-Sites aktivieren, sodass Benutzer, die die Citrix Workspace-App 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

April 1, 2020

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 mit 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.

Authentifizierungsmethoden auswählen

Verwenden Sie die Aufgabe “Authentifizierungsmethoden verwalten”, 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. Navigieren Sie auf der Windows-Startseite oder auf der Apps-Seite zur 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 “Stores” auf **Receiver für Web-Sites verwalten**, klicken Sie auf **Konfigurieren** und wählen Sie **Authentifizierungsmethoden**, um die Zugriffsmethoden für die Benutzer festzulegen.
    - Aktivieren Sie **Benutzername und Kennwort**, um die explizite Authentifizierung zu aktivieren. Benutzer geben beim Zugriff auf ihre Stores ihre Anmeldeinformationen ein.
    - Wählen Sie **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 **Domänen-Passthrough**, um Passthrough für Active Directory-Domänenanmeldeinforma 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 bzw. die Citrix Workspace-App auf den Benutzergeräten installiert ist.

      > Hinweis:
      >
      > Domänenpassthrough für Citrix Receiver für Web ist auf Windows-Betriebssysteme mit Chrome, Firefox und Internet Explorer beschränkt.

    - Aktivieren Sie **Smartcard**, um die Smartcardauthentifizierung zu aktivieren. Benutzer authentifizieren sich mit Smartcards und PINs beim Zugriff auf ihre Stores.
    - Aktivieren Sie **Passthrough-Authentifizierung von Citrix Gateway** zum Aktivieren der Passthrough-Authentifizierung von Citrix Gateway. Die Benutzer authentifizieren sich bei Citrix Gateway und werden beim Zugriff auf ihre Stores automatisch angemeldet.

4. Nach dem Auswählen der Authentifizierungsmethode klicken Sie auf **OK**.

   Weitere Informationen zum Ändern der Einstellungen für Authentifizierungsmethoden finden Sie unter Konfigurieren des Authentifizierungsdiensts.

Hinzufügen von Ressourcenverknüpfungen mit anderen Websites

Verwenden Sie die Aufgabe **Websites Verknüpfungen hinzufügen**, um Benutzern schnellen Zugriff auf Desktops und Anwendungen über vertrauenswürdige Websites, die im internen Netzwerk gehostet werden, zu gestatten. Dafür generieren Sie URLs für Ressourcen, die über eine Citrix Receiver 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.

Bevor Sie Ressourcenverknüpfungen generieren können, müssen Sie die URLs von Hostwebsites mit der Citrix StoreFront-Verwaltungskonsole oder PowerShell der Liste “Vertrauenswürdige URLs” hinzufügen. Vertrauenswürdige URLs werden im Abschnitt `<trustedUrls>` der Datei web.config für die Citrix Receiver für Web-Site aufgeführt. Die Datei web.config ist normalerweise im Verzeichnis `C:\inetpub\wwwroot\Citrix\storenameWeb\`, wobei *storename* der Name ist, der beim Erstellen des Stores angegeben wurde.

Standardmäßig warnt StoreFront Benutzer, wenn sie versuchen, Ressourcenverknüpfungen von nicht vertrauenswürdigen Websites zu starten, Benutzer können die Ressource jedoch weiterhin starten. Um diese Warnungen zu stoppen, klicken Sie im Bereich “Stores” auf **Receiver für Web-Sites verwalten**, klicken Sie auf **Konfigurieren**, wählen Sie **Erweiterte Einstellungen**. Deaktivieren Sie die Option **Aufforderung für nicht vertrauenswürdige Verknüpfungen**.

Hinzufügen vertrauenswürdiger Websites über die Verwaltungskonsole

1. Navigieren Sie auf der Windows-Startseite oder auf der Apps-Seite zur 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.
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 ist, der für die Kommunikation mit dem Host 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 Citrix Receiver für Web-Site an und kopieren Sie die erforderlichen URLs in Ihre Website.

Hinzufügen vertrauenswürdiger Websites mit PowerShell

Sie können "vertrauenswürdige" URLs mit dem PowerShell Cmdlet **Set-STFWebReceiverApplicationShortcuts** hinzufügen, das unter https://developer-docs.citrix.com/projects/storefront-powershell-sdk/en/latest/Citrix.StoreFront.SubscriptionsStore/ beschrieben wird.

Festlegen des Sitzungstimeouts

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. Navigieren Sie auf der Windows-**Startseite** oder auf der **Apps**-Seite zur 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.

Angeben anderer Ansichten für Desktops und Anwendungen

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

1. Navigieren Sie auf der Windows-**Startseite** oder auf der **Apps**-Seite zur 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, die angezeigt werden sollen.

Aktivieren der Ordneransicht:

1. Navigieren Sie auf der Windows-**Startseite** oder auf der **Apps**-Seite zur 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 auf **Konfigurieren**.
3. Wählen Sie **Erweiterte Einstellungen** und aktivieren Sie **Ordneransicht aktivieren**.

Beenden des Angebots von Provisioningdateien für Benutzer

Standardmäßig werden von Citrix Receiver für Web-Sites Provisioningdateien angeboten, damit die Benutzer Citrix Receiver bzw. die Citrix Workspace-App 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 Citrix Gateway-Bereitstellungen und Beacons. In diesem Artikel gelten die Erläuterungen zur Citrix Workspace-App, sofern nicht anders angegeben, auch für die unterstützten Versionen von Citrix Receiver.

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

1. Klicken Sie auf dem Windows-Bildschirm **Start** oder **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 **Receiver-/Workspace-App-Konfiguration aktivieren**.

Konfigurieren der Site-Funktionsweise für Benutzer ohne Citrix Workspace-App

Verwenden Sie die Aufgabe **Citrix Workspace-App bereitstellen** zum Konfigurieren der Funktionsweise einer Citrix Receiver für Web-Site,wenn ein Windows- oder Mac OS X-Benutzer ohne Citrix Workspace-App 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 die Citrix Workspace-App installiert ist.

Wenn die Citrix Workspace-App nicht erkannt wird, wird der Benutzer aufgefordert, die App herunterzuladen und zu installieren. Standardmäßig erfolgt der Download von der Citrix Website. Sie

können die Citrix Workspace-App-Installationsprogramme jedoch auch auf den StoreFront-Server kopieren, damit die Benutzer sie direkt vom StoreFront-Server herunterladen können.

Für Benutzer, die die Citrix Workspace-App nicht installieren können, können Sie die Citrix Workspace-App für HTML5 auf den Citrix Receiver für Web-Sites aktivieren. Mit der Citrix Workspace-App für HTML5 können Benutzer direkt in HTML5-kompatiblen Browsern auf Desktops und Anwendungen zugreifen, ohne die Citrix Workspace-App installieren zu müssen. Sowohl interne Netzwerkverbindungen als auch Verbindungen über Citrix Gateway werden unterstützt. Bei Verbindungen über das interne Netzwerk unterstützt die Citrix Workspace-App für HTML5 allerdings nur den Zugriff auf Ressourcen, die von bestimmten Produkten bereitgestellt werden. Außerdem sind bestimmte Versionen von Citrix 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 die Citrix Workspace-App für HTML5 auf Ressourcen, die von Citrix Virtual Apps and Desktops bereitgestellt werden, standardmäßig deaktiviert. Sie aktivieren den lokalen Zugriff auf Desktops und Anwendungen über die Citrix Workspace-App für HTML5, indem Sie die Richtlinie für ICA-WebSockets-Verbindungen auf den Citrix Virtual Apps and Desktops-Servern aktivieren. Citrix Virtual Apps and Desktops verwendet Port 8008 für Verbindungen mit der Citrix Workspace-App für HTML5. Stellen Sie sicher, dass Firewalls und andere Netzwerkgeräte den Zugriff auf diesen Port zulassen. Weitere Informationen finden Sie unter Einstellungen der Richtlinie “WebSockets”.

Damit Ressourcen von Citrix Virtual Apps and Desktops mit der Citrix Workspace-App für HTML5 und einer direkten Verbindung mit StoreFront gestartet werden können, müssen TLS-Verbindungen mit den VDAs konfiguriert werden, auf denen die Apps und Desktops gehostet werden. Bei Remoteverbindungen über ein Citrix Gateway können Ressourcen über die Citrix Workspace-App für HTML5 ohne Konfiguration von TLS-Verbindungen mit dem VDA gestartet werden.

1. Klicken Sie auf dem Windows-Bildschirm **Start** oder **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/Workspace-App bereitstellen** und geben Sie eine **Bereitstellungsoption** an.
    - Wenn Sie möchten, dass der Zugriff auf Ressourcen über die Citrix Workspace-App für HTML5 ohne Aufforderung zum Download und Installieren der Citrix Workspace-App erfolgt, wählen Sie **Immer Receiver für HTML5 verwenden** aus. Wenn diese Option aktiviert ist, greifen die Benutzer immer über die Citrix Workspace-App für HTML5 auf Desktops und Anwendungen auf der Site zu, sofern sie einen HTML5-kompatiblen Browser haben. Benutzer ohne HTML5-kompatiblen Browser können nicht auf Ressourcen zugreifen. Der Zugriff über eine lokal installierte Citrix Workspace-App ist deaktiviert.

- Wählen Sie **Receiver für HTML5 verwenden, wenn lokaler Receiver nicht verfügbar ist**, wenn die Benutzer aufgefordert werden sollen, die Citrix Workspace-App herunterzuladen und zu installieren, aber auf die Citrix Workspace-App für HTML5 zurückgegriffen wird, wenn eine Installation der Citrix Workspace-App nicht möglich ist. Benutzer ohne Citrix Workspace-App werden dann bei jeder Anmeldung an der Site aufgefordert, die App herunterzuladen und zu installieren.
- Wählen Sie **Lokal installieren**, wenn immer über eine lokal installierte Citrix Workspace-App auf Ressourcen zugegriffen werden soll. Die Benutzer werden aufgefordert, die Citrix Workspace-App für ihre Plattform herunterzuladen und zu installieren. Der Zugriff über HTML5-kompatible Browser ist deaktiviert.
  - Wenn Sie **Benutzer können HDX Engine (Plug-In) herunterladen** auswählen, ermöglichst Citrix Receiver für Web, dass Benutzer die Citrix Workspace-App herunterladen und auf dem Endbenutzerclient installieren, wenn sie nicht verfügbar ist.
  - Wenn Sie **Plug-In beim Anmelden aktualisieren** auswählen, wird in Citrix Receiver für Web die Option für das Upgrade auf die Citrix Workspace-App angezeigt, wenn sich ein Benutzer anmeldet. Die Benutzer können das Upgrade überspringen und werden nur dann erneut zum Upgrade aufgefordert, wenn Citrix Receiver für Web-Cookies gelöscht werden. Zur Verwendung dieses Features müssen Sie sicherstellen, dass die Citrix Workspace-App-Dateien auf dem StoreFront-Server verfügbar sind.
  - Wählen Sie in der Dropdownliste eine Quelle aus.

Verfügbarmachen der Citrix Workspace-App-Installationsdateien auf dem Server

Standardmäßig versucht die Site zu ermitteln, ob die Citrix Workspace-App auf dem Benutzergerät installiert ist, wenn ein Benutzer über einen Computer unter Windows oder Mac OS X auf Citrix Receiver für Web-Sites zugreift. Wenn die Citrix Workspace-App nicht erkannt wird, wird der Benutzer aufgefordert, die App von der Citrix Website (bzw. die geeignete Installationsdatei aus StoreFront) herunterzuladen und zu installieren.

1. Klicken Sie auf dem Windows-Bildschirm **Start** oder **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 Sei **Citrix Receiver/Workspace-App bereitstellen** und **Quelle für Receiver/Workspace-App** und navigieren Sie dann zu den Installationsdateien.

Ausführen der Aufforderung zur Installation der Citrix Workspace-App nach der Anmeldung

Vor der Anmeldung bei StoreFront fordert Citrix Receiver für Web Benutzer auf, die aktuelle Citrix Workspace-App zu installieren, wenn sie noch nicht seinem Computer installiert ist. Abhängig von der Konfiguration wird diese Aufforderung auch angezeigt, wenn die vorhandene Installation der Citrix Workspace-App 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 dem Windows-Bildschirm **Start** oder **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.
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/Workspace-App nach der Anmeldung**.

Entfernen von Citrix Receiver für Web-Sites

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 Benutzeroberfläche

April 1, 2020

> Hinweis:
>
> "StoreFront" wird weiter für den Unternehmensappstore verwendet, der Anwendungen und Desktops von Citrix Virtual Apps and Desktops-Sites in einem einzigen benutzerfreundlichen Store für Benutzer zusammenfasst. Die Citrix Receiver-Technologie ist jetzt in der Citrix Workspace-App enthalten. Die Umsetzung dieser Umstellung in unseren Produkten und Dokumentationen ist ein andauernder Prozess. Produktinhalte können noch den alten Namen enthalten, z. B. verweist die einheitliche Benutzeroberfläche auf "Citrix Receiver". Wir danken Ihnen für Ihre Geduld während dieser Umstellung. Weitere Informationen zu den neuen Namen finden Sie unter https://www.citrix.com/about/citrix-product-guide/.

StoreFront unterstützt die *einheitliche* Benutzeroberfläche. In einer Umgebung mit der einheitlichen Benutzeroberfläche erhalten alle Web- und systemeigenen Citrix Workspace-Apps 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, verwenden die einheitliche Benutzeroberfläche.

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

- Erstellen einer Citrix Receiver für Web-Site.
- Ändern der Benutzeroberfläche der Citrix Receiver für Web-Site.
- Auswählen einer Citrix Receiver für Web-Site mit einheitlicher Benutzeroberfläche zur Zuweisung zum Store.
- Anpassen der Receiver-Darstellung

Verwenden Sie Javascript und CSS zum Konfigurieren von Citrix Receiver für Web-Sites.

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. Zum Abschluss übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden.

> Hinweis:
>
> Mit XenApp 6.x werden Anwendungen mit der Einstellung **Stream zum Client** oder **Streaming (falls möglich), sonst Zugriff von einem Server** nicht unterstützt, wenn die einheitliche Benutzeroberfläche aktiviert ist.

Erstellen einer Citrix Receiver für Web-Website

Eine Citrix Receiver für 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 dem Windows-Bildschirm “Start” oder “Apps” 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 folgen Sie den Anweisungen im Assistenten.

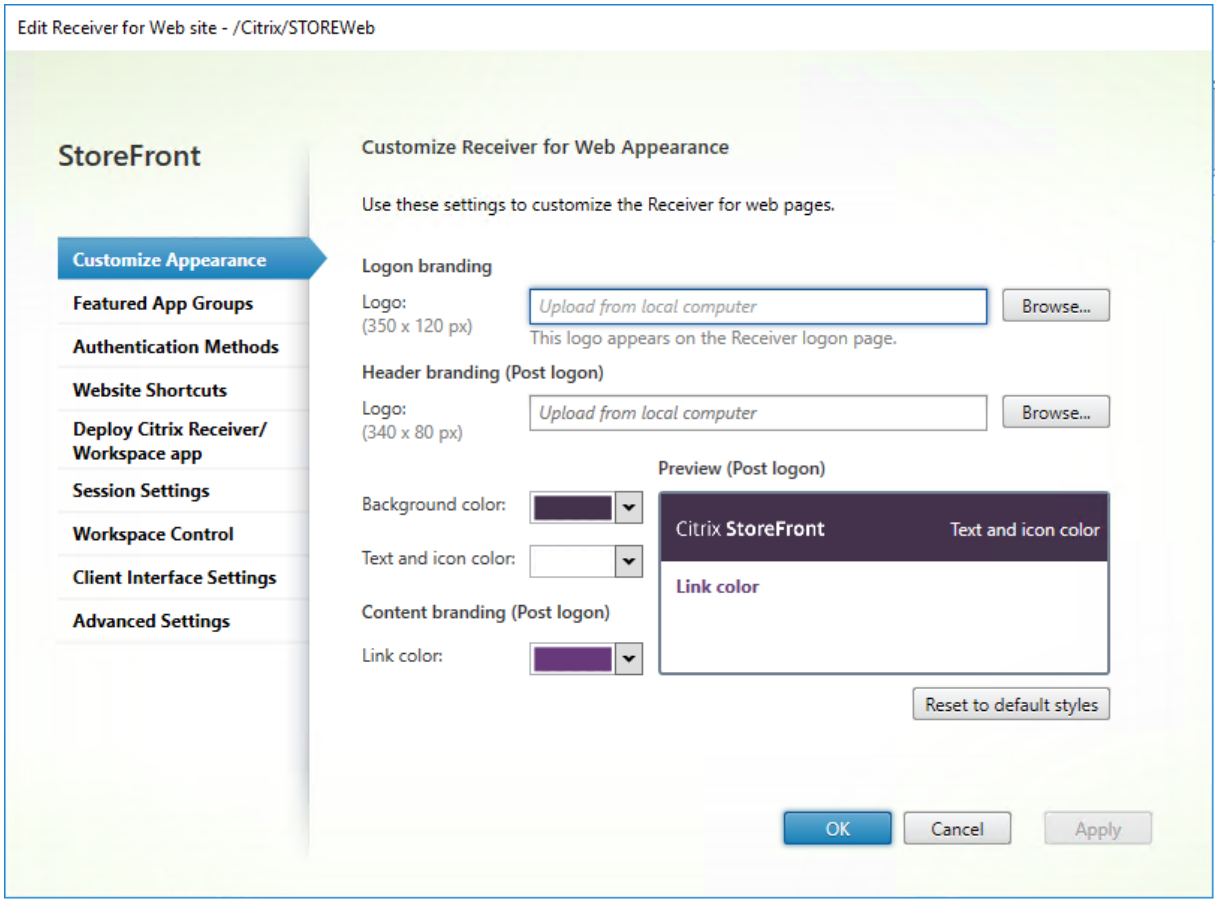
Auswählen einer Citrix Receiver für Web-Site mit einheitlicher Benutzeroberfläche zur Zuweisung zum Store

Bei der Erstellung eines neuen Stores mit StoreFront wird automatisch eine Citrix Receiver für Web-Site erstellt und dem Store zugewiesen. Citrix Receiver für Web-Sites verwenden die einheitliche Benutzeroberfläche. Wenn ein Store über mehrere Receiver für Web-Sites verfügt, müssen Sie diejenige auswählen, die angezeigt werden soll, wenn die Benutzer mit der Citrix Workspace-App auf den Store zugreifen.

1. Navigieren Sie auf der Windows-**Startseite** oder auf der **Apps**-Seite zur 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 Bereich **Aktionen** die Option **Einheitliche Benutzeroberfläche konfigurieren**. Wenn Sie keine Citrix Receiver für Web-Site erstellt haben, wird eine entsprechende Meldung mit einem Link zum Assistenten zum Hinzufügen einer solchen Site angezeigt.
3. Wählen Sie die Standardwebsite für Receiver für Web, die von Citrix Workspace-App-Clients angezeigt werden soll, wenn die Benutzer auf den Store zugreifen.
4. Klicken Sie auf **OK**.

Anpassen der Citrix Receiver-Darstellung

1. Klicken Sie auf dem Windows-Bildschirm **Start** oder “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 **Receiver für Web-Sites verwalten** und klicken Sie auf **Konfigurieren**.
3. Wählen Sie **Benutzeroberfläche anpassen** und legen Sie fest, wie die Website nach der Anmeldung angezeigt werden soll.



Weitere Konfiguration mit Javascript und CSS

> Hinweis:
>
> Fügen Sie in den Beispielen in diesem Abschnitt Javascript der Datei *script.js* hinzu (z. B. in C:\inetpub\wwwroot\Citrix\StoreWeb\custom) und fügen Sie CSS der Datei *style.css* im selben Verzeichnis hinzu.

Hinzufügen einer statischen Kopfzeile zur Anmeldeseite in Receiver für Web

"Statisch" bedeutet in diesem Zusammenhang einen feststehenden Text, etwa eine Begrüßung oder ein Firmenname. Informationen zu veränderlichem Text (z. B. Nachrichtenmeldung oder Serverstatus) finden Sie unter Hinzufügen einer dynamischen Kopfzeile zur Anmeldeseite in Receiver für Web.

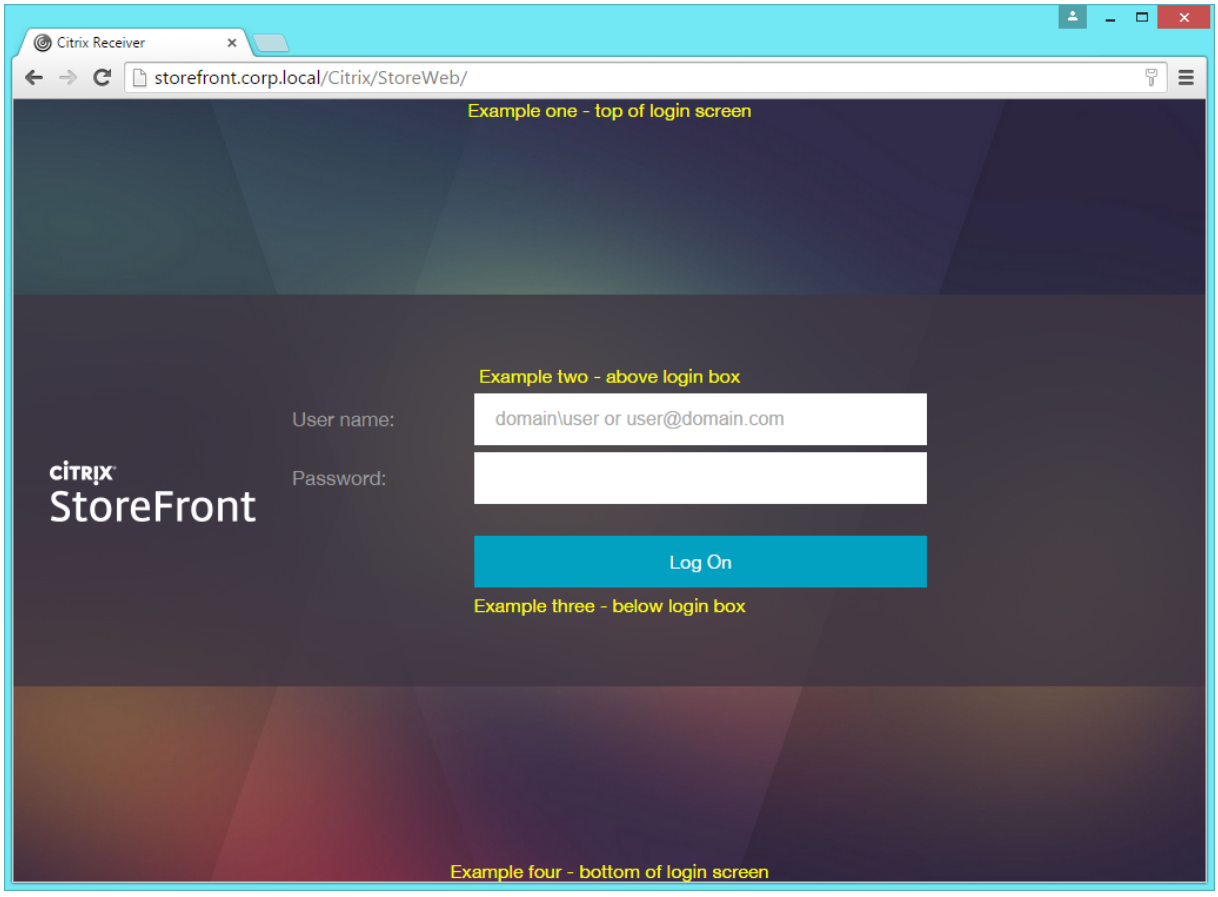
Sie können statischen Text mit den folgenden Javascript-Zeilen an vier Positionen hinzufügen:

```
1 $('.customAuthHeader').html("Example one - top of login screen");
2 $('.customAuthTop').html("Example two - above login box");
3 $('.customAuthBottom').html("Example three - below login box");
4 $('.customAuthFooter').html("Example four - bottom of login screen");
```


Um den Text hervorzuheben, fügen Sie custom.css den folgenden Stil hinzu:

```
.customAuthHeader,
.customAuthFooter,
.customAuthTop,
.customAuthBottom
{

 font-size:16px;
 color:yellow;
 text-align: center;
 }
```

Dies ergibt folgendes Ergebnis:



Zur Verwendung einer HTML-Formatierung ersetzen Sie die 4 Javascript-Zeilen durch Folgendes:

```
$('.customAuthHeader').html("<b>Example one</b>  -  top of login screen"
    );
```



```
2 $('.customAuthTop').html("<div style='background:black'>Example two -
     above login box</div>");
3 $('.customAuthBottom').html("<i>Example three - below login box</i>");
4 $('.customAuthFooter').html("<img src='logo.png'>Example four - bottom
     of login screen");
```

> Hinweis:
>
> Die vierte Zeile in dem Beispiel sucht das Bild *logo.png* im benutzerdefinierten Verzeichnis.

Hinzufügen einer dynamischen Kopfzeile zur Anmeldeseite in Receiver für Web

"Dynamisch" bedeutet in diesem Zusammenhang, dass Inhalte nicht zwischengespeichert, sondern jedes Mal geladen und angezeigt werden. In Webbrowsern werden Inhalte oft zwischengespeichert, die Citrix Workspace-App speichert jedoch immer die Benutzeroberfläche und lädt diese. Wenn Sie das Beispiel oben also für einen Dienststatus oder Ähnliches verwenden, erhalten Sie nicht das gewünschte Ergebnis.

Stattdessen ist ein Ajax-Aufruf zum dynamischen Laden und Einfügen des Inhalts erforderlich. Gehen Sie hierzu folgendermaßen vor:

1. Definieren Sie eine Hilfsprogrammfunktion, die den Inhalt von einer Seite im Verzeichnis *customweb* auf dem Server abruft und der Seite hinzufügt. Dies entspricht den obigen HTML-Beispielen und die benutzerdefinierte Seite kann Text oder einen HTML-Ausschnitt enthalten. Verwenden Sie das Verzeichnis *customweb*, da es auf alle Server in einer StoreFront-Servergruppe kopiert wird (genau wie \custom). Es wird jedoch nicht heruntergeladen und zwischengespeichert.
2. Programmieren Sie den Aufruf dieser Funktion zu einem geeigneten Zeitpunkt. Ein zu früher Aufruf führt zu Problemen in der Citrix Workspace-App, da das Skript ausgeführt wird, bevor die Konfiguration vollständig geladen ist. Ein guter Zeitpunkt ist **beforeDisplayHomeScreen**, sollen jedoch Inhalte auf der Anmeldeseite angezeigt werden, verwenden Sie stattdessen **beforeLogin**. Der folgende Code ist für beide Fälle geeignet und kann für Web- und native Clients verwendet werden.

Vollständiges Skript:

```
1 function setDynamicContent(txtFile, element) {
2
3    CTXS.ExtensionAPI.proxyRequest({
4
5       url: "customweb/"+txtFile,
6       success: function(txt) {
7  $(element).html(txt); }
```



```
  }
 );
 }


var fetchedContent=false;
function doFetchContent(callback)
{

  if(!fetchedContent) {

    fetchedContent = true;
    setDynamicContent("ReadMe.txt", "#customScrollTop");
   }

  callback();
 }


CTXS.Extensions.beforeDisplayHomeScreen = doFetchContent;
CTXS.Extensions.beforeLogon = doFetchContent;
```

Dadurch werden Inhalte aus *customwebreadme.txt* geladen, die immer einige uninteressante Informationen enthält. Fügen Sie Ihre eigene Datei (*status.txt*) hinzu und passen Sie das Skript entsprechend an, um das gewünschte Ergebnis zu erzielen.

Anzeigen einer Durchklick-Meldung vor oder nach der Anmeldung

Das folgende Beispiel ist bereits in der Datei *script.js* als Beispiel enthalten, muss jedoch auskommentiert werden. Es gibt zwei Codeversionen: Die erste für die Anzeige vor der Anmeldung für Webbrowser und die zweite für die Anzeige vor Aufrufen der Hauptbenutzeroberfläche für native Clients. Wenn Sie nur eine Meldung nach der Anmeldung wünschen, löschen Sie die erste Funktion. Die alleinige Verwendung einer Meldung vor Anmeldung ist keine gute Wahl, da der Anmeldefluss nur in Webbrowsern (und nicht in nativen Clients) angezeigt wird. Außerdem wird der Anmeldefluss verborgen, wenn Benutzer über Citrix Gateway zugreifen.

```
var doneClickThrough = false;

// Before web login
CTXS.Extensions.beforeLogon = function (callback) {

  doneClickThrough = true;
  CTXS.ExtensionAPI.showMessage({
```



```
8
9       messageTitle: ”Welcome!”,
10      messageText: ”Only for WWCo Employees”,
11      okButtonText: ”Accept”,
12      okAction: callback
13     }
14  );
15  }
16  ;
17
18 // Before main screen (both web and native)
19 CTXS.Extensions.beforeDisplayHomeScreen = function (callback) {
20
21   if (!doneClickThrough) {
22
23     CTXS.ExtensionAPI.showMessage({
24
25       messageTitle: ”Welcome!”,
26       messageText: ”Only for WWCo Employees”,
27       okButtonText: ”Accept”,
28       okAction: callback
29      }
30  );
31    }
32   else {
33
34     callback();
35    }
36
37  }
38  ;
```

Verbreitern des Meldungsfelds

Das Meldungsfeld für **CTXS.ExtensionAPI.showMessage()** ist vorformatiert. Sie können es verbreitern, sodass es sich auch für andere Meldungen eignet. Fügen Sie script.js die folgende Beispielfunktion hinzu, um das Feld anschließend erneut zu verkleinern. Rufen Sie **showLargeMessage()** anstelle von **CTXS.ExtensionAPI.showMessage()** auf, wenn Sie ein größeres Feld wünschen.

```
1  function mkLargeMessageExitFn(origfn)
2  {
3
4    if(origfn) {
```



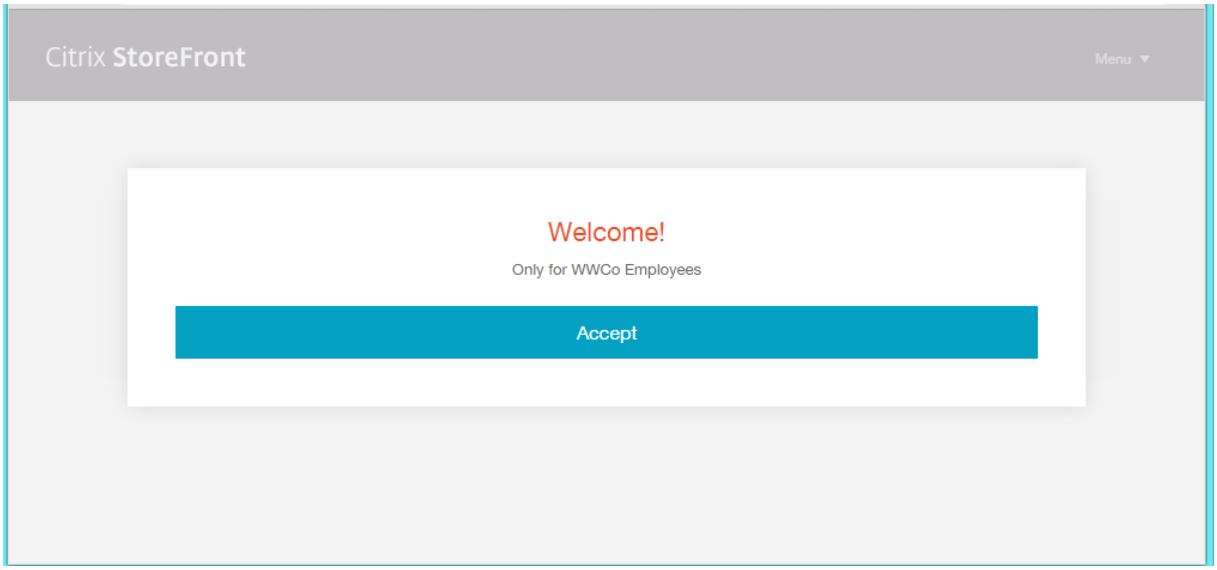
```
5
6       return function() {
7
8         origfn();
9         window.setTimeout(function() {
10   $('body').removeClass('largeMessage'); }
11   ,500);
12       }
13   ;
14     }
15
16   }
17
18
19  function showLargeMessage(details)
20  {
21
22    $('body').addClass('largeMessage');
23    details.cancelAction = mkLargeMessageExitFn(details.cancelAction);
24    details.okAction = mkLargeMessageExitFn(details.okAction);
25    CTXS.ExtensionAPI.showMessage(details);
26   }
27   ;
```

Dadurch wird eine Markerklasse hinzugefügt, wenn das größere Feld angezeigt wird. Wenn das Feld geschlossen ist, wird die Markerklasse nach einer kurzen Verzögerung (zum Vermeiden eines Ruckelns) entfernt.

Fügen Sie CSS hinzu, um die Feldgröße basierend auf dem Vorhandensein der Markerklasse anzupassen. Beispiel in custom\style.css:

```
1  .largeTiles .largeMessage .messageBoxPopup
2  {
3
4    width:800px;
5   }
```

Wenn dann ein MessageBoxPopup auf einer großen Benutzeroberfläche angezeigt wird und das LargeMessage-Flag gesetzt ist, ist das Feld 800 Pixel breit. Vorhandener Code stellt sicher, dass es zentriert ist. (Auf einer kleinen Benutzeroberfläche, etwa einem Mobiltelefon, hat das Standardmeldungsfeld bereits die volle Breite.)



Um noch mehr Text einzufügen, können Sie die Schriftgröße durch folgende Angabe in custom-style.css reduzieren. Alternativ können Sie Scrollbare Inhalte hinzufügen.

```
.largeTiles .largeMessage .messageBoxText
{

  font-size:10px;
 }
```

Durchklick-Meldungsfeld scrollbar konfigurieren

Wenn Sie **showMessage** aufrufen, können Sie anstelle der reinen Zeichenfolge HTML übergeben, um einen Stil zu verwenden. Ersetzen Sie hierzu messageText für showMessage durch Folgendes:

```
    CTXS.ExtensionAPI.showMessage({

          messageTitle: ”Welcome!”,
          messageText: ”&lt;div class=’disclaimer’&gt;rhubarb rhubarb
              rhubarb ... rhubarb rhubarb&lt;/div&gt;”,
          okButtonText: ”Accept”,
          okAction: callback  }
 );
```

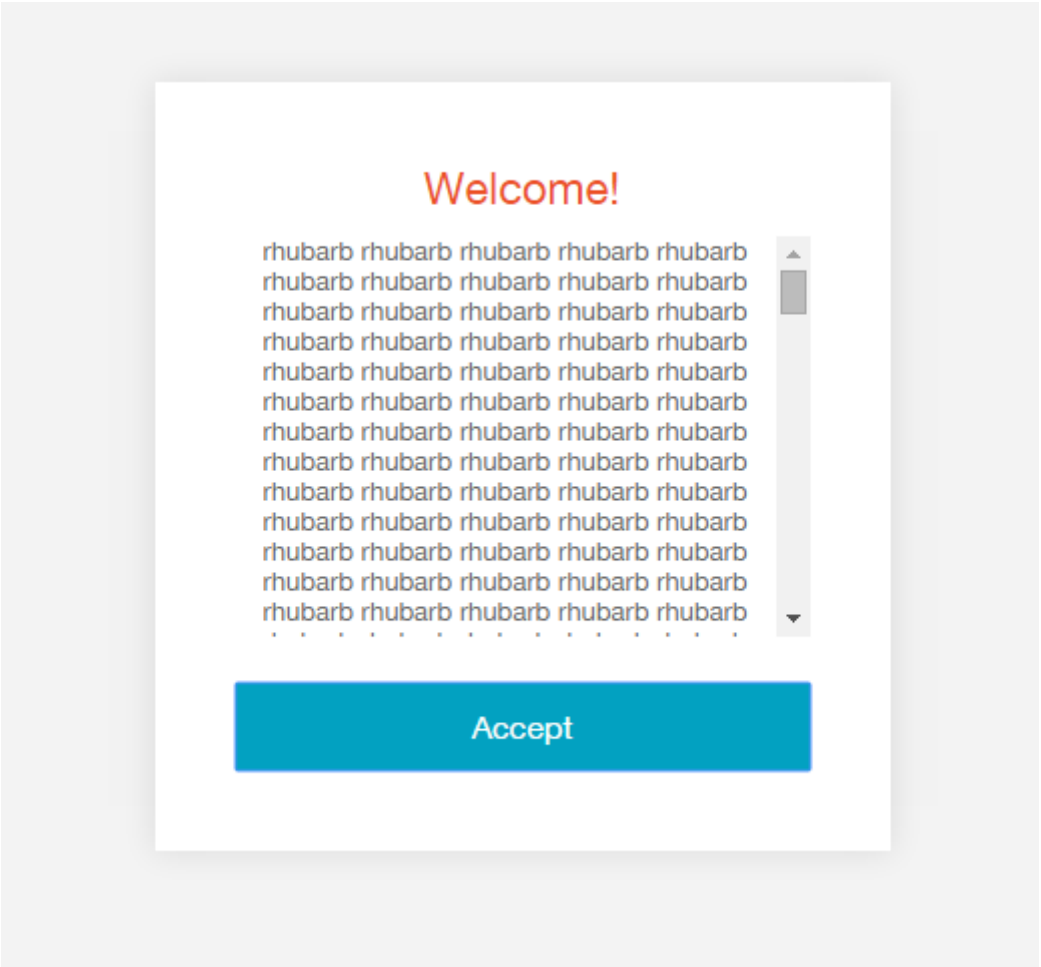
Fügen Sie dann style.css Folgendes hinzu:

```
.disclaimer {

    height: 200px;
```



```
    overflow-y: auto;
}
```

Dies ergibt folgendes Ergebnis:



Hinzufügen einer Fußzeile zu jeder Seite

Hierfür gibt es einen weiteren benutzerdefinierbaren Bereich. Sie können dessen Inhalt über folgende JavaScript-Zeile festlegen:

```
$('#customBottom').html("For ACME Employees Only");
```

Definieren Sie den Stil in style.css. Legen Sie `position:static` fest, um sicherzustellen, dass der Scrollbereich wie gewünscht funktioniert.

```
#customBottom
{

```



```
text-align:center;
font-size:30px;
position:static;
}
```

> Hinweis:
>
> Wenn Sie die Größe dieses Bereichs per Skript dynamisch ändern, müssen Sie den Befehl **CTXS.ExtensionAPI.resize()** aufrufen, damit die Citrix Workspace-App erfährt, dass sich etwas geändert hat.

Festlegen der Ordneransicht auf Registerkarte “Apps” als Standard

Überwachen Sie dazu das Ereignis “view change”. Wenn sich die Ansicht zu “store” (interner Name der Apps-Ansicht) ändert, navigieren Sie zum Stammordner. Achten Sie auf Folgendes:

- Wird das Ereignis **OnViewChange** ausgelöst (= Store-Ansicht ändert sich), ist die Anzeige noch nicht abgeschlossen. Wenn Sie sofort zum Ordner navigieren, macht der Initialisierungscode für die Store-Ansicht Ihre Arbeit rückgängig, da er nach Ihrem Code ausgeführt wird. Um dies zu vermeiden, fügen Sie eine Verzögerung von 1 ms hinzu, damit Ihr Code nach dem aktuellen Stack ausgeführt wird.
- Die drei Zeilen mit dem Wort “whitespace” sorgen dafür, dass die anfängliche Benutzeroberfläche von “All Apps” durch Überlagerung mit einem großen benutzerdefinierten Bereich bildschirmextern aufgebaut wird. Dadurch wird verhindert, dass die All Apps-Ansicht flimmert, bevor die Ordner angezeigt werden.

Fügen Sie script.js folgenden Code hinzu:

```
$('#customScrollTop').append('&lt;div class="whitespace"&gt;&lt;/div&gt
    ;');

CTXS.Extensions.onViewChange = function(view) {

  if (view == "store") {

    $('.whitespace').height(5000);
    window.setTimeout(function() {

      CTXS.ExtensionAPI.navigateToFolder("/");
      $('.whitespace').height(0);
     }
 , 1);
   }
```



```
15
16  }
17  ;
```

Verbergen von Highlight-Apps aus der Anzeige aller Apps

Sie können folgenden Code verwenden, um dies zu erreichen. Beginnen Sie mit dem Speichern jeder App in einem Paket und entfernen Sie diese dann aus der Liste “All Apps display”.

```
var bundleApps = [];

CTXS.Extensions.sortBundleAppList = function(apps,bundle, defaultfn) {

  for (var i = 0; i &lt; apps.length; i++) {

    bundleApps.push(apps[i]);
   }

  defaultfn();
 }
 ;

CTXS.Extensions.filterAllAppsDisplay = function(allapps) {

  for (var i = 0; i &lt; allapps.length; i++) {

    if ($.inArray(allapps[i], bundleApps) != -1) {

       allapps.splice(i, 1);
       i--;
     }

   }

 }
 ;
```

Wenn Sie diese Anpassung vornehmen, sollten Sie die Textzeichenfolge “Alle Apps” in “Andere Apps” ändern, damit Sie die Benutzer nicht verwirren. Bearbeiten Sie hierfür die Datei *strings.en.js* im benutzerdefinierten Verzeichnis und fügen Sie dann ein Tag für **AllAppsTitle** hinzu. Beispiel (Änderungen in Gelb):

```
(function ($) {
```

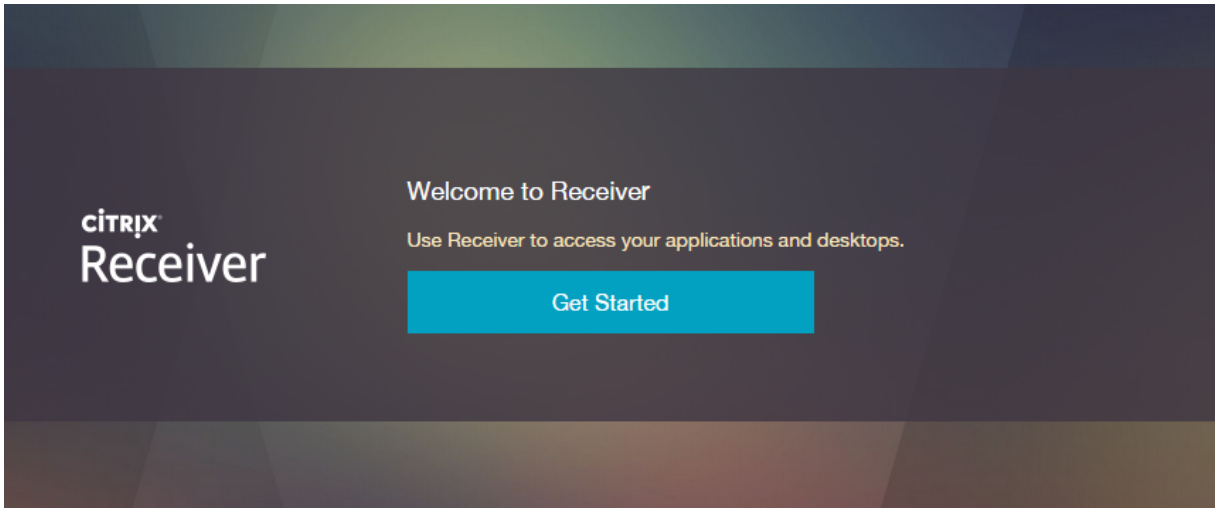


```
2
3   $.localization.customStringBundle(”en”, {
4
5    <span style=”background-color: yellow;”>AllAppsTitle: ”Other Apps”
        ,</span>
6    Example1: ”This is an example”,
7    Example2: ”This is another example”
8   }
9   );
10  }
11  )(jQuery);
```

Ändern des standardmäßigen UI-Texts

Sie können jeglichen Text der Benutzeroberfläche ändern, wenn Sie dessen Bezeichnung kennen. Um beispielsweise den Installationsbildschirm in Receiver für Web für Google Chrome in “Get Started” zu ändern, fügen Sie eine benutzerdefinierte Zeichenfolge wie folgt hinzu:

```
1  (function ($) {
2
3   $.localization.customStringBundle(”en”, {
4
5    <span style=”background-color: yellow;”>Install: ”Get Started”,</
        span>
6    Example1: ”This is an example”,
7    Example2: ”This is another example”
8   }
9   );
10  }
11  )(jQuery);
```

Ermitteln der Textbezeichnung für eine Änderung:

1. Öffnen Sie auf dem StoreFront-Server das Verzeichnis C:\inetpub\wwwroot\citrix\StoreWeb\receiver\js\local (im Beispiel wird als Name für den Store “Store” verwendet).
2. Öffnen Sie die Datei *ctxs.strings_something.js* im Editor.
3. Suchen Sie die Zeichenfolge, die Sie ändern möchten. **Hinweis**: Anstatt diese Datei direkt zu bearbeiten, erstellen Sie Außerkraftsetzungswerte im benutzerdefinierten Verzeichnis wie im “install”-Beispiel.

Ändern der Hintergrundbilder für Highlight-Kategorien

> Wichtig:
>
> Überschreiben Sie nicht die Bilder auf dem Server. Dies sorgt für, wo die Bilder bereits heruntergeladen wurden, da dort nichts von der Änderung bekannt ist. Außerdem werden Upgrades erschwert oder unmöglich gemacht.

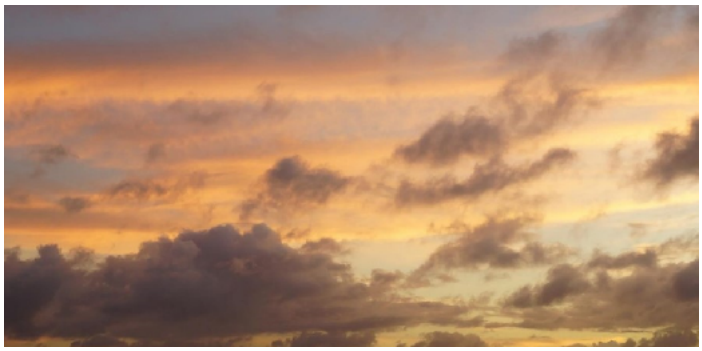
Sie können eigene Bilder im Verzeichnis *custom* einfügen und per CSS referenzieren. Jede Kategorie (= intern “bundles”) hat zwei Bilder:

- Das erste Bild wird als Kachel im Karussell verwendet.
- Das zweite Bild wird als Hintergrundbild für die Kopfzeile auf der Detailseite verwendet. Dieses Bild wird gestreckt, damit es die Bildschirmbreite abdeckt, am unteren Rand wird ein Schleier hinzugefügt.

Sie können für jeden Bildschirm verschiedene Bilder verwenden. Sie können auch das gleiche Bild verwenden, jedoch die Hintergrundhöhe auf der Detailseite verdoppeln, sodass nur die obere Bildhälfte angezeigt wird. Da das Bild auf der Detailseite gestreckt wird, sollten Sie ein Bild verwenden, das auch bei Verformung gut aussieht.

Das erste Paket hat die Klasse “AppBundle1”, das zweite “AppBundle2” und so weiter bis zu “AppBun-

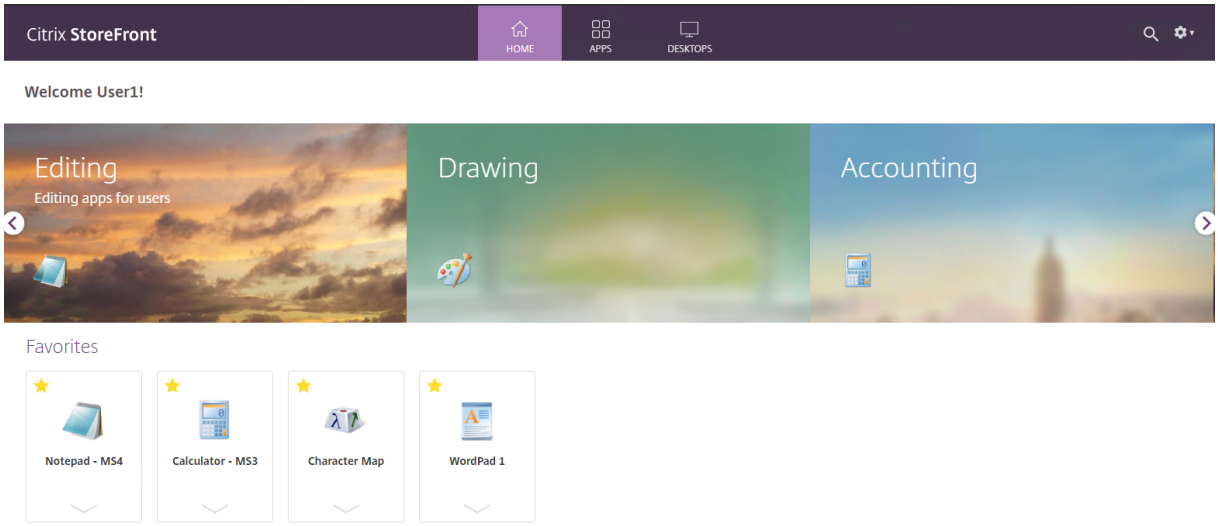
dle8”. Im folgenden Beispiel wird das Bild “clouds.png” verwendet (Sie können es mit einem rechten Maustaste auf das folgende Bild herunterladen):

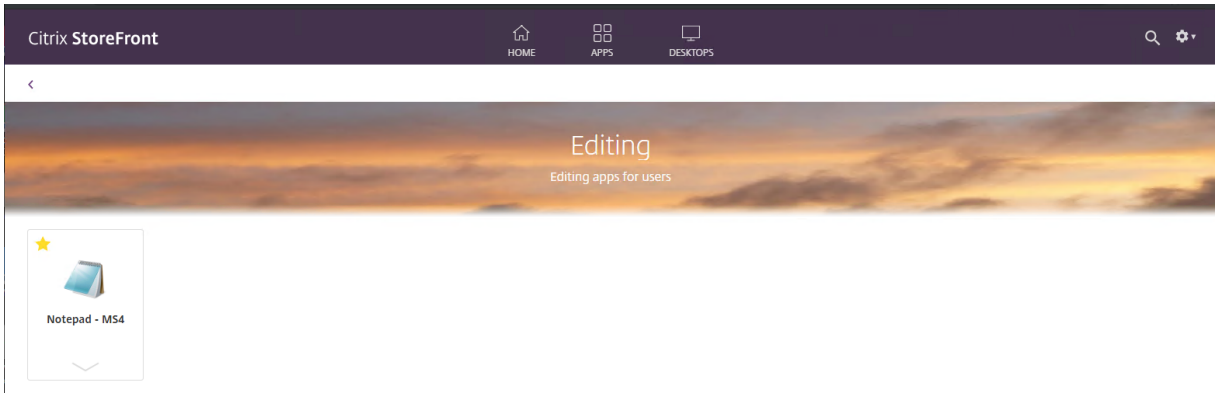


1. Speichern Sie das Bild im Verzeichnis *custom*. Das Bild muss etwa 520 × 256 Pixel groß sein, um den anderen zu entsprechen (es wird nach Bedarf skaliert).
2. Fügen Sie style.css Folgendes hinzu:

```
.appBundle1 {

  background-image: url('clouds.png');
 }


.bundleDetail.appBundle1 {

  background-image: url('clouds.png');
  background-size: 100% 200%;
 }
```

Dies ergibt folgendes Ergebnis:





Verhindern, dass ein Firmenlogo unscharf wirkt

Receiver für Web muss sowohl normale Bildschirme (“low DPI”) als auch neuere, hochauflösende (“high DPI”) korrekt verarbeiten. Bei Apple Retina-Bildschirmen ist die Auflösung beispielsweise doppelt so hoch wie bei normalen Bildschirmen. Auf Laptops haben Bildschirme in der Regel das 1,5-, 2- oder sogar 3-Fache der “normalen” Pixelgröße. Da zweifach bei weitem am häufigsten ist und den größten Unterschied ausmacht, liegen die meisten Bilder der Citrix Workspace-App in zwei Größen vor. Ein Bild mit 100 × 100 Pixeln für den normalen Bildschirm liegt auch in 200 × 200 Pixeln vor.

Wenn Sie Logobilder von der StoreFront-Verwaltungskonsole hochladen, stellen Sie sicher, dass es sich um die Bilder mit der zweifachen Größe handelt. Anders gesagt: Sie sind ungefähr doppelt so groß wie die Breite und Höhe des Platzes (“space”) auf einem normalen Bildschirm. (Bilder mit einfacher Auflösung werden nicht auf zweifache Auflösung vergrößert.) Der Platz auf einem normalen Bildschirm beträgt 170 × 40 Pixel, daher sollte ein von Ihnen hochgeladenes Logobild etwa 340 × 80 Pixel haben.

StoreFront erstellt eine Kopie des Logos und skaliert es auf die Hälfte der Größe. Dieses Bild wird auf Bildschirmen mit niedriger Auflösung verwendet.

Gelegentlich kann dies zu einer Unschärfe führen, die Hälfte der Bilddetails gelöscht wurde. Dies ist selten, da Logos in der Regel plakativ und einfach sind. Wenn Ihr Logo unscharf wirkt, verwenden Sie folgenden Workaround:

1. Erstellen Sie zwei Versionen Ihres Logos, eine in der einfachen und eine in der zweifachen Größe, und speichern Sie sie im Verzeichnis *\custom*.
2. Bearbeiten Sie *customstyle.css* so, dass sie die beiden Bilder referenziert. Beispiel:

```
<span style="color: green;">/* The following section of the file is
    reserved for use by StoreFront. \*/</span>
<span style="color: green;">/\* CITRIX DISCLAIMER: START OF MANAGED
    SECTION. PLEASE DO NOT EDIT ANY STYLE IN THIS SECTION \*/</span>
<span style="color: green;">/\* CITRIX DISCLAIMER: END OF MANAGED
    SECTION. \*/</span>
```



```
<span style="color: green;">/\* You may add custom styles below this line. */</span>

.logo-container {

    background-image: url('mylogo_x1.png');
    background-size: 169px 21px;
 }


.highdpi .logo-container {

    background-image: url('mylogo_x2.png');
    background-size: 169px 21px;
 }
```

> Hinweis:
>
> - Stellen Sie sicher, dass die benutzerdefinierten Stile nicht im Abschnitt "managed" sind. Andernfalls werden sie überschrieben, oder führen zu Problemen auf der StoreFront-Verwaltungskonsole.
> - Beide Stile geben die gleiche Hintergrundgröße an. Dies liegt daran, dass die Größe in logischen Einheiten angegeben wird, und die Hintergrundgröße für das Zweifach-Bild die Hälfte der Breite und Höhe des tatsächlichen Logos beträgt.

Festlegen eines Hintergrundbilds

> Hinweis:
>
> Die einheitliche Benutzeroberfläche ist auf einen einfachen weißen Hintergrund ausgelegt. Hintergrundbilder wirken gerne ablenkend. Wenn Sie ein Hintergrundbild verwenden, sollte dieses hell und unkompliziert sein. Passen Sie ggf. Schriftarten so an, dass sie vor dem Bild sichtbar sind.

Beispiel 1: CSS-Verweis auf hochgeladenes Bild

Ändern Sie die Datei custom.css wie folgt:

```
.storeViewSection {

   background: url('images/background.jpg') no-repeat center center fixed;
   background-size: cover;
 }
```

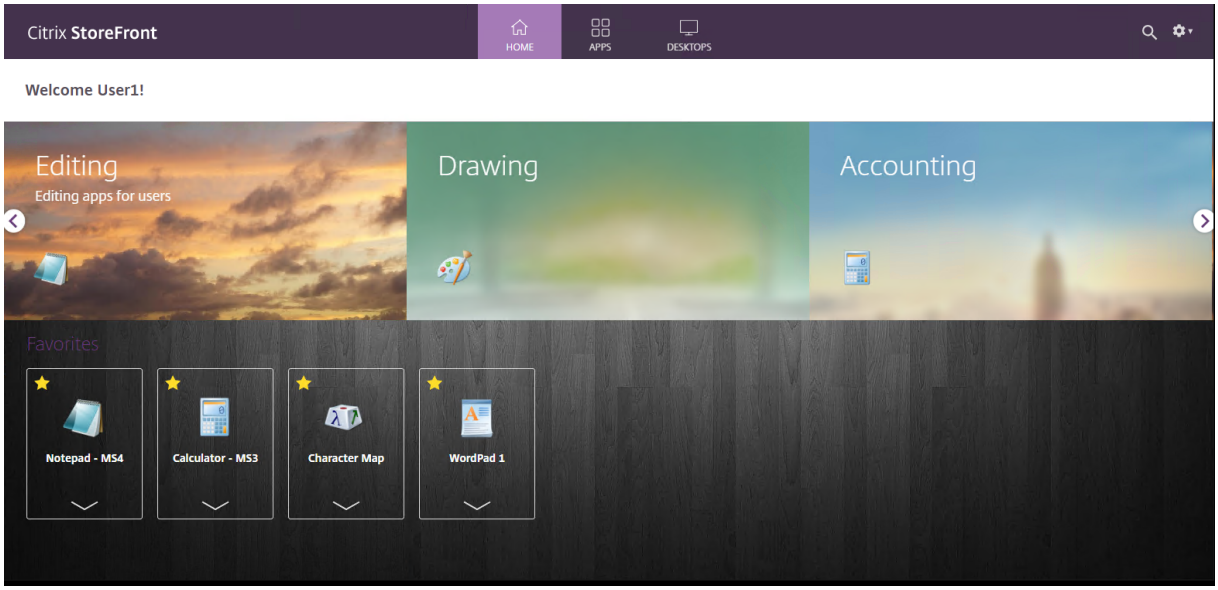

> Hinweis:
>
> Die Anweisung background-size:cover; funktioniert bei einigen älteren Browsern nicht.

Beispiel 2: CSS-Verweis auf vorhandenes Bild mit Modifizierungen

Ändern Sie die Datei custom.css wie folgt:

```
.storeViewSection {

   background: url('../media/bg_bubbles.jpg') no-repeat center center
      fixed;
    background-size: cover;
    color: white;
 }


// Tweak fonts
.smallTiles .storeapp .storeapp-name,
.largeTiles .storeapp .storeapp-name {

    color: white;
 }


// Tweak bundle area so it doesn't clash as badly
.largeTiles .applicationBundleContainer {

    background-color: rgba(255, 255, 255, 0.4);
    margin-top: 0;
    padding-top: 25px;
 }


.smallTiles .applicationBundleContainer {

    background-color: rgba(255, 255, 255, 0.4);
    margin-top: 0;
    padding-top: 14px;
 }
```

Dies ergibt folgendes Ergebnis:



Suchen von Fehlern im eigenen Code

Es gibt mehrere Möglichkeiten zum Debuggen. Versuchen Sie es immer zuerst mit einem Browser. Das ist viel einfacher als das Debuggen von Anpassungen in der Citrix Workspace-App. Sie können die folgenden Argumente nach dem ? bzw. # in der Seiten-URL hinzufügen. Sie können außerdem mehrere verketten. Beispiel:

```
1 http://storefront.wwco.net/Citrix/StoreWeb/#-tr-nocustom
```

-errors: Normalerweise versuchen wir, Fehler im Code zu unterdrücken, Sie können sie stattdessen aber anzeigen lassen. Dieses Argument zeigt ein Warnfeld an, wenn ein Fehler auftritt.

-debug: Dieses Argument deaktiviert die Ausnahmebehandlung für benutzerdefinierten Code. Es ist nützlich bei den in modernen Browsern integrierten Entwicklungstools (z. B. F12 in Google Chrome oder Internet Explorer) und wenn Sie Ausnahmen selbst debuggen.

-nocustom: Dieses Argument deaktiviert Ihre Skript- und CSS-Anpassungen. Dies ist nützlich, wenn die Citrix Workspace-App nicht funktioniert und Sie herausfinden möchten, ob dies auf einen von Ihnen eingeführten Fehler zurückzuführen ist.

-tr: Dieses Argument bietet die Ablaufverfolgung für den UI-Code der Citrix Workspace-App in einer separaten Browserregisterkarte, einschließlich einer evtl. von Ihnen über **CTXS.ExtensionAPI.trace()** hinzugefügten Ablaufverfolgung.

Einheitliche Benutzeroberfläche

In diesem Abschnitt werden die Features und das Erscheinungsbild der einheitlichen Benutzeroberfläche beschrieben.

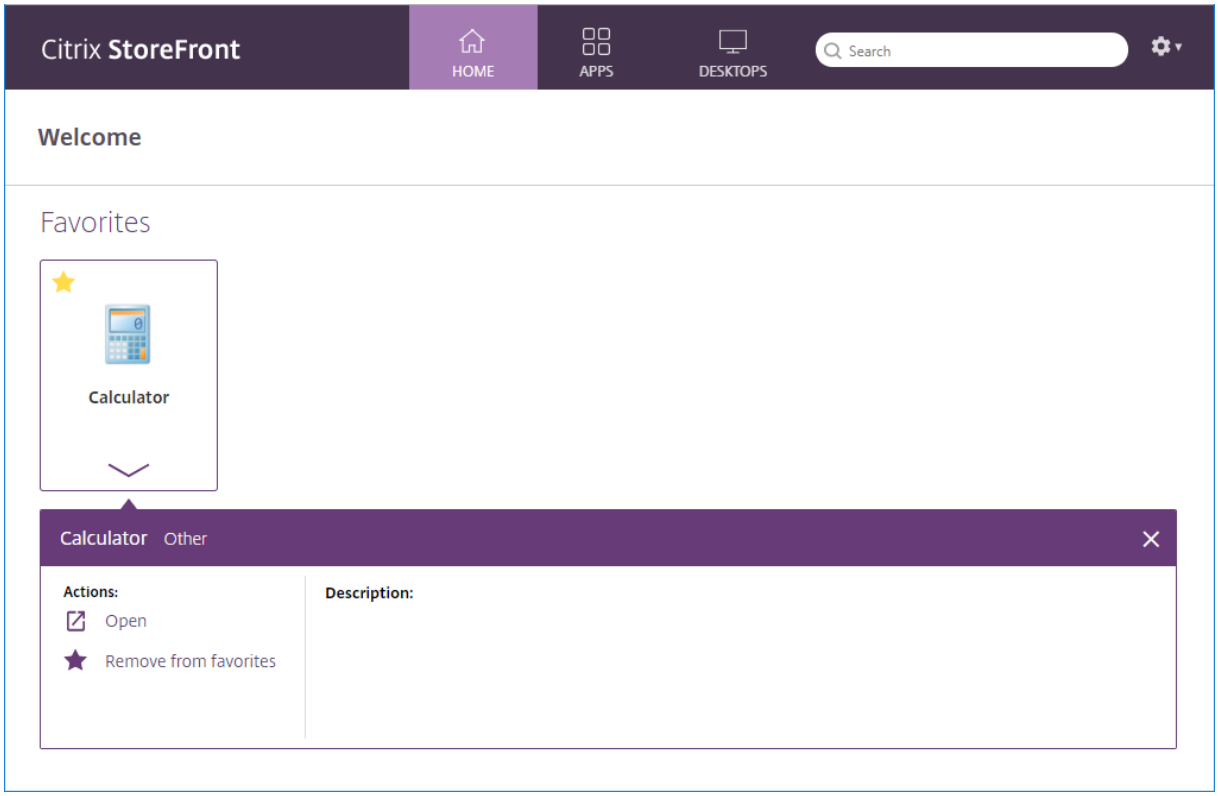
Kartenlayout

Apps im Store werden im “Kartenlayout” dargestellt. Sie können den Bereich unter jeder Karte erweitern, um weitere Details und Aktionen anzuzeigen.

> **Hinweis:**
>
> In der einheitlichen Benutzeroberfläche können Sie Anwendungen nicht per Drag & Drop neu anzuordnen.

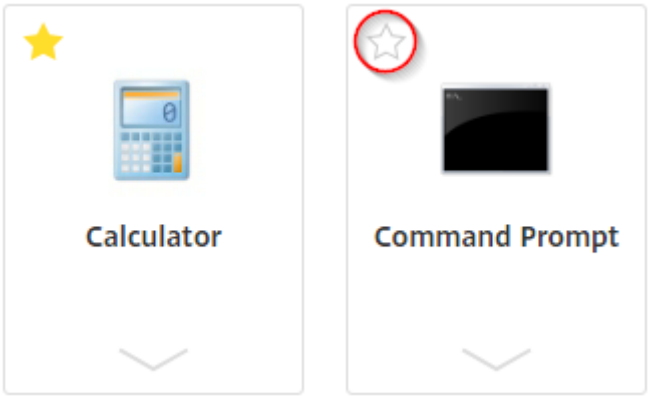
Pos1

Die Homepage zeigt die Favoriten.



Favoriten

Klicken oder tippen Sie auf den Stern, um ein Element zu einem Favoriten zu machen:



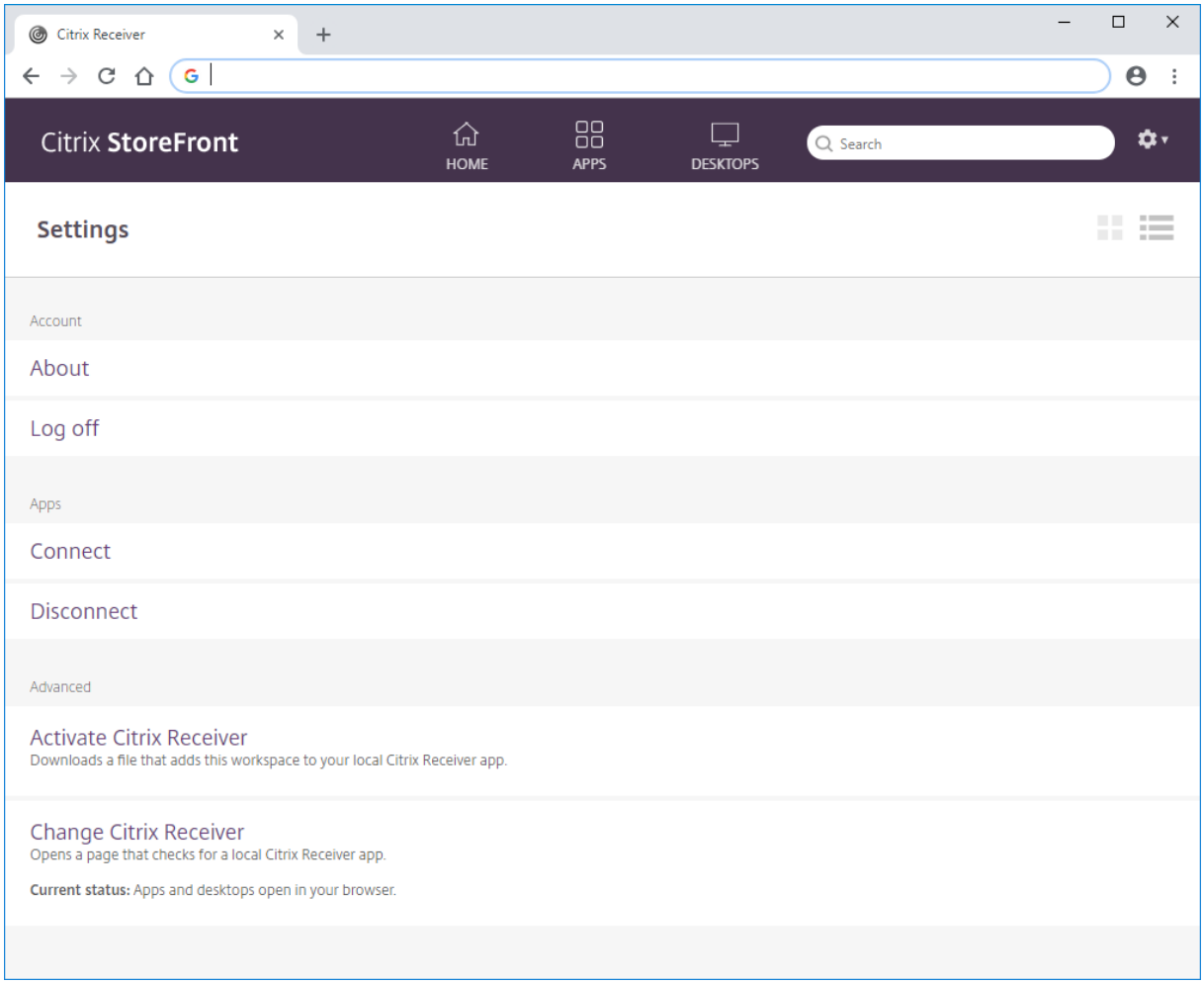
Suchen

Alle Apps, Desktops und Kategorien durchsuchen:

Einstellungen

Der Zugriff auf die Einstellungen erfolgt über das Dropdownmenü:

Das Menü zeigt den Benutzernamen, der vom Active Directory-Anzeigenamen stammt. Wenn der Anzeigename leer ist (nicht empfohlen), werden die Domäne und der Kontoname angezeigt. Verwenden Sie das Menü, um die Einstellungen zu öffnen, die Version der Citrix Workspace-App zu überprüfen oder sich abzumelden.



In den Einstellungen können Sie alle getrennten Sitzungen fortsetzen und alle aktuellen Sitzungen trennen und sich abmelden. Zeigen Sie die Einstellungen im Karten- oder Listenlayout an:

Verbinden. Setzt getrennte Sitzungen fort.

Trennen. Trennt aller aktuellen Sitzungen und meldet Sie ab.

Citrix Receiver aktivieren. Lädt eine Datei herunter, die diesen Store der lokalen Citrix Workspace-App hinzufügt.

Citrix Receiver ändern. Öffnet eine Seite, die nach einer lokalen Citrix Workspace-App sucht. So können Benutzer zwischen dem Starten von Ressourcen mit der lokal installierten Citrix Workspace-App und dem Starten der Ressourcen in einem HTML5-Browser wechseln.

Erstellen und Verwalten empfohlener Apps

April 1, 2020

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.

1. Klicken Sie auf dem Windows-Bildschirm **Start** oder “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 **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**.

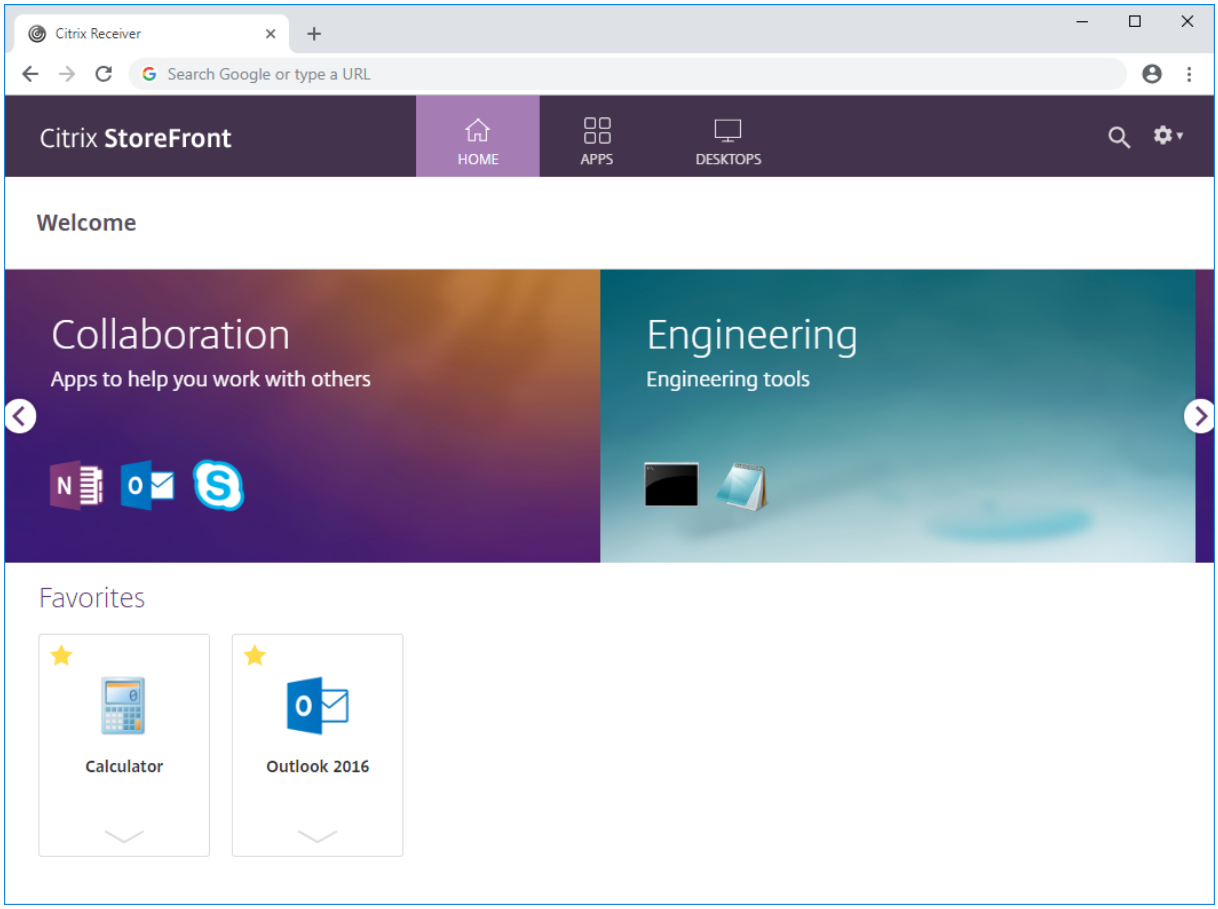
Option	Beschreibung
Schlüsselwörter	Definieren Sie die Schlüsselwörter in Studio.
Anwendungskategorie	Definieren Sie die Anwendungskategorie in Studio.

Option	Beschreibung
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

April 1, 2020

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 dem Windows-Bildschirm **Start** oder **Apps** auf die Kachel “Citrix StoreFront”.
2. Wählen Sie links **Stores** und dann im Aktionsbereich die Option **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 die Citrix Workspace-App für HTML5

April 1, 2020

Standardmäßig werden Desktops und Anwendungen in der Citrix Workspace-App für HTML5 auf einer neuen Browserregisterkarte gestartet. Beim Start von Ressourcen über Verknüpfungen mit der Citrix Workspace-App 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 dem Windows-Bildschirm **Start** oder **Apps** auf die Kachel “Citrix StoreFront”.
2. Wählen Sie links **Stores** und dann im Aktionsbereich die Option **Receiver für Web-Sites verwalten** und klicken Sie auf **Konfigurieren**.
3. Wählen Sie **Citrix Receiver/Workspace-App bereitstellen**.
4. Wählen Sie **Immer Receiver für HTML5 verwenden** in den **Bereitstellungsoptionen** 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

March 3, 2020

Standardmäßig erfolgt bei Anforderungen von einer Citrix 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 **Erweiterte Einstellungen**, 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. Navigieren Sie auf der Windows-**Startseite** oder auf der **Apps**-Seite zur 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 unter **Aktion** die Option **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 Sitzungstimeouts

Wenn das Sitzungstimeout in StoreFront nicht richtig konfiguriert ist, sehen Benutzer möglicherweise die folgende Timeoutmeldung: “Sitzungstimeout aufgrund von Inaktivität”. Sie können den Sitzungstimeoutwert neu einstellen, um den Inaktivitätstimer entsprechend dem Nutzungsmuster Ihrer Benutzer zu erhöhen.

Führen Sie die folgenden Schritte aus, um das Sitzungstimeout in StoreFront zu konfigurieren:

Erhöhen des Sitzungstimeouts für StoreFront

1. Navigieren Sie in StoreFront zu **c:\inetpub\wwwroot\Citrix<StoreWeb>**.
2. Suchen Sie den Eintrag `<sessionState timeout=”20”/>` in der Datei `web.config`.
3. Ändern Sie `sessionState timeout` zum gewünschten Wert in Minuten.

Erhöhen der maximalen Tokenlebensdauer des Authentifizierungsdiensts

Wenn Sie das Sitzungstimeout für Citrix Receiver für Web auf mehr als eine Stunde erhöhen, müssen Sie auch die maximale Lebensdauer des Tokens unter **Authentifizierungsdienst** entsprechend erhöhen.

Erhöhen des Sitzungszeitlimits für die Citrix Workspace-App

1. Navigieren Sie für die auf dem StoreFront-Server installierte Citrix Workspace-App zum Pfad des Authentifizierungsdiensts Ihres Stores. In neueren StoreFront-Versionen ist dies **c:\inetpub\wwwroot\Citrix\<Store>Auth** (und je nach Anzahl der Stores einer von mehreren Authentifizierungsdiensten).

   In älteren StoreFront-Versionen ist der Pfad **c:\inetpub\wwwroot\Citrix\Authentication** (und kann von Authentifizierungsdiensten geteilt werden oder als einziger auf dem Server vorliegen).

2. Suchen Sie in der Datei `web.config` den Eintrag **<defaultLifetime="01:00:00" maxLifetime="01:00:00">**
3. Ändern Sie **maxLifetime** zum gewünschten Wert.

> Hinweis:
>
> Citrix Workspace-App für Windows und Citrix Workspace-App für Linux. Nach dem Abmelden von der aktuellen Sitzung wird möglicherweise Citrix Virtual Apps and Desktops im Hintergrund angezeigt. Sie sollten Ihre Anmeldeinformationen jedoch neu eingeben, wenn Sie nach dem StoreFront-Sitzungstimeout auf eine App oder einen Desktop klicken.

Erhöhen der Lebensdauer des Authentifizierungstokens

Wenn der Timeoutwert mehr als acht Stunden ist, bearbeiten Sie die Datei `web.config` unter Citrix Receiver für Web, um die Lebensdauer des Authentifizierungstoken zu erhöhen:

1. Navigieren Sie in StoreFront zu **c:\inetpub\wwwroot\Citrix<StoreWeb>**.
2. Gehen Sie zu dem Eintrag: **<authentication tokenLifeTime="08:00:00"method="Auto"/>**
3. Ändern Sie **tokenLifeTime** zum gewünschten Wert.

Neustarten von IIS

- Führen Sie den Befehl **iisreset** aus, um die Änderungen anzuwenden. Wenn Sie diesen Befehl ausführen, werden die Benutzer von Citrix Receiver für Web abgemeldet und es hat keine Auswirkungen auf die aktuelle ICA-Sitzung.

> **Hinweis:**
>
> Das Formt für die Lebensdauer ist `.d.hh:mm:ss[.ff]`. Die maximale Lebensdauer ist nicht auf 24 Stunden begrenzt.

Weitere Ressourcen

- Citrix Blog - Idle timeout Receiver for Web
- Security Token Services API

Konfigurieren des Benutzerzugriffs

April 1, 2020

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 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. Navigieren Sie auf der Windows-**Startseite** oder auf der **Apps**-Seite zur 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 **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 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 bei der Erstellung angegebene Name.

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

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 Citrix Workspace-App. Dieses Feature wird über die StoreFront-Konsole oder PowerShell verwaltet.

Verwenden der StoreFront-Verwaltungskonsole

1. Klicken Sie auf dem Windows-Bildschirm **Start** oder "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 die Option **Sitzungswiederverbindung zulassen**.

Verwenden von PowerShell

Schließen Sie die Verwaltungskonsole und führen Sie das folgende Codesnippet aus, um die StoreFront PowerShell-Module zu importieren:

```
$ 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] <Int64>] [[-VirtualPath] <String> ]
[[-IsAllowed] <Boolean>]
```

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
```

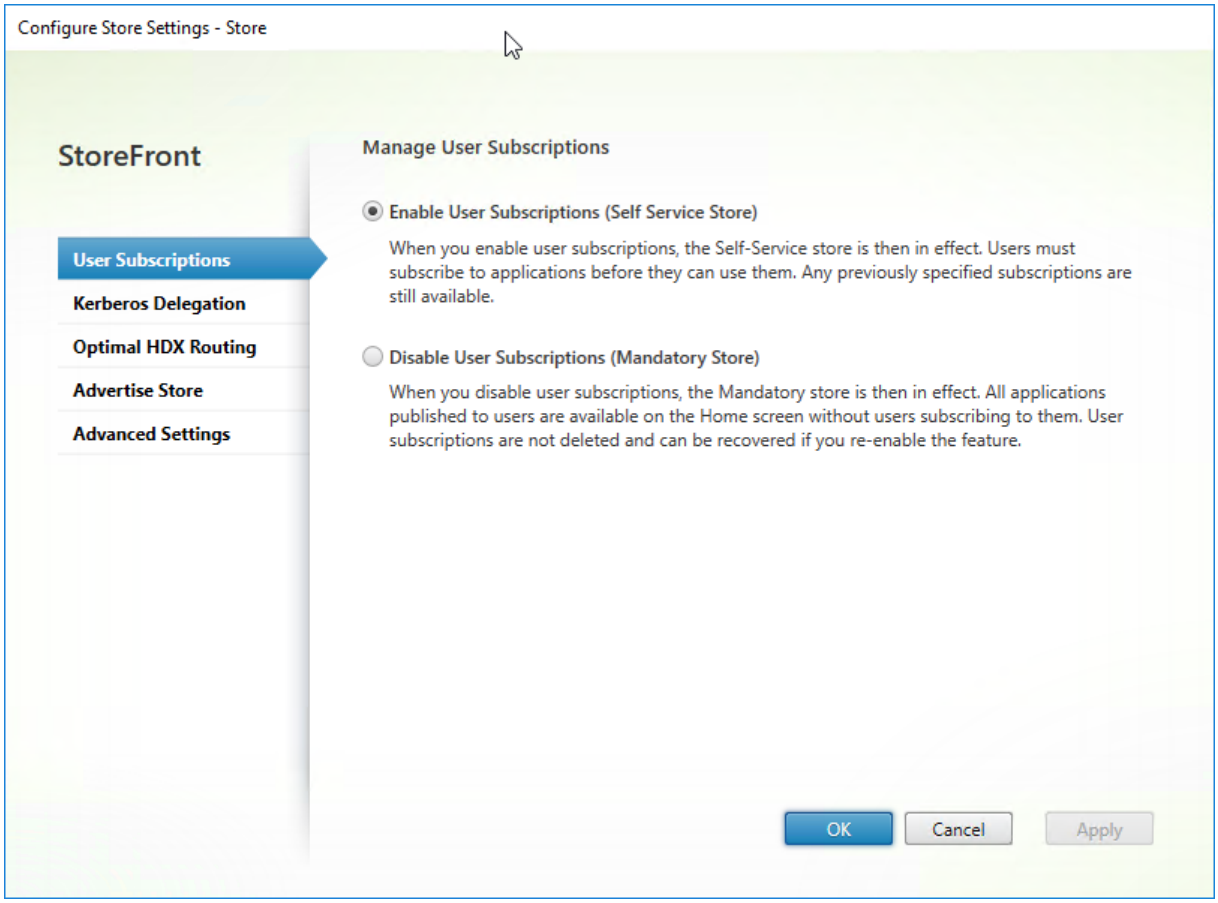
Konfigurieren von Benutzerabonnements

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 den Benutzern nicht die Registerkarte “Favoriten” in der Citrix Workspace-App angezeigt. Das Deaktivieren der Abonnements hat keine Löschung der Store-Abonnementdaten zur Folge. Werden Abonnements für den Store reaktiviert, können Benutzer ihre abonnierten Apps in den Favoriten anzeigen, sobald sie sich das nächste Mal anmelden.

1. Navigieren Sie auf der Windows-**Startseite** oder auf der **Apps**-Seite zur 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** > **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:

```
1 $StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath ”/citrix/<
    yourstore>”
2 Set-STFStoreService -StoreService $StoreObject -LockedDown $True -
    Confirm:$False
```

Weitere Informationen zu Get-STFStoreService finden Sie unter https://developer-docs.citrix.com/projects/storefront-powershell-sdk/en/latest/Get-STFStoreService/

Konfigurieren von StoreFront zum Starten von Anwendungen und Desktops im Fenstermodus

June 12, 2019

Das Starten der Anwendungen im Seamlessmodus hängt von der Verfügbarkeit von StoreFront in der Bereitstellung ab. Wenn Sie die Seamlessoption für Anwendungen und Desktops deaktivieren, sollten

Sie stattdessen die Ressourcen im Fenstermodus starten.

Im Folgenden finden Sie ein Beispiel für einen veröffentlichten Editor. Verwenden Sie den Namen der veröffentlichten Anwendung, wie er in der Citrix Virtual Apps and Desktops-Konsole angezeigt wird.

> **Hinweis:**
>
> Bei den meisten Einstellungen in ICA-Dateien wird die Groß- und Kleinschreibung nicht berücksichtigt. Ausnahmen sind die Einstellungen `DesiredHRES` und `DesiredVRES`. Wenn Sie die Version im Fenstermodus anwenden, verwenden Sie den Browsernamen, um auf die App in der Datei *default.ica* auf dem StoreFront-Server zu verweisen. Überprüfen Sie den Browsernamen der Anwendung mit PowerShell auf dem Delivery Controller:
>
> ```
> >>asnp citrix*
> ```
>
> ```
> >>Get-BrokerApplication -ApplicationName
> ```

Konfigurieren von StoreFront

1. Bearbeiten Sie die Datei default.ica auf dem StoreFront-Server im Verzeichnis `\inetpub\wwwroot\Citrix\StoreName\App_Data`.
2. Suchen Sie in der Datei default.ica folgende Zeilen: `[ApplicationServers] application =`.
3. Erstellen Sie eine Zeile nach `application=` und fügen Sie die folgenden Parameter hinzu:

   ```
   [Notepad]
   TWIMode=Off
   DesiredHRES=1024
   DesiredVRES=768
   ```

4. Speichern Sie die Datei.

Für veröffentlichte Desktops in Citrix Virtual Apps and Desktops 7.x und StoreFront 3.x

1. Bearbeiten Sie die Datei *web.config* auf dem StoreFront-Server im Verzeichnis `C:\inetpub\wwwroot\Citrix\storeWeb`.
2. Suchen Sie in der Datei web.config die folgende Zeile: `showDesktopViewer=''true''`.
3. Ändern Sie den Wert von **true** in **false**.
4. Verwenden Sie auf der Clientseite oder in AD-GPMC die administrative Vorlage `receiver.adm` oder `receiver.admx\receiver.adml` (je nach Betriebssystem) zum Konfigurieren der folgenden Richtlinie:
   - **Computerkonfiguration > Citrix Komponenten > Citrix Receiver > Benutzererfahrung > Clientanzeigeeinstellungen: Aktivieren**
   - **Seamlessfenster: False**

- **Fensterbreite: <`As per requirement`>, Fensterhöhe: <`As per requirement`>**

Hinweise

`DeisredHRES` und `DesiredVRES` können auf jede gewünschte Auflösung eingestellt werden, z. B. 800x600 oder 1024x768.

Wenn die Anwendung in Prozent der Bildschirmgröße ausgeführt werden muss, fügen Sie nach der Einstellung `TWIMode=Off` die Zeile `ScreenPercent=90` hinzu, die den Bildschirm auf 90 Prozent konfiguriert. Sie können dies auch mit der XenApp Services-Site erreichen. Stellen Sie sicher, dass die entsprechende Datei im Ordner `conf` für diese Site (Inetpub\wwwroot\Citrix\PNAgent\conf) bearbeitet wird.

Wenn Sie den 10.x-Client verwenden und die Datei **`default`**`.ica` oder `template.ica` bearbeiten, fügen Sie nur die Zeile `TWIMode=Off` hinzu. Er erhält die Einstellungen `HRES` und `VRES` aus den Eigenschaften der veröffentlichte Anwendung. Andernfalls wird ein Fehler für doppelte Einträge in der ICA-Datei angezeigt, wenn ein Benutzer versucht, die Anwendung zu starten.

Einrichten hoch verfügbarer Stores mit mehreren Sites

April 1, 2020

> **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.

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

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.
- **Bereitstellungen Zonen zuordnen:** Wenn der Zugriff mit Citrix Gateway in einer Konfiguration mit globalem Lastausgleich erfolgt, priorisiert StoreFront beim Starten von Ressourcen Bereitstellungen aus Zonen, die mit der Gateway-Zone übereinstimmen.

1. Stellen Sie sicher, dass Sie den Store mit Details aller Citrix Virtual Apps and Desktops-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. Navigieren Sie auf der Windows-**Startseite** oder auf der **Apps**-Seite zur Kachel **Citrix StoreFront**.
3. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores** und klicken Sie auf **Delivery Controller verwalten** im Bereich **Aktionen**.
4. Wenn zwei oder mehr Controller definiert sind, 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**, um Ressourcen aus mehreren Bereitstellungen zusammenzufassen. Wenn Delivery Controller aggregiert werden, werden Anwendungen und Desktops von Delivery Controllern mit dem gleichen Anzeigenamen und Pfad als Einzelanwendung oder -desktop in der Citrix Workspace-App angezeigt.

    a) Um Delivery Controller zu aggregieren, wählen Sie mehrere Controller aus und klicken Sie auf **Aggregieren**.

    b) Wählen Sie Optionen für **Aggregierte Controllereinstellungen** aus:

    Controller veröffentlichen identische Ressourcen - Wenn aktiviert, enumeriert StoreFront nur die Ressourcen von einem der Controller in dem aggregierten Satz. 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 - Wenn aktiviert, werden Starts gleichmäßig auf die verfügbaren Controller verteilt. Ist diese Option deaktiviert, wer-

den Starts an den ersten Controller geleitet, der im Benutzerzuordnungsdialogfeld angegeben wurde. Es wird ein Failover auf weitere Controller durchgeführt, wenn der Start fehlschlägt.

7. Klicken Sie im Dialogfeld “Konfiguration der Benutzerzuordnung und der Multisiteaggregation” auf **OK**.
8. Klicken Sie auf im Dialogfeld “Delivery Controller verwalten” auf **OK**.

Erweiterte Konfigurationen

Sie können viele gängige Einstellungen für Multisitebereitstellungen und Hochverfügbarkeit mit der StoreFront-Verwaltungskonsole konfigurieren. Sie können StoreFront auch per PowerShell oder durch Bearbeitung der StoreFront-Konfigurationsdateien konfigurieren, wodurch sich folgende zusätzliche Möglichkeiten bieten:

- Angeben mehrerer Gruppierungen von Bereitstellungen für die Aggregation.
  - 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.
- Angeben komplexer Prioritätsreihenfolgen für aggregierte Bereitstellungen. Die Verwaltungskonsole ermöglicht den Lastausgleich für aggregierte Bereitstellungen oder ein einzelne Failoverliste.
- Definieren von Bereitstellungen für die Notfallwiederherstellung (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.

1. Stellen Sie sicher, dass Sie den Store mit Details aller Citrix Virtual Apps and Desktops-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 Texteditor. 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.


```
<resourcesWingConfigurations>
<resourcesWingConfiguration name="Default" wingName="Default" />
</resourcesWingConfigurations>
```

4. Geben Sie Ihre Konfiguration wie unten gezeigt an.

```
<resourcesWingConfigurations>
<resourcesWingConfiguration name="Default" wingName="Default">
<userFarmMappings>
<clear />
<userFarmMapping name="user_mapping">
<groups>
<group name="domain\usergroup" sid="securityidentifier" />
<group ... />
...
</groups>
<equivalentFarmSets>
<equivalentFarmSet name="setname" loadBalanceMode="{
 LoadBalanced | Failover }
 "
aggregationGroup="aggregationgroupname">
<primaryFarmRefs>
<farm name="primaryfarmname" />
<farm ... />
...
</primaryFarmRefs>
<backupFarmRefs>
<farm name="backupfarmname" />
<farm ... />
...
</backupFarmRefs>
</equivalentFarmSet>
<equivalentFarmSet ... >
...
</equivalentFarmSet>
</equivalentFarmSets>
</userFarmMapping>
<userFarmMapping>
...
</userFarmMapping>
</userFarmMappings>
</resourcesWingConfiguration>
</resourcesWingConfigurations>
```

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 Zuweisen von Zugriff 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 in der Reihenfolge, in der diese 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 eine 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 Citrix Virtual Apps and Desktops-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 Citrix 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 Citrix 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 Abonnements von Stores in verschiedenen 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.

Für die Abonnementsynchronisierung müssen die konfigurierten Delivery Controller der synchronisierten Stores identische Namen haben. Beachten Sie bei den Namen der Delivery Controller die Groß- und Kleinschreibung beachtet wird. Wenn die Namen der Delivery Controller nicht identisch sind, haben Benutzer in den synchronisierten Stores möglicherweise unterschiedliche Abonnements. Wenn Sie Abonnements aus aggregierten Ressourcen synchronisieren, müssen auch die von beiden Stores verwendeten Name der Aggregationsgruppen übereinstimmen. Bei Namen von Delivery Controllern und Aggregationsgruppen wird zwischen Groß- und Kleinschreibung unterschieden. Beispiel: *XenDesktop7* wird von *Xendesktop7* unterschieden.

1. Verwenden Sie ein Konto mit lokalen Administratorberechtigungen, um Windows PowerShell ISE zu starten.
2. Führen Sie den folgenden Befehl aus, um die Synchronisierung zu einem bestimmten Zeitpunkt jeden Tag zu konfigurieren.

```
1 $RepeatMinutes = 30
2 Add-STFSubscriptionSynchronizationSchedule -StartTime (Get-Date -
     Format t) -RepeatMinutes $RepeatMinutes
```


Verwenden Sie **-StartTime**, um anzugeben, wann der Synchronisationszeitplan beginnt. Mit **(Get-Date -Format t)** beginnt der Synchronisationszeitplan sofort, bei die Angabe von *10:00* beginnt der Zeitplan zum angegebenen Zeitpunkt.

-RepeatMinutes legt die Häufigkeit fest, mit der die Synchronisierung ausgeführt wird. Beispielsweise führt *30* die Synchronisierung jede halbe Stunde aus und *180* alle 3 Stunden. Es wird empfohlen, Abrufzeitpläne zu staffeln, um zu vermeiden, dass zwei Servergruppen gleichzeitig Abonnementdaten voneinander abrufen. Beispielsweise würde ein Zeitplan zum Abrufen von Daten aus jeder Servergruppe alle 60 Minuten wie folgt konfiguriert. Servergruppe 1 ruft Daten aus Servergruppe 2 um 01:00, 02:00, 03:00 usw. ab. Servergruppe 2 ruft Daten aus Servergruppe 1 um 01:30, 02:30, 03:30 usw. ab.

3. Geben Sie den folgenden Befehl ein, um die Remoteimplementierung von StoreFront anzugeben, die den zu synchronisierenden Store enthält. Sie müssen dies für jedes Datencenter konfigurieren, in dem sich eine StoreFront-Servergruppe befindet, damit Abonnementdaten aus anderen Remotedatencentern abgerufen werden können. Siehe folgende Beispiele für Datencenter in den USA und Großbritannien:

   - Befehl für StoreFront-Server im US-Datencenter, um Daten von den britischen Servern abzurufen:

   ```
   $StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/
       Citrix/Store"
   Add-STFSubscriptionSynchronizationSource -FriendlyName "
       SyncFromUKStore" -StoreService $StoreObject -
       RemoteStoreFrontAddress "UKloadbalancedStoreFront.example.
       com"
   ```

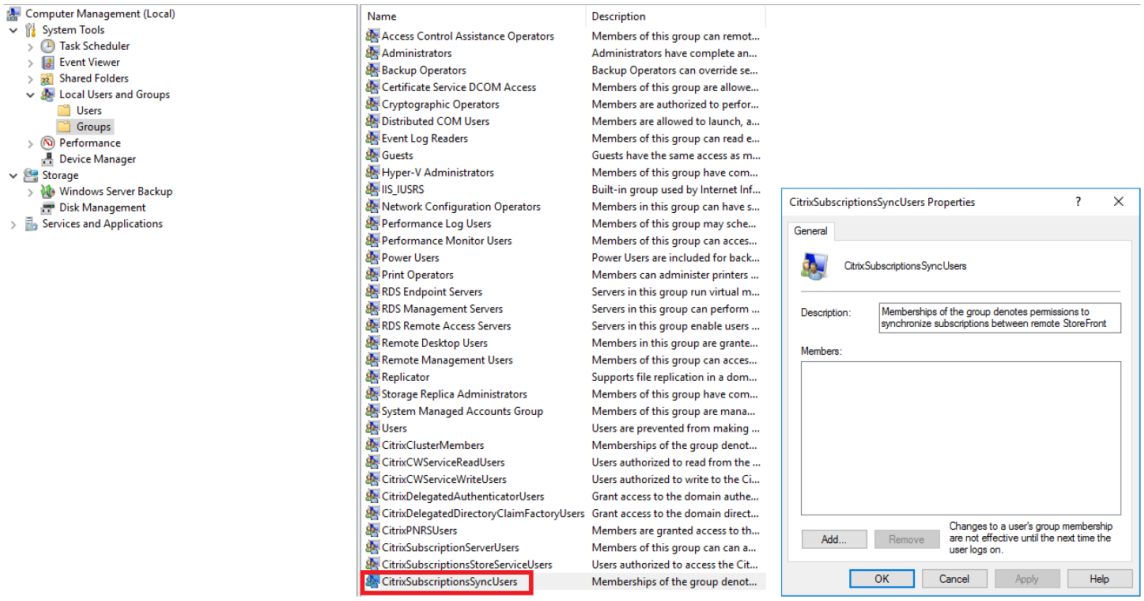
   - Befehl für StoreFront-Server im britischen Datencenter, um Daten von den US-Servern abzurufen:

   ```
   $StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/
       Citrix/Store"
   Add-STFSubscriptionSynchronizationSource -FriendlyName "
       SyncFromUSStore" -StoreService $StoreObject -
       RemoteStoreFrontAddress "USloadbalancedStoreFront.example.
       com"
   ```

   FriendlyName ist ein Name zum Identifizieren der Remotebereitstellung und *RemoteStoreFrontAddress* ist der FQDN des StoreFront-Servers oder der Lastausgleichsservergruppe für die Remotebereitstellung. Anwendungsabonnements zwischen zwei oder mehr Stores können nur synchronisiert werden, wenn die Namen aller Stores in den jeweiligen StoreFront-Bereitstellungen übereinstimmen.

4. Fügen Sie die Microsoft Active Directory-Domänencomputerkonten für jeden StoreFront-Server in der Remotebereitstellung der lokalen Windows-Benutzergruppe CitrixSubscriptionSyncUsers auf dem aktuellen Server hinzu.

   So können die aktuellen Server neue oder aktualisierte Abonnementdaten von den in CitrixSubscriptionSyncUsers aufgeführten Remoteservern abrufen, sobald Sie einen Synchronisierungszeitplan konfiguriert haben. Weitere Informationen zum Ändern lokaler Benutzergruppen finden Sie unter http://technet.microsoft.com/en-us/library/cc772524.aspx.



5. Wenn Sie den Zeitplan wie gewünscht konfiguriert haben, verwenden Sie die Citrix StoreFront-Verwaltungskonsole oder das PowerShell-Skript unten, um die Synchronisierungszeitpläne und -quellen auf alle anderen Server in der Gruppe zu verteilen.

```
1 Publish-STFServerGroupConfiguration
```

   Weitere Informationen über die Übertragung von Änderungen in einer StoreFront-Multiserverbereitstellung finden Sie unter Konfigurieren von Servergruppen.

6. Um einen vorhandenen Abonnementsynchronisierungszeitplan zu entfernen, führen Sie den folgenden Befehl aus und verteilen Sie dann die Konfigurationsänderungen auf die anderen StoreFront-Server in der Bereitstellung.

```
1 Clear-STFSubscriptionSynchronizationSchedule
```

7. Um eine spezifische Abonnementsynchronisierungsquelle zu entfernen, führen Sie den folgenden Befehl aus und verteilen Sie dann die Konfigurationsänderungen auf die anderen StoreFront-Server in der Bereitstellung.


```
Remove-STFSubscriptionSynchronizationSource -FriendlyName ”
    SyncFromUKStore”
```

8. Um alle Abonnementsynchronisierungsquellen zu entfernen, führen Sie den folgenden Befehl aus und verteilen Sie dann die Konfigurationsänderungen auf die anderen StoreFront-Server in der Bereitstellung.

```
Clear-STFSubscriptionSynchronizationSource
```

9. Führen Sie den folgenden Befehl aus, um die derzeit für Ihre StoreFront-Bereitstellung konfigurierten Abonnementsynchronisierungszeitpläne aufzulisten.

```
Get-STFSubscriptionSynchronizationSchedule
```

10. Führen Sie den folgenden Befehl aus, um die derzeit für Ihre StoreFront-Bereitstellung konfigurierten Abonnementsynchronisierungsquellen aufzulisten.

```
Get-STFSubscriptionSynchronizationSource
```

Konfigurieren des optimalen HDX-Routings für einen Store

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 Citrix Virtual Apps and Desktops-Controller und veröffentlichten Ressourcen können Sie nun Citrix Virtual Apps and Desktops-Bereitstellungen in Zonen aufteilen. Definieren Sie Zonen in Citrix Virtual Apps and Desktops-Studio. StoreFront wirkt mit Citrix Virtual Apps and Desktops zusammen. In StoreFront definierte Zonen müssen genau mit den in Citrix Virtual Apps and Desktops definierten Zonennamen übereinstimmen.

Mit 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 Citrix Virtual Apps and Desktops 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

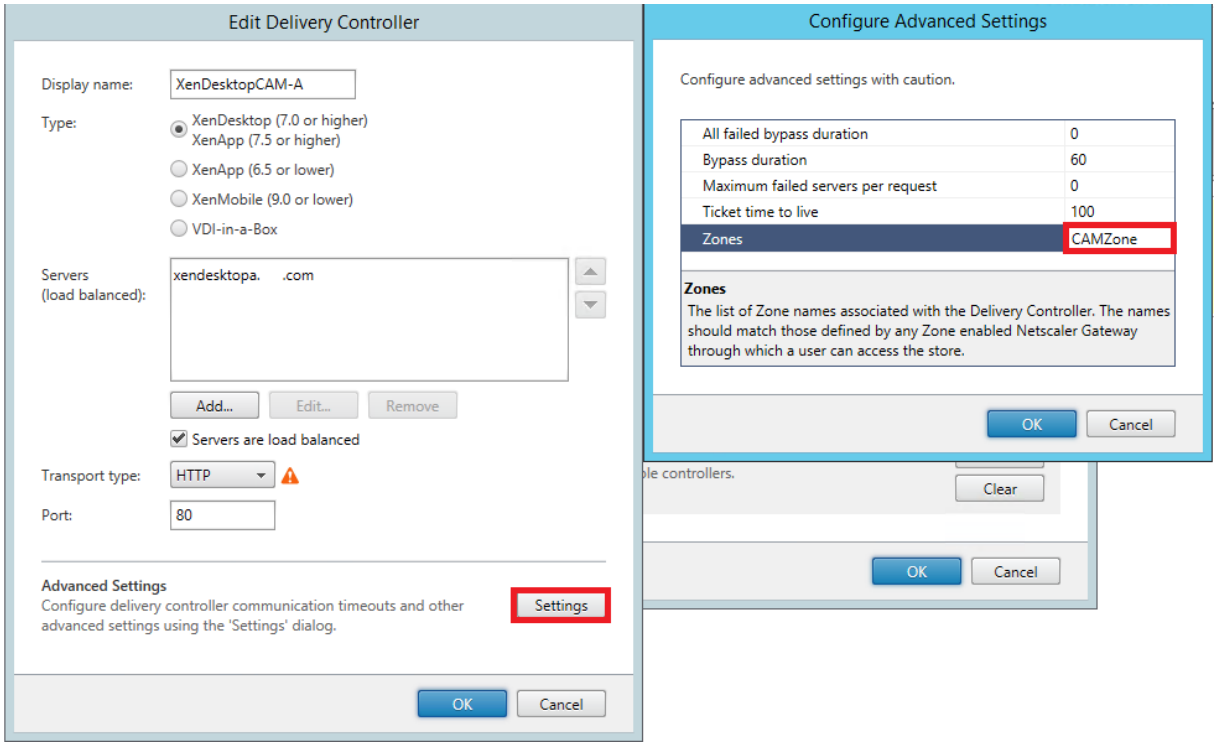
Standort. Es wird erwartet, dass jede Zone mindestens ein optimales Citrix Gateway hat, das für HDX-Verbindungen mit Ressourcen in der Zone verwendet wird.

Weitere Informationen über 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 dem Windows-Bildschirm **Start** oder "Apps" auf die Kachel **Citrix StoreFront**.
2. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores** und klicken Sie auf **Delivery Controller verwalten** im Bereich **Aktionen**.
3. Wählen Sie einen Controller aus, klicken Sie auf **Bearbeiten** und dann auf **Einstellungen** auf dem Bildschirm **Delivery Controller bearbeiten**.
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 Citrix Gateway-Routing zum Optimieren der Handhabung von ICA-Verbindungsrouting von der HDX Engine zu veröffentlichten Ressourcen, wie XenDesktop-VDAs oder mit Citrix Virtual Apps and Desktops veröffentlichte Anwendungen. In der Regel ist das optimale Gateway für eine Site am selben geografischen Standort.

Sie müssen optimale Citrix Gateway-Geräte für Bereitstellungen nur definieren, wenn das Gerät, über das die Benutzer auf StoreFront zugreifen, nicht das optimale Gateway ist. Wenn Starts über das Gate-

way, das die Startanforderung durchführt, zurückgeleitet werden sollen, macht StoreFront das automatisch.

Beispielszenario mit Farmen

1 x UK-Gateway –> 1 x UK-StoreFront

- UK-lokale Apps und Desktops
- US Apps und Desktops ausschließlich für UK-Failover

1 x US-Gateway–> 1 x US-StoreFront

- US-lokale Apps und Desktops
- UK Apps und Desktops ausschließlich für US-Failover

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

UK-StoreFront hat ein UK-basiertes und ein US-basiertes Citrix Gateway definiert und UK- und US-Controller in der Delivery Controller-Liste. UK-Benutzer greifen über den Gateway, StoreFront und die Farmen, die sich am selben Standort befinden, auf Remoteressourcen zu. Wenn kein Zugriff auf die UK-Ressourcen möglich ist, können sie als temporäre Failoverlösung auf US-Ressourcen zugreifen.

Ohne optimales Gatewayrouting würden alle ICA-Starts über das UK-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 einen optimalen Gateway pro Site zuordnen.

Beispielszenario mit Zonen

1 x CAMZone -> 2 x UK-StoreFronts

- Cambridge, UK: Apps und Desktops
- Fort Lauderdale, US-Osten: Apps und Desktops
- Bangalore, Indien: Apps und Desktops

1 x FTLZone -> 2 x USA-StoreFronts

- Fort Lauderdale, US-Osten: 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, US-Osten: Apps und Desktops

Abbildung 1. Suboptimales Gatewayrouting

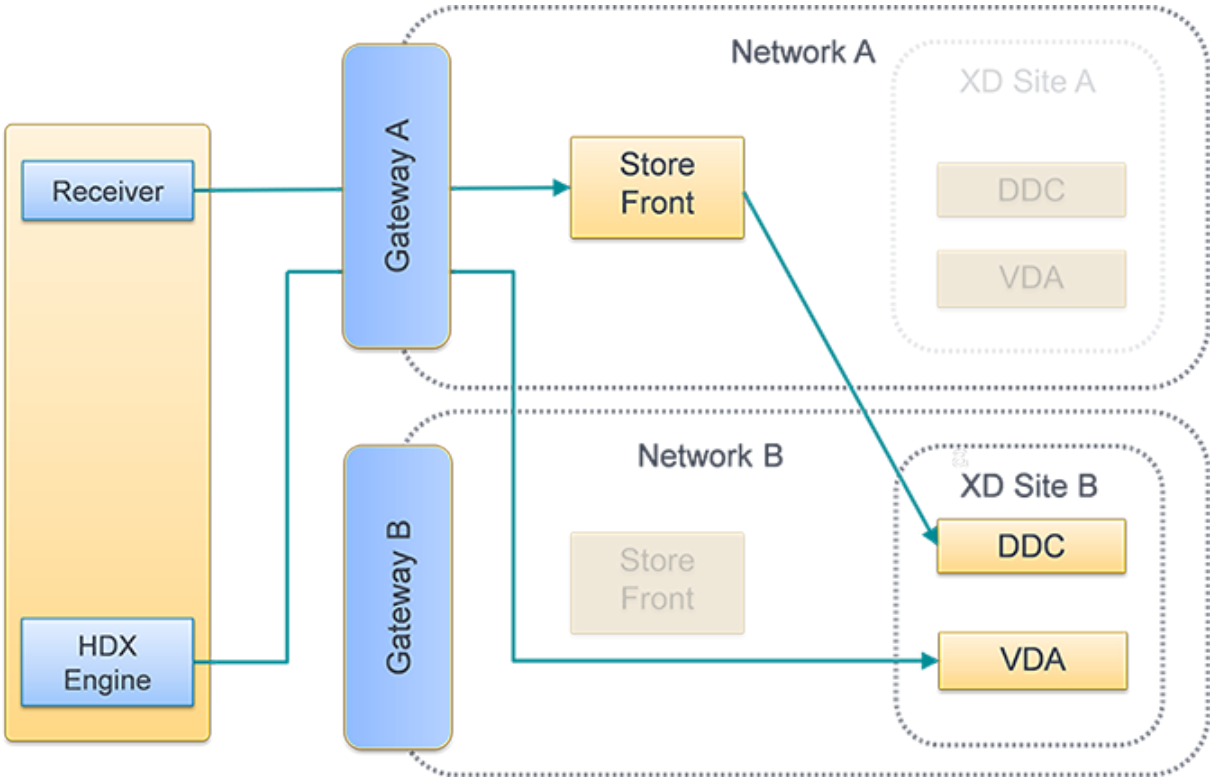
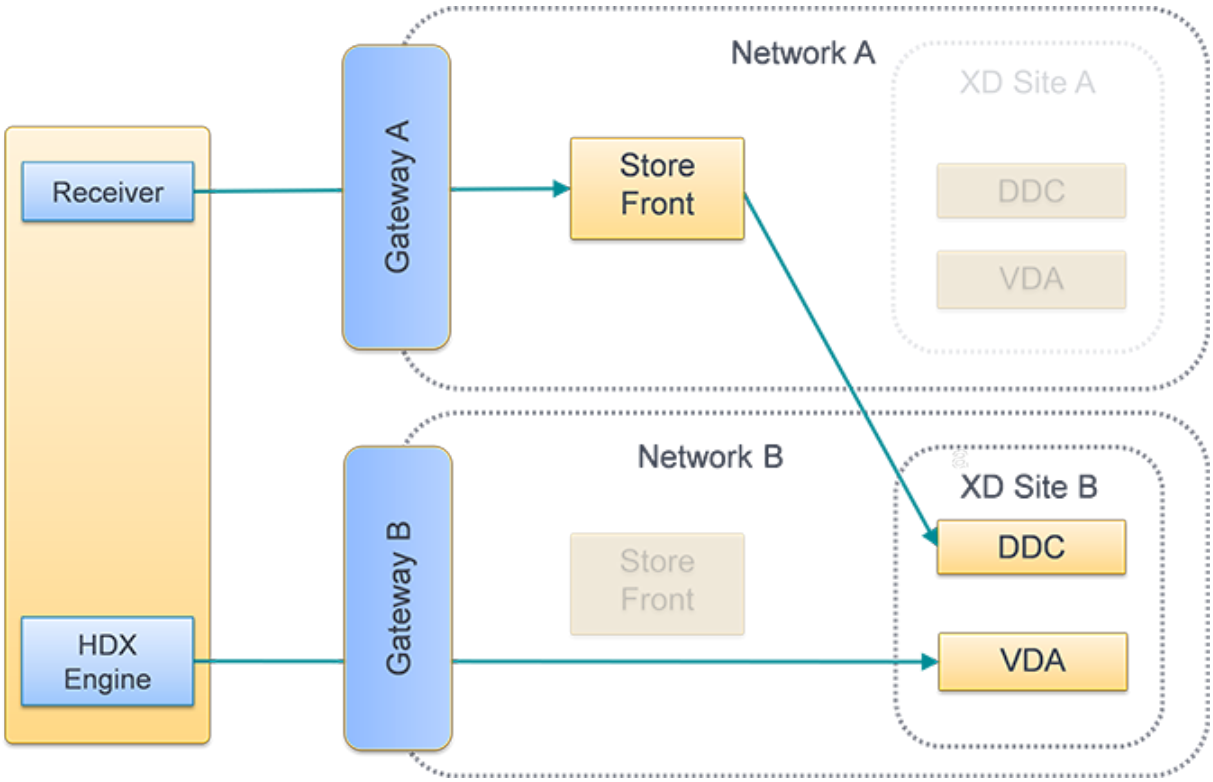


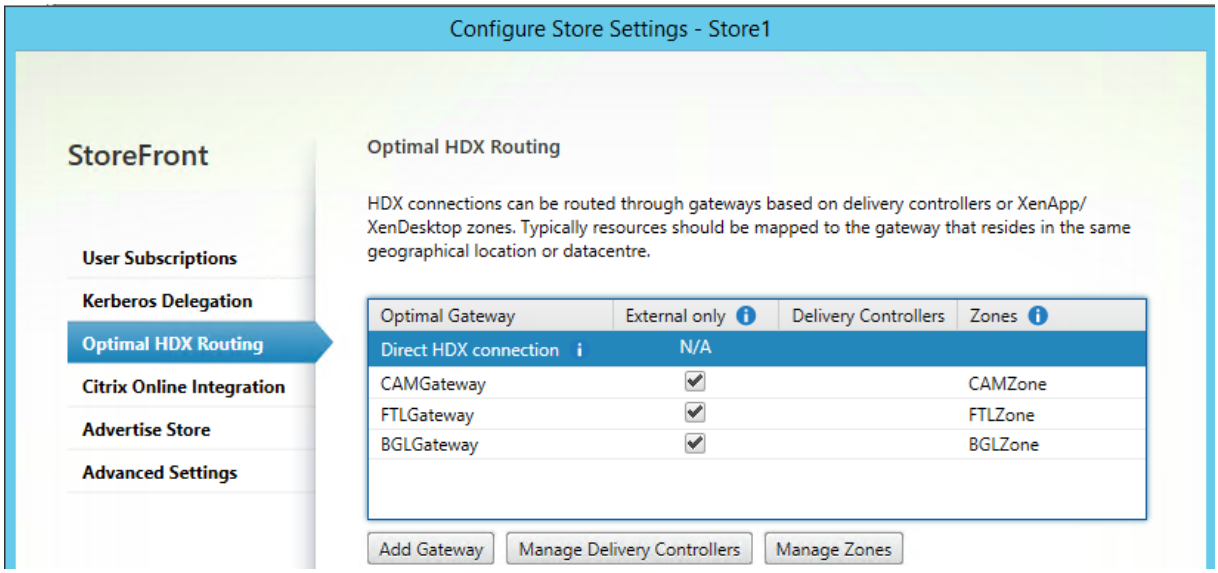
Abbildung 2. Optimales Gatewayrouting



Verwenden der Citrix StoreFront-Verwaltungskonsole

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

1. Navigieren Sie auf der Windows-**Startseite** oder auf der **Apps**-Seite zur 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. Wählen Sie auf der Seite **Einstellungen** > **Optimales HDX-Routing** ein Gateway aus.
4. Wenn Sie das Kontrollkästchen **Nur externe** wählen, entspricht das **-enabledOnDirectAccess = false** und “Direkte HDX-Verbindung” entspricht **Set-DSFarmsWithNullOptimalGateway** für Farmen oder Zonen.



Hinzufügen eines neuen Gateways

Eine der Optionen im Verfahren oben ist **Neues Gateway**. Nachdem Sie **Gateway hinzufügen** wählen wird der Bildschirm zum Hinzufügen eines Citrix Gateways angezeigt.

1. Geben Sie im Bildschirm **Allgemeine Einstellungen** den Anzeigenamen, die Citrix Gateway-URL und Verwendung oder Rolle an, um für Benutzer, die über öffentliche Netzwerke eine Verbindung herstellen, den Zugriff auf Stores über Citrix Gateway zu konfigurieren. Remotezugriff über Citrix 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 Citrix Virtual Apps and Desktops-Servern gehostet und gibt Sitzungstickets als Reaktion auf Verbindungsanforderungen aus. Auf diesen Sitzungstickets basiert die Authentifizierung und Autorisierung für den Zugriff auf Citrix Virtual Apps and Desktops-Ressourcen.
3. Geben Sie auf dem Bildschirm **Authentifizierungseinstellungen** an, wie der Remotebenutzer die Anmeldeinformationen zur Authentifizierung angibt.

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

PowerShell-API-Parameter

-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 Gatewayzuordnung verwendet werden kann.

Beispiel: “/Citrix/Store”

-GatewayName (String) - Name zum Identifizieren von Citrix Gateway innerhalb von StoreFront.

Beispiel 1: ExternalGateway

Beispiel 2: InternalGateway

-Hostnames (String Array) - Vollqualifizierter Domänennamen (FQDN) und Port des optimalen Citrix Gateway-Geräts.

Beispiel 1 für den vServer-Standardport 443: `gateway.example.com`

Beispiel 2 für den nicht standardmäßigen vServer-Port 500: `gateway.example.com:500`

-Farms (String Array) - Gibt einen Satz (normalerweise am selben Standort) Citrix Virtual Apps and Desktops-Bereitstellungen an, die ein optimales Citrix Gateway-Gerät gemeinsam verwenden. Eine Farm kann einen oder mehrere Delivery Controller enthalten, die veröffentlichte Ressourcen bereitstellen.

Sie können eine Citrix Virtual Desktops-Site in StoreFront unter “Delivery Controller” als “XenDesktop” konfigurieren. Dies repräsentiert eine einzelne Farm. Sie kann mehrere Delivery Controller in ihrer Failoverliste enthalten.

Beispiel: “XenDesktop”

`XenDesktop-A.example.com`

`XenDesktop-B.example.com`

`XenDesktop-C.example.com`

-Zones (String Array) - 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) - URLs für Citrix Virtual Apps and Desktops-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) - Wenn **true** werden Sitzungstickets nach dem Zufallsprinzip aus allen STAs abgerufen, sodass alle Anforderungen gleichmäßig über alle STAs verteilt werden. Wenn **false** werden Benutzer 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) - Wenn **true** bleiben getrennte Sitzungen 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) - Wenn **true** werden Sitzungstickets von zwei verschiedenen STAs abgerufen, falls eine STA während der Sitzung ausfällt. Wenn **false** wird nur ein STA-Server verwendet.

-EnabledOnDirectAccess (Boolean) - Wenn **true** wird sichergestellt, 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. Wenn **false** werden die Verbindungen zu Ressourcen nicht durch das optimale, für die Farm festgelegte Gerät geleitet, es sei denn, Benutzer greifen auf StoreFront über Citrix Gateway zu.

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

> **Tipp:**
>
> 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"
Configure direct HDX connections for farms
```

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.

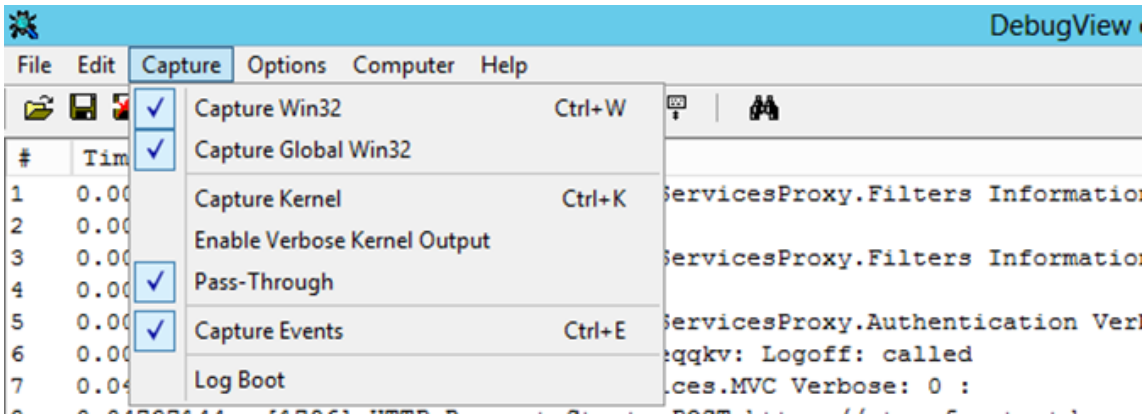
```
Get-DSFarmsWithNullOptimalGateway -SiteId 1 -ResourcesVirtualPath "/Citrix/
Internal"
```


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 ü
    ber das dedizierte optimale Gateway **Gateway2** für die Farm **
    Farm2** geleitet.
```



```
2
3       ‘Set-DSOptimalGatewayForFarms -onDirectAccess=false‘
4
5       Farm2 ist zum Verwenden des optimalen Gateways ”Gateway2”
            konfiguriert.
6
7       Für Farm2 ist das optimale Gateway bei direktem Zugriff deaktiviert
            .
8
9       Das optimale Gateway ”Gateway2” wird für den Start verwendet.
10
11  -   Ein interner Client meldet sich über StoreFront an. Der Start wird ü
        ber das dedizierte optimale Gateway ”Gateway1” für die Farm ”Farm1”
        geleitet.
12
13      ‘Set-DSOptimalGatewayForFarms -onDirectAccess=true‘
14
15      Kein dynamisch identifiziertes Gateway wird angefordert. StoreFront
            wurde direkt kontaktiert.
16
17      Farm1 ist zum Verwenden des optimalen Gateways Gateway1
            konfiguriert.
18
19      Für Farm1 ist das optimale Gateway bei direktem Zugriff aktiviert.
20
21      Das optimale Gateway ”Gateway1” wird für den Start verwendet.
22
23  -   Ein interner Client meldet sich über Gateway1 an. Die Starts von
        Ressourcen auf Farm1 können keinen Gateway passieren und StoreFront
        wird direkt kontaktiert.
24
25      ‘Set-DSFarmsWithNullOptimalGateway‘
26
27      Angefordertes dynamisch identifiziertes Gateway: Gateway1.
28
29      Farm1 ist nicht zum Verwenden eines Gateways konfiguriert. Zum
            Start wird kein Gateway verwendet.
```

Integration in Citrix Gateway und Citrix ADC

January 6, 2020

Durch Verwenden von Citrix Gateway mit StoreFront können Sie Benutzern außerhalb des Unternehmensnetzwerks einen sicheren Remotezugriff ermöglichen, während Citrix ADC für den Lastausgleich eingesetzt werden kann.

Planen des Einsatzes von Gateway- und Serverzertifikaten

Die Integration von Citrix Gateway und Citrix ADC 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 Citrix Virtual Apps and Desktops-Controller, die äquivalente Ressourcen bereitstellen
- Planen Sie eine durch Hardware geschützte Speicherung privater Schlüssel. Bei Gateways und Servern, einschließlich einigen Citrix ADC-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 gemein-

same Nutzung von Zertifikaten und ihren privaten Schlüssel vorgesehen (siehe Dokumentation der einzelnen Komponenten). Wenn Sie GSLB mit Citrix 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 Ende-zu-Ende-Verschlüsselung mit Citrix Virtual Apps and Desktops und dem Citrix Virtual Apps and Desktops-Abschnitt Sicherheit.

Konfigurieren der StoreFront-Anmeldung, wenn die Authentifizierung auf Citrix Gateway-VIP deaktiviert ist

Melden Sie sich bei StoreFront an, wenn die Authentifizierung auf Citrix Gateway-VIP deaktiviert ist. Dieses Verfahren funktioniert in zwei Szenarios:
Interne Netzwerke. App-Start von Remotestandorten schlägt fehl, da STAs nicht verwendet werden können, wenn die Authentifizierung für Citrix Gateway deaktiviert ist während der X-Citrix-Gateway-Header an StoreFront übergeben wird.
Citrix Receiver für Web. Receiver-Clients authentifizieren sich nicht, wenn die Authentifizierung am Citrix Gateway-VIP nicht aktiviert ist.

Änderungen auf dem StoreFront-Server

1. Deaktivieren Sie das Feld **Tokenkonsistenz erforderlich**:

   - StoreFront 3.0
     a) Bearbeiten Sie die Datei `web.config` für die Storewebsite. Beispielsweise ist für den StoreFront-Storenamen `NoAuth` der Pfad für die Datei `web.config` auf dem StoreFront-Server **inetpub\wwwroot\Citrix\NoAuth**.

   a) Suchen Sie die folgende Zeile in der Datei `web.config` und ändern Sie den Wert von “True” in “False”.
   Vorher
   `<resourcesGateways requireTokenConsistency=”true”>`
   nacher
   `<resourcesGateways requireTokenConsistency=”false”>`

   > **Hinweis:**
   >
   > In StoreFront 3.x ist **Tokenkonsistenz erforderlich** ein Kontrollkästchen in der GUI. Weitere Informationen finden Sie unter Erweiterte Storeeinstellungen.

   b) Speichern Sie die Datei `web.config` und starten Sie den IIS-Dienst neu.

2. Öffnen Sie die **Citrix StoreFront-Verwaltungskonsole**.
3. Klicken Sie auf **Receiver für Web-Sites verwalten**.
4. Wählen Sie die Citrix Receiver für Web-Site aus, klicken Sie auf **Konfigurieren** und wählen Sie dann **Authentifizierungsmethoden**.
5. Stellen Sie sicher, dass die Option **Passthrough-Authentifizierung von Citrix Gateway** deaktiviert ist.

> **Hinweis:**
>
> Es wird angenommen, dass Citrix Gateway und “Remotezugriff aktivieren” auf dem StoreFront-Server eingerichtet wurden.

Änderungen auf dem Citrix Gateway

1. Öffnen Sie dem virtuellen Citrix Gateway-Server.
2. Klicken Sie auf die Registerkarte **Authentifizierung**, und stellen Sie sicher, dass das Kontrollkästchen **Authentifizierung aktivieren** deaktiviert ist.
3. Binden Sie die entsprechende Sitzungsrichtlinie an den virtuellen Citrix Gateway-Server.
4. Testen Sie die Verbindung.

Hinzufügen einer Citrix Gateway-Verbindung

January 30, 2020

Verwenden Sie die Aufgabe “Citrix Gateway-Gerät hinzufügen”, um Citrix Gateway-Bereitstellungen hinzuzufügen, über die Benutzer auf Ihre Stores zugreifen können. Sie müssen die Passthrough-Authentifizierungsmethode von Citrix Gateway aktivieren, um Remotezugriff auf die Stores über Citrix Gateway konfigurieren zu können. Weitere Informationen zum Konfigurieren von Citrix Gateway für StoreFront finden Sie unter Integration in StoreFront über WebFront.

> **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. Navigieren Sie auf der Windows-Startseite oder auf der Apps-Seite zur Kachel Citrix StoreFront.
2. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores** und klicken Sie im Bereich "Aktionen" auf **Citrix Gateways verwalten**.
3. Klicken Sie auf **Hinzufügen** gefolgt von **Allgemeine Einstellungen** und geben Sie einen Anzeigenamen für die Citrix 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 Citrix Gateway-Bereitstellungen einfügen, damit Benutzer problemlos das beste Gateway für ihren Standort identifizieren können.
4. Geben Sie die URL des virtuellen Servers oder Benutzeranmeldepunkts (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 Citrix Gateway-Servers entsprechen. Das Verwenden desselben FQDN für StoreFront und den virtuellen Citrix 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 Citrix 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 Citrix Gateway für die Kommunikation mit Servern im internen Netzwerk das Benutzergerät darstellt. Dies kann auch die zugeordnete IP-Adresse des Citrix 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 Citrix Gateway hinzufügen, wählen Sie aus der Liste Anmeldetyp die Authentifizierungsmethode aus, die Sie auf dem Gerät für Benutzer der Citrix Workspace-App konfiguriert haben.

   Die von Ihnen angegebenen Informationen über die Konfiguration des Citrix Gateway-Geräts werden der Provisioningdatei für den Store hinzugefügt. Dadurch kann die Citrix Workspace-App die richtige Verbindungsanforderung senden, wenn ein 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 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 Citrix Gateway oder ein einzelnes Access Gateway 5.0-Gerät konfigurieren, geben Sie in das Feld “Callback-URL” die URL des Citrix 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 Citrix Gateway-Authentifizierungsdienst, um zu überprüfen, ob von Citrix 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 Citrix Virtual Apps and Desktops 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 Citrix Virtual Apps and Desktops-Servern gehostet und gibt Sitzungstickets als Reaktion auf Verbindungsanforderungen aus. Auf diesen Sitzungstickets basiert die Authentifizierung und Autorisierung für den Zugriff auf Citrix Virtual Apps and Desktops-Ressourcen.

12. Wenn Citrix Virtual Apps and Desktops getrennte Sitzungen aufrechterhalten soll, während die Citrix Workspace-App eine automatische Wiederverbindung versucht, wählen Sie das Kontrollkästchen "Sitzungszuverlässigkeit aktivieren". 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 Citrix 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 Citrix Gateway-Verbindungseinstellungen.

Für den Zugriff auf Stores über Citrix Gateway sind ein interner und mindestens zwei externe Beacons erforderlich. Die Citrix Workspace-App 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 Citrix Gateway-Bereitstellung werden standardmäßig als externe Beacons verwendet. Weitere Informationen zum Ändern von Beacons finden Sie unter Konfigurieren von Beacons.

Damit Benutzer auf Stores über Citrix Gateway zugreifen können, stellen Sie sicher, dass Sie den Remotebenutzerzugriff für diese Stores konfigurieren.

Importieren eines Citrix Gateways

April 1, 2020

Die Remotezugriffeinstellungen in der Citrix Gateway-Verwaltungskonsole müssen mit denen in StoreFront identisch sein. In diesem Artikel wird erläutert, wie Sie die Details eines virtuellen Citrix Gateway-Servers importieren, sodass Citrix Gateway 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 später erforderlich.

  > **Hinweis:**
  >
  > Citrix ADC-Geräte können nur virtuelle Gateway-Server exportieren, die mit dem Citrix Virtual Apps and Desktops-Assistenten erstellt wurden.

- Die Server-URLs aller STAs (Secure Ticket Authority) in der Datei GatewayConfig.json in der von dem Citrix ADC-Gerät generierten ZIP-Datei müssen von DNS aufgelöst und von StoreFront kontaktiert werden können.
- Die Datei GatewayConfig.json in der von dem Citrix ADC-Gerät generierten ZIP-Datei muss die URL einer Citrix Receiver für Web-Site auf dem StoreFront-Server enthalten. Ab Citrix ADC 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

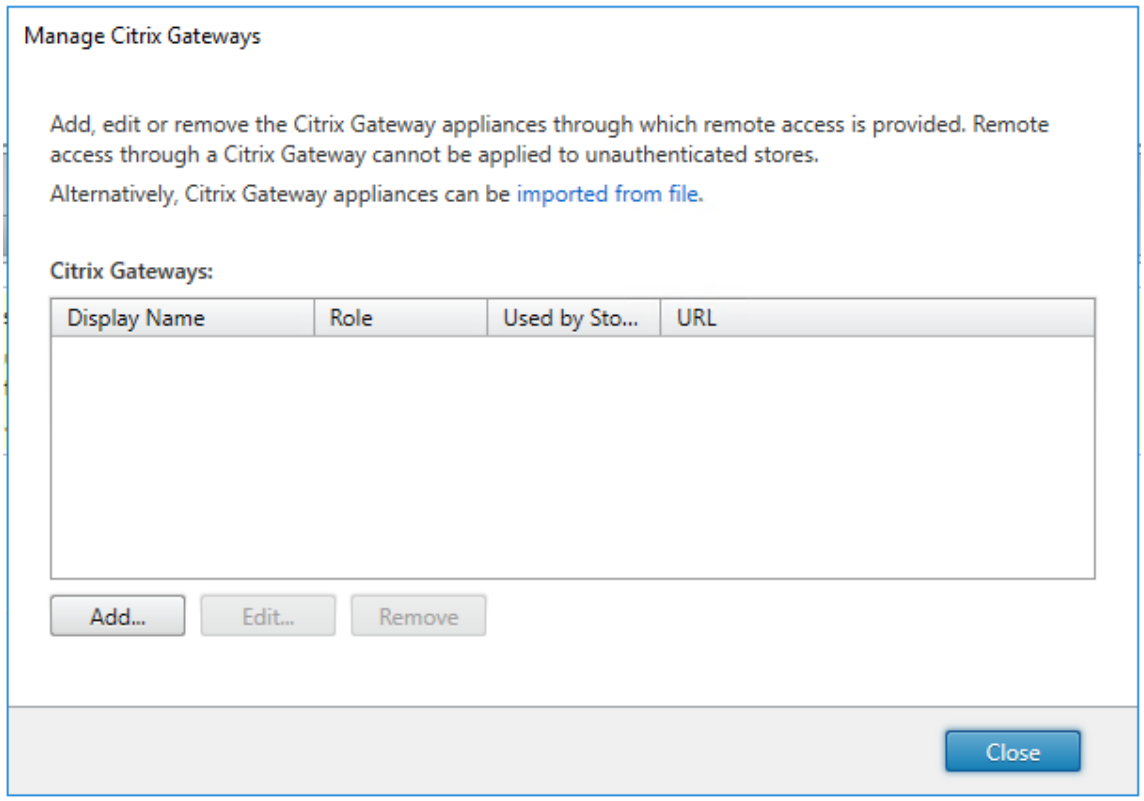
  Die Kombination aus URL und Port für den Rückruf darf sich von der für das Gateway unterscheiden, wenn Sie verschiedene externe und interne DNS-Namespaces in Ihrer Umgebung verwenden. Ist das Gateway in einer DMZ und hat eine <example.com>-URL und StoreFront ist im privaten Unternehmensnetzwerk und hat eine <example.local>-URL, können Sie eine <example.local>-Rückruf-URL verwenden, die auf den virtuellen Gateway-Server in der DMZ verweist.

Importieren eines Citrix Gateways mit der Konsole

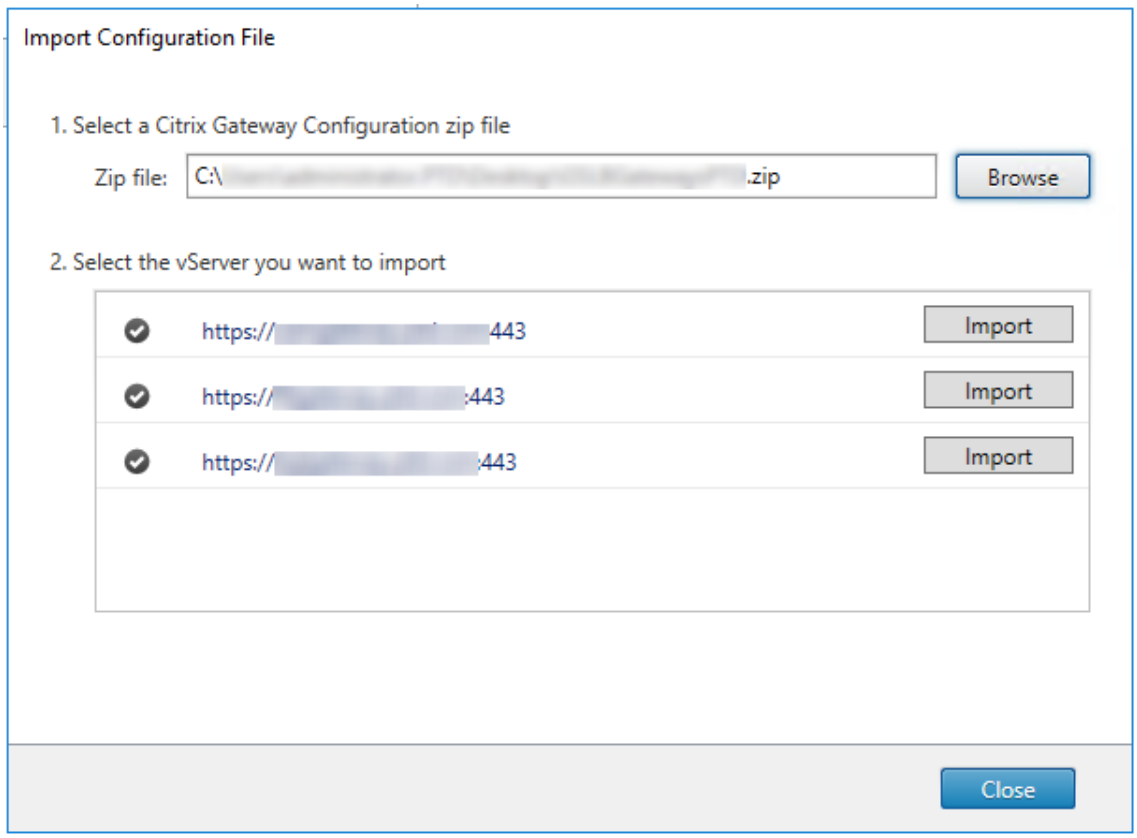
Sie können die Konfiguration eines oder mehrerer virtueller Citrix Gateway-Server mit derselben Importdatei importieren. Für mehrere virtuelle Gateway-Server von verschiedenen Citrix ADC-Geräten müssen Sie mehrere Importdateien verwenden.

> Wichtig:
>
> Manuelles Bearbeiten der Konfigurationsdatei, die aus Citrix Gateway exportiert wurde, wird nicht unterstützt.

1. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole **Stores** und klicken Sie im Bereich **Aktionen** auf **Citrix Gateways verwalten**.
2. Klicken Sie auf dem Bildschirm **Citrix Gateways verwalten** auf den Importiert-aus-Datei-Link.

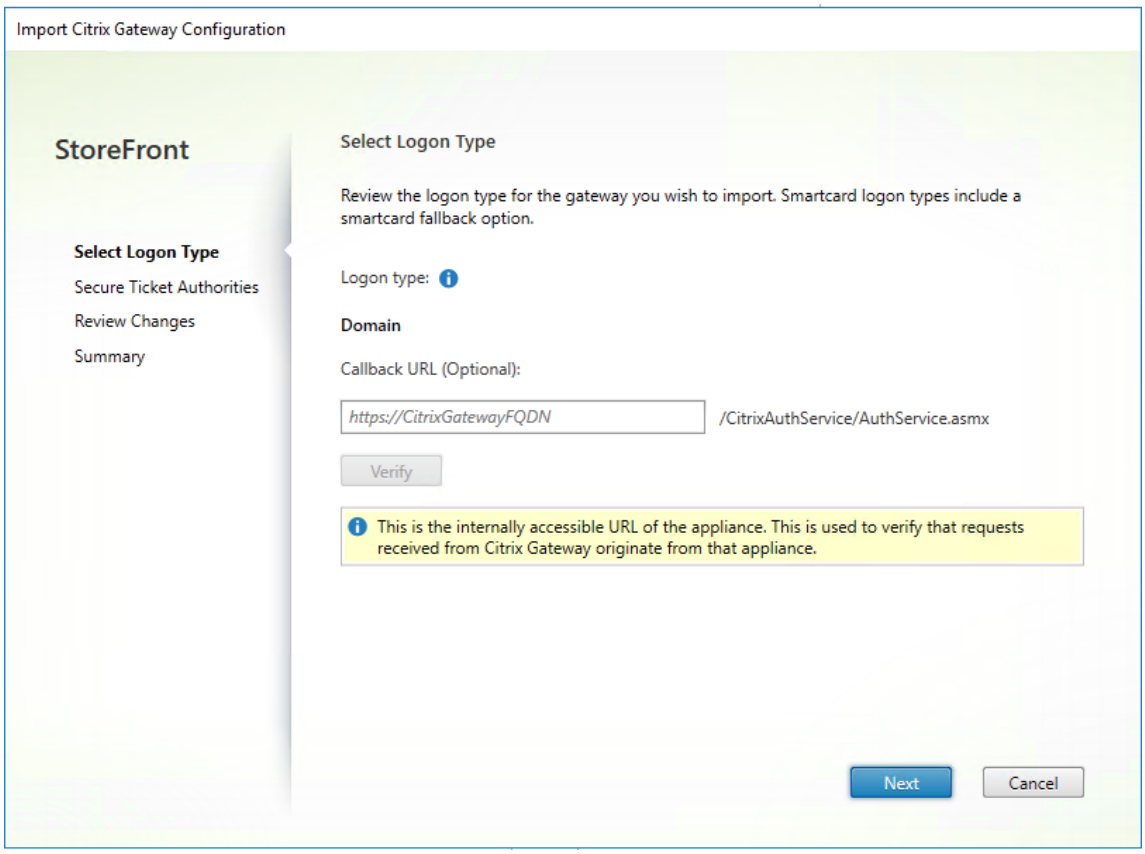


3. Navigieren Sie zu der Konfigurationsdatei des virtuellen Citrix Gateway-Servers.
4. Eine Liste der virtuellen Gateway-Server aus der ausgewählten ZIP-Datei wird angezeigt. Wählen Sie den gewünschten virtuellen Gateway-Server und klicken Sie auf **Importieren**. Wenn Sie den Import eines virtuellen Servers wiederholen, heißt die Schaltfläche “Update”. Mit **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 Citrix Gateway-Gerät für Benutzer der Citrix Workspace-App 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.



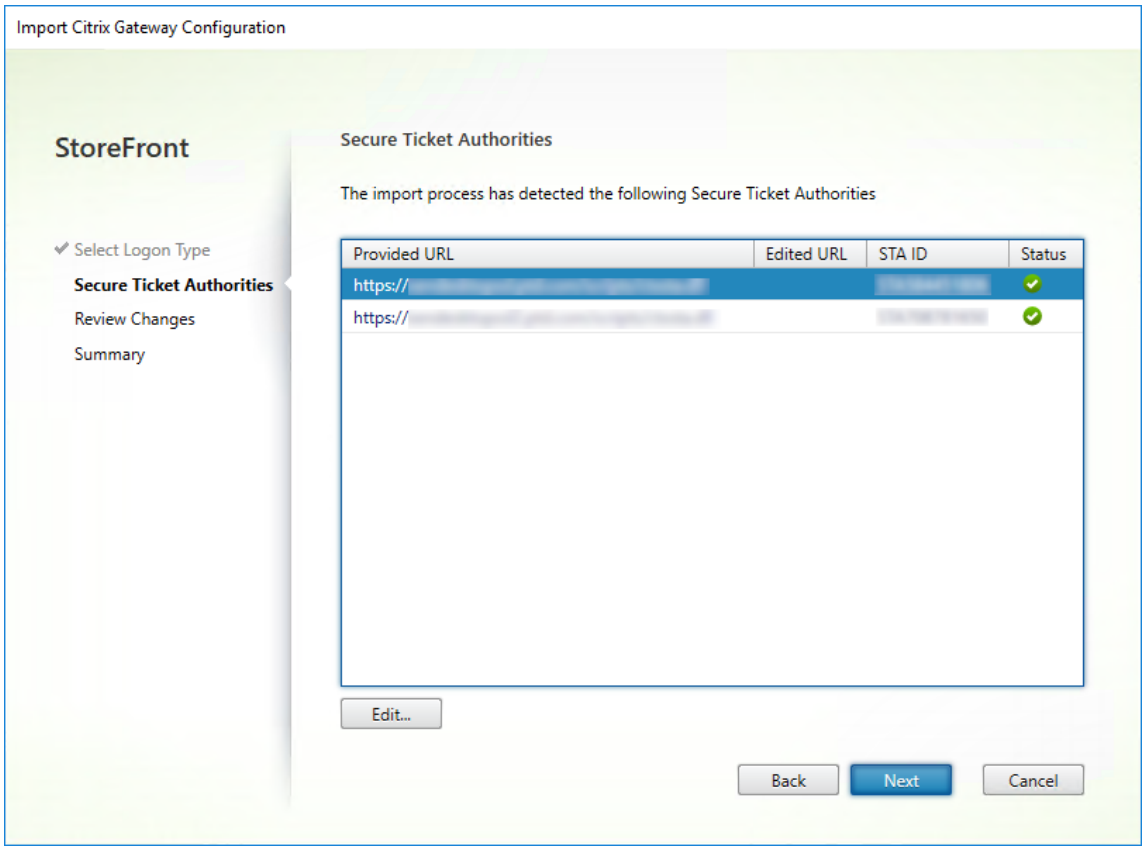
Anmeldeart in der Konsole	LogonType in der JSON-Datei	Rückruf-URL erforderlich
Domäne	Domäne	Nein
Domäne und Sicherheitstoken	DomainAndRSA	Nein
Sicherheitstoken	RSA	Ja
Smartcard - Kein Fallback	SmartCard	Ja
Smartcard - Domäne	SmartCardDomain	Ja
Smartcard - Domäne und Sicherheitstoken	SmartCardDomainAndRSA	Ja
Smartcard - Sicherheitstoken	SmartCardRSA	Ja
Smartcard - SMS-Authentifizierung	SmartCardSMS	Ja
SMS-Authentifizierung	SMS	Ja

Wenn eine Rückruf-URL erforderlich ist, wird sie von StoreFront automatisch basierend auf der

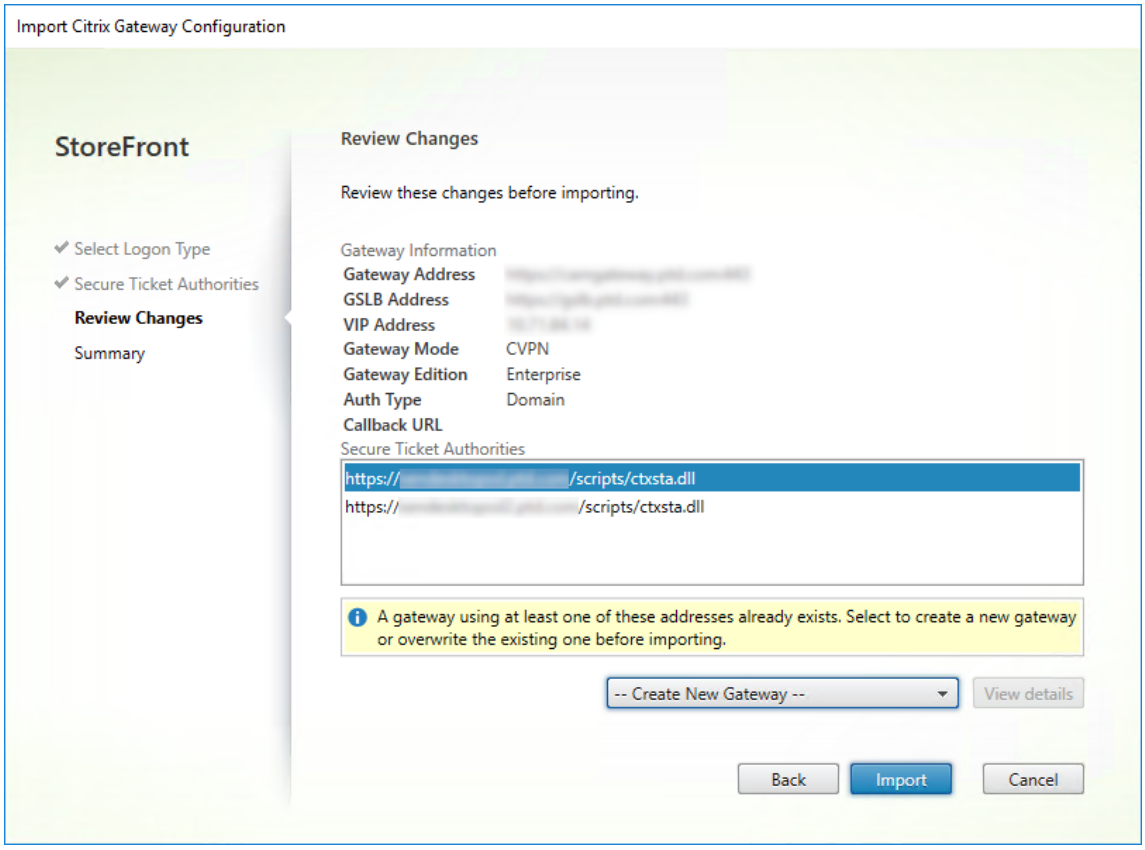
Gateway-URL in der ZIP-Datei eingetragen. Sie können sie in eine beliebige gültige URL ändern, die auf die korrekte virtuelle Citrix Gateway-IP-Adresse verweist. Bei GSLB-Gateways ist für jedes importierte Gateway eine eindeutige Rückruf-URL erforderlich.

Für die Verwendung von Smart Access 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 (GatewayURL: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 von StoreFront 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 **Fertig stellen**.

Zum Importieren einer weiteren Konfiguration eines virtuellen Servers wiederholen Sie die Schritte oben.

> **Hinweis:**
>
> Das Standardgateway eines Stores ist das Gateway, über das die Citrix Workspace-App eine Verbindung herstellt, es sei denn, sie ist 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 Citrix Workspace-App. Durch den Import nachfolgender Gateways ändert sich nichts an dem für den Store festgelegten Standardgateway.

Importieren mehrerer Citrix Gateways mit PowerShell

Read-STFNetScalerConfiguration

- Kopieren Sie die ZIP-Datei auf den Desktop des aktuell angemeldeten StoreFront-Administrators.
- Lesen Sie den Inhalt der ZIP-Datei mit der Konfiguration des virtuellen Citrix Gateway-Servers in den Speicher ein und suchen Sie die drei Gateways anhand ihrer Indexwerte.

```
$ImportedGateways = Read-STFNetScalerConfiguration -path "$env:
    USERPROFILE\desktop\GatewayConfig.zip"
```

Zeigen Sie die drei Gateway-Objekte aus dem Netscaler-ZIP-Importpaket mit dem Cmdlet **STFNetScalerConfiguration** im Speicher an.

```
$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 }
```



```
14
15  StaLoadBalance         : True
16  CertificateThumbprints : {
17  F549AFAA29EBF61E8709F2316B3981AD503AF387 }
18
19  GatewayAuthType        : Domain
20  GatewayEdition         : Enterprise
21  ReceiverForWebSites    : {
22  Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.
       ReceiverForWebSite }
23
24
25  GatewayMode            : CVPN
26  CallbackUrl            :
27  GslbAddressUri         : https://gslb.example.com/
28  AddressUri             : https://emeagateway.example.com/
29  Address                : https://emeagateway.example.com:444
30  GslbAddress            : https://gslb.example.com:443
31  VipAddress             : 10.0.0.2
32  Stas                   : {
33  STA298854503, STA909374257 }
34
35  StaLoadBalance         : True
36  CertificateThumbprints : {
37  F549AFAA29EBF61E8709F2316B3981AD503AF387 }
38
39  GatewayAuthType        : DomainAndRSA
40  GatewayEdition         : Enterprise
41  ReceiverForWebSites    : {
42  Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.
       ReceiverForWebSite }
43
44
45  GatewayMode            : CVPN
46  CallbackUrl            : https://emeagateway.example.com:445
47  GslbAddressUri         : https://gslb.example.com/
48  AddressUri             : https://emeagateway.example.com/
49  Address                : https://emeagateway.example.com:445
50  GslbAddress            : https://gslb.example.com:443
51  VipAddress             : 10.0.0.2
52  Stas                   : {
53  STA298854503, STA909374257 }
54
55  StaLoadBalance         : True
56  CertificateThumbprints : {
```



```
57  F549AFAA29EBF61E8709F2316B3981AD503AF387 }
58
59  GatewayAuthType         :SmartCard
60  GatewayEdition          : Enterprise
61  ReceiverForWebSites     : {
62  Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.
        ReceiverForWebSite }
```

Import-STFNetScalerConfiguration ohne eine CallbackURL

Kopieren Sie die ZIP-Datei auf den Desktop des aktuell angemeldeten StoreFront-Administrators. Lesen Sie das ZIP-Importpaket mit der Citrix Gateway-Konfiguration in den Speicher ein und suchen Sie die drei Gateways anhand ihrer Indexwerte.

```
1 $ImportedGateways = Read-STFNetScalerConfiguration -path "$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 GUI zum Zulassen jedes einzelnen zu importierenden Gateways aufgefordert werden. Entfernen Sie den Parameter, wenn Sie Gateways sorgfältig einzeln importieren möchten.

```
1 ```
2 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
      GatewayIndex 0 -Confirm:$False
3 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
      GatewayIndex 1 -Confirm:$False
4 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
      GatewayIndex 2 -Confirm:$False
5 ```
```

Import-STFNetScalerConfiguration mit einer eigenen CallbackURL

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.

```
1 $ImportedGateways = Read-STFNetScalerConfiguration -path "$env:
      USERPROFILE\desktop\GatewayConfig.zip"
2
```



```
3 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 0 -CallbackUrl "https://emeagatewaycb.example.com:443 -
    Confirm:$False
4
5 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 1 -CallbackUrl "https://emeagatewaycb.example.com:444 -
    Confirm:$False
6
7 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 2 -CallbackUrl "https://emeagatewaycb.example.com:445 -
    Confirm:$False
```

Import-STFNetScalerConfiguration überschreibt die Authentifizierungsmethode, die in der Importdatei gespeichert ist, und lässt Sie ein eine eigene CallbackURL angeben

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.

```
1 $ImportedGateways = Read-STFNetScalerConfiguration -path "$env:
    USERPROFILE\desktop\GatewayConfig.zip"
2
3 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 0 -LogonType "SmartCard" -CallbackUrl "https://
    emeagatewaycb.example.com:443" -Confirm:$False
4
5 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 1 -LogonType "SmartCard" -CallbackUrl "https://
    emeagatewaycb.example.com:444" -Confirm:$False
6
7 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 2 -LogonType "SmartCard" -CallbackUrl "https://
    emeagatewaycb.example.com:445" -Confirm:$False
```

Konfigurieren von Citrix Gateway-Verbindungseinstellungen

January 30, 2020

Anhand der folgenden Anleitungen können Sie die Details von Citrix Gateway-Bereitstellungen aktualisieren, über die die Benutzer auf Stores zugreifen. Weitere Informationen zum Konfigurieren von Citrix Gateway für StoreFront finden Sie unter Integration in StoreFront über WebFront.

Wenn Sie ihre Citrix Gateway-Bereitstellungen ändern, müssen die Benutzer, die durch diese Bereitstellungen auf Stores zugreifen, die Citrix Workspace-App mit den geänderten Verbindungsinformationen aktualisieren. Bei der Konfiguration einer Citrix Receiver für Web-Site für einen Store können die Benutzer eine aktualisierte Citrix Workspace-App-Provisioningdatei von der Site beziehen. Andernfalls können Sie eine Provisioningdatei 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 Citrix Gateway-Einstellungen

Mit "Allgemeine Einstellungen ändern" bearbeiten Sie die Namen der Citrix Gateway-Bereitstellungen, die den Benutzern angezeigt werden, und aktualisieren die StoreFront-Konfiguration, wenn sich die URL des virtuellen Servers oder des Anmeldepunkts und der Bereitstellungsmodus der Citrix Gateway-Infrastruktur ändert.

1. Navigieren Sie auf der Windows-Startseite oder auf der Apps-Seite zur Kachel Citrix StoreFront.
2. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten "Stores" und klicken Sie auf "Citrix Gateways verwalten".
3. Geben Sie einen Namen für die Citrix Gateway-Bereitstellung an, über den die Benutzer sie erkennen können.

   Den Benutzern wird der Anzeigename angezeigt, den Sie in der Citrix Workspace-App angegeben haben. Nehmen Sie deshalb relevante Informationen in den Namen auf, damit die Benutzer leichter entscheiden können, ob sie die Bereitstellung verwenden möchten. Beispielsweise können Sie den geographischen Standort in die Anzeigenamen der Citrix Gateway-Bereitstellungen einfügen, damit Benutzer problemlos das beste Gateway für ihren Standort identifizieren können.
4. Geben Sie die URL des virtuellen Servers oder Benutzeranmeldepunkts (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 Citrix Gateway-Servers entsprechen. Das Verwenden desselben FQDN für StoreFront und den virtuellen Citrix Gateway-Server wird nicht unterstützt.

5. Wenn Ihre Bereitstellung Access Gateway 5.0 verwendet, fahren Sie mit Schritt 7 fort. Andernfalls und geben Sie ggf. die Subnetz-IP-Adresse des Citrix Gateway-Geräts an.

   Die Subnetzadresse ist die IP-Adresse, durch die Citrix Gateway für die Kommunikation mit Servern im internen Netzwerk das Benutzergerät darstellt. Dies kann auch die zugeordnete IP-Adresse des Citrix Gateway-Geräts sein. Wenn angegeben, verwendet StoreFront die Subnetz-IP-Adresse, um zu überprüfen, ob eingehende Anfragen von einem vertrauenswürdigen Gerät stammen.

6. Wenn auf Ihrem Gerät Citrix Gateway ausgeführt wird, wählen Sie aus der Liste "Anmeldetyp" die Authentifizierungsmethode aus, die Sie auf dem Gerät für Benutzer der Citrix Workspace-App konfiguriert haben.

   Die von Ihnen angegebenen Informationen über die Konfiguration des Citrix Gateway-Geräts werden der Provisioningdatei für den Store hinzugefügt. Dadurch kann die Citrix Workspace-App die richtige Verbindungsanforderung senden, wenn ein 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 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 Citrix Gateway oder ein einzelnes Access Gateway 5.0-Gerät umfasst, geben Sie die URL für den Citrix 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 Citrix Gateway-Authentifizierungsdienst, um zu überprüfen, ob von Citrix 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 Citrix Virtual Apps and Desktops-Servern gehostet und gibt Sitzungstickets als Reaktion auf Verbindungsanforderungen aus. Auf diesen Sitzungstickets basiert die Authentifizierung und Autorisierung für den Zugriff auf Citrix Virtual Apps and Desktops-Ressourcen.

1. Navigieren Sie auf der Windows-Startseite oder auf der Apps-Seite zur Kachel Citrix StoreFront.
2. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten “Stores” und im Ergebnisbereich eine Citrix Gateway-Bereitstellung aus. Klicken Sie im Bereich “Aktionen” auf “Citrix 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. Wenn Citrix Virtual Apps and Desktops getrennte Sitzungen aufrechterhalten soll, während die Citrix Workspace-App eine automatische Wiederverbindung versucht, wählen Sie das Kontrollkästchen “Sitzungszuverlässigkeit aktivieren”. 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 Citrix Gateway-Bereitstellungen

Verwenden Sie im Bereich **Aktionen** die Aufgabe "Entfernen" für **Citrix Gateways verwalten**, um die Details einer Citrix Gateway-Bereitstellung aus StoreFront zu löschen. Nach dem Entfernen eines Citrix Gateway-Geräts können die Benutzer nicht mehr über diese Bereitstellung auf Stores zugreifen.

Lastausgleich mit Citrix ADC-Gerät

April 1, 2020

Dieser Artikel enthält Informationen zum Bereitstellen einer StoreFront-Servergruppe mit mindestens zwei StoreFront-Servern in einer aktiven Konfiguration mit Lastausgleich. Der Artikel enthält Angaben zum Konfigurieren eines Citrix ADC-Geräts für den Lastausgleich für von der Citrix Workspace-App bzw. Citrix Receiver für Web eingehende Anforderungen über alle StoreFront-Knoten in der Servergruppe hinweg. Außerdem wird erläutert, wie Sie StoreFront Monitor zur Verwendung mit einem Citrix ADC-Gerät konfigurieren.

Die Beispiele in diesem Abschnitt wurden in der folgenden Umgebung getestet:

- Vier Windows Server 2012 R2 StoreFront 3.x-Knoten in einer einzelnen Servergruppe
- Ein für Least-Connection-Lastausgleich und Cookie-Persistenz konfiguriertes Citrix ADC-Gerät der Version 12.1.
- Ein Windows 10-Testclient mit installierter Citrix Workspace-App.

Zertifikatanforderungen für den Lastausgleich bei Verwendung von HTTPS

Siehe Planen des Einsatzes von Gateway- und Serverzertifikaten.

Ziehen Sie die folgenden Optionen in Betracht, bevor Sie ein Zertifikat von einer kommerziellen Zertifizierungsstelle erwerben oder von der Zertifizierungsstelle Ihres Unternehmens ausstellen lassen.

- **Option 1:** Verwenden Sie ein Platzhalterzertifikat **.example.com* auf dem Citrix ADC virtuellen Lastausgleichsserver und den Knoten der StoreFront-Servergruppe. Dies vereinfacht die Kon-

figuration und ermöglicht das künftige Hinzufügen weiterer StoreFront-Server, ohne dass das Zertifikat ersetzt werden muss.

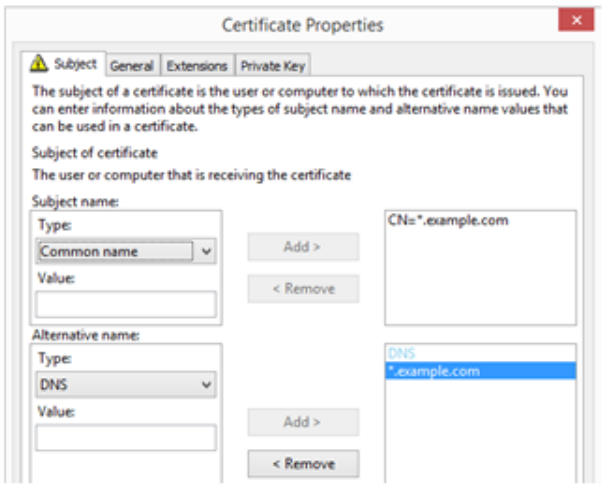
- **Option 2**: Verwenden Sie ein Zertifikat mit alternativem Antragstellernamen (SANs) auf dem virtuellen Citrix ADC-Lastausgleichsserver und den Knoten der StoreFront-Servergruppe. Zusätzliche SANs in dem Zertifikat, die allen vollqualifizierten Domänennamen der StoreFront-Server entsprechen, sind 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/.

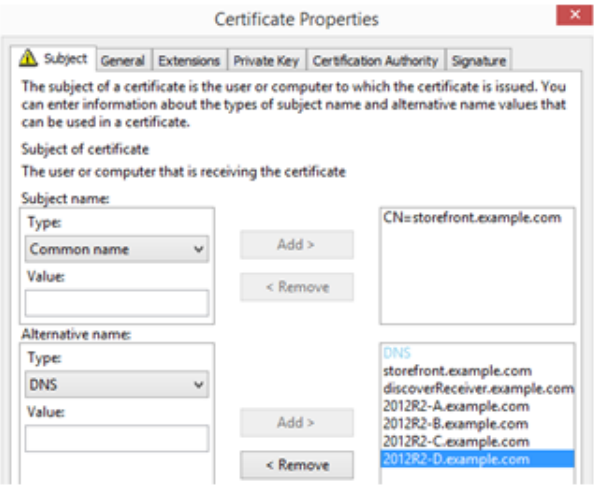
> **Hinweis:**
>
> Wenn der private Schlüssel des Zertifikats nicht exportiert werden kann. Verwenden Sie zwei Zertifikate, eines auf dem virtuellen Citrix ADC-Lastausgleichsserver und eines auf den Knoten der StoreFront-Servergruppe. Beide Zertifikate müssen alternative Antragstellernamen enthalten.

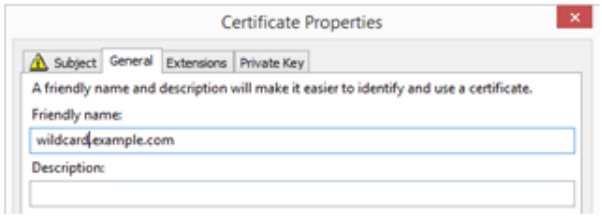
Example Web server certificates

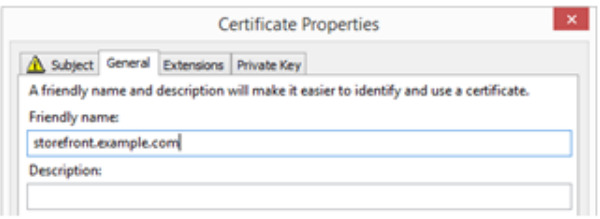
Option 1: Wildcard certificate



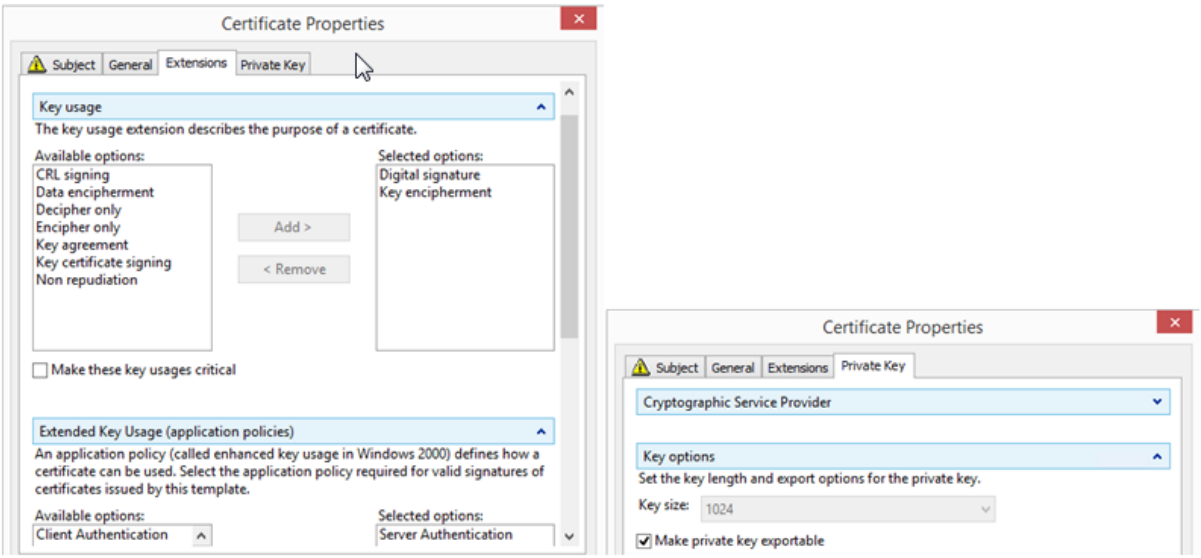
Option 2: SAN certificate with every StoreFront server







Common Properties



Erstellen eines SSL-Zertifikats für den Citrix ADC-Load Balancer und alle StoreFront-Server

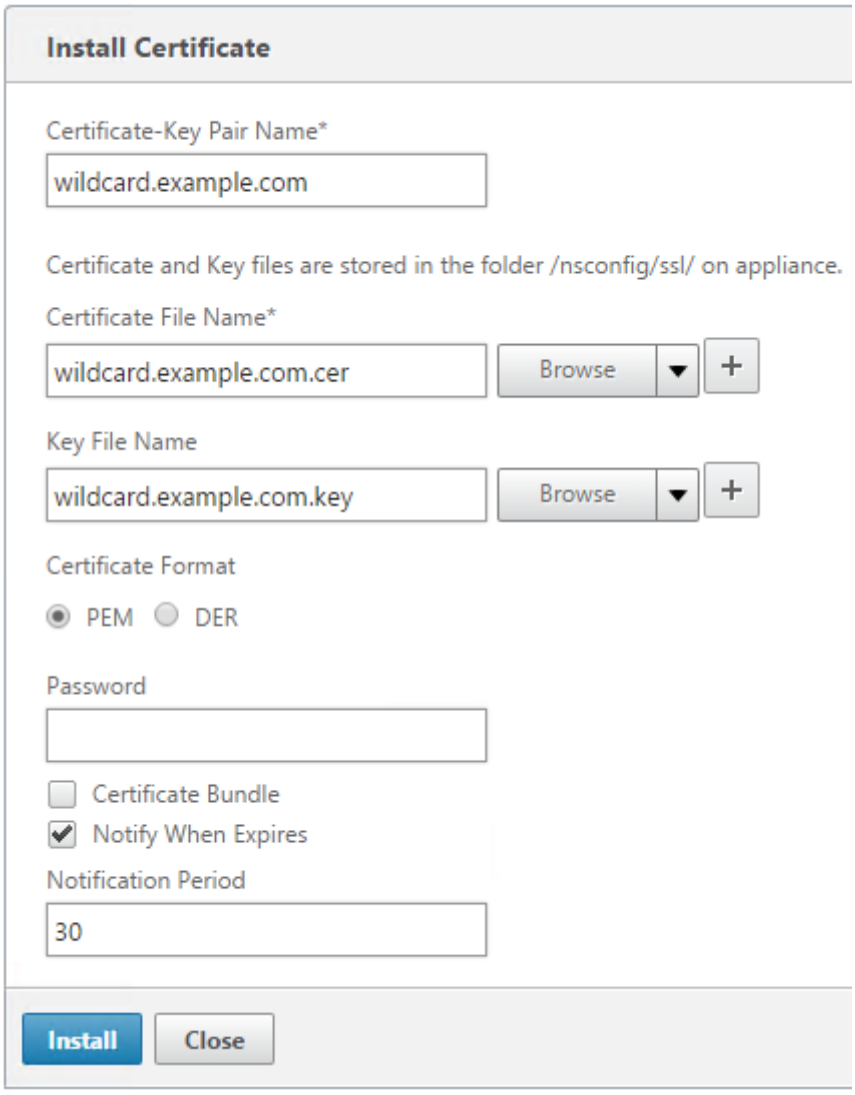
Importieren eines Zertifikats einer Windows-Zertifizierungsstelle in ein Citrix ADC-Gerät

- WinSCP ist ein nützliches Drittanbietertool zum Verschieben von Dateien von einer Windows-Maschine in das Dateisystem eines Citrix ADC-Geräts. Kopieren Sie Zertifikate für den Import in den Ordner */nsconfig/ssl/* im Dateisystem des Citrix ADC-Geräts.
- Sie können auch OpenSSL-Tools auf dem Citrix ADC-Gerät verwenden, um das Zertifikat und den Schlüssel aus einer *PKCS12/PFX*-Datei zu extrahieren, um zwei separate CER- und KEY X.509-Dateien im PEM-Format zu erstellen, die Citrix ADC verwenden kann.

1. Kopieren Sie die PFX-Datei in den Ordner */nsconfig/ssl* auf dem Citrix ADC-Gerät oder VPX.
2. Öffnen Sie die Befehlszeilenschnittstelle (CLI) des Citrix ADC-Geräts.
3. Geben Sie **Shell** ein, um die Befehlszeilenschnittstelle des Citrix ADC-Geräts zu beenden und zur FreeBSD-Shell zu wechseln.
4. Wechseln Sie das Verzeichnis mit `cd /nsconfig/ssl/`.
5. Führen Sie `openssl pkcs12 -in <imported cert file>.pfx -nokeys -out <certfilename>.cer` aus und geben Sie auf Aufforderung das PFX-Kennwort ein.
6. Führen Sie `openssl pkcs12 -in <imported cert file>.pfx -nocerts -out <keyfilename>.key` aus und geben Sie auf Aufforderung das PFX-Kennwort ein und legen Sie eine 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 erfolgreich in `/nsconfig/ssl/` erstellt wurden.
8. Geben Sie **Exit** ein, um zur CLI des Citrix ADC-Geräts zurückzukehren.

Konfigurieren des Serverzertifikats auf dem Citrix ADC-Gerät nach dem Import

1. Melden Sie sich bei der Verwaltungs-GUI des Citrix ADC-Geräts 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 Dateisystem des Citrix ADC-Geräts 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 Citrix ADC-Load Balancers.

Beispiel: `storefront.example.com` wird in die virtuelle IP (VIP) des virtuellen Lastausgleichservers aufgelöst.

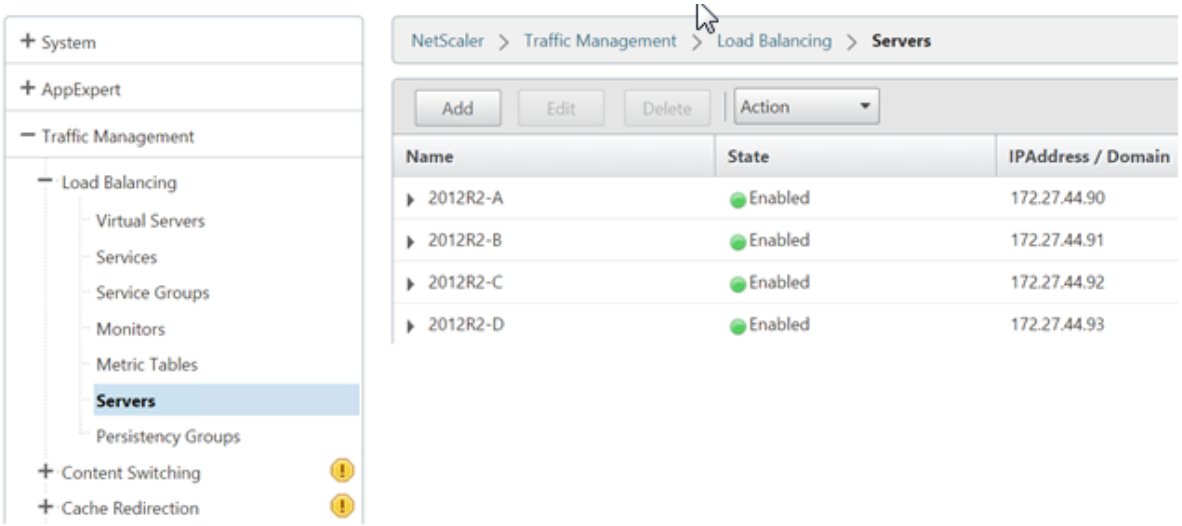
Szenario 1: Eine durchgängige sichere HTTPS 443-Verbindung zwischen Client und Citrix ADC-Load Balancer und zwischen Load Balancer und mehreren StoreFront 3.x-Servern

Bei diesem Szenario wird ein modifizierter StoreFront-Monitor unter Einsatz von Port 443 verwendet.

Hinzufügen einzelner StoreFront-Serverknoten zum Citrix ADC-Load Balancer

1. Melden Sie sich bei der Verwaltungs-GUI des Citrix ADC-Geräts an.
2. Wählen Sie **Traffic Management > Load Balancing > Servers > Add** und fügen Sie die vier StoreFront-Knoten für den Lastausgleich hinzu.

   Beispiel = 4 x 2012R2 StoreFront-Knoten names 2012R2-A bis -D
3. Verwenden Sie die IP-basierte Serverkonfiguration und geben Sie die Server-IP-Adresse für jeden StoreFront-Knoten ein.

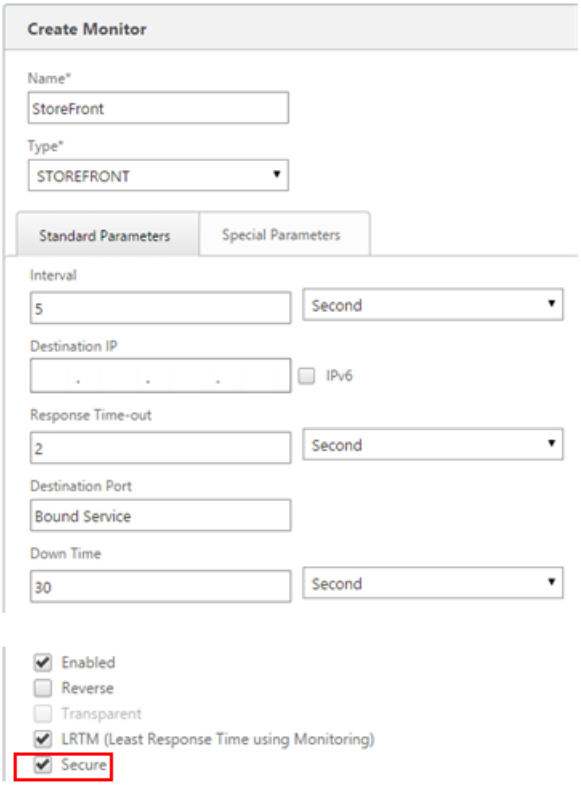


Definieren eines StoreFront-Monitors zur Prüfung des Status aller StoreFront-Knoten in der Servergruppe

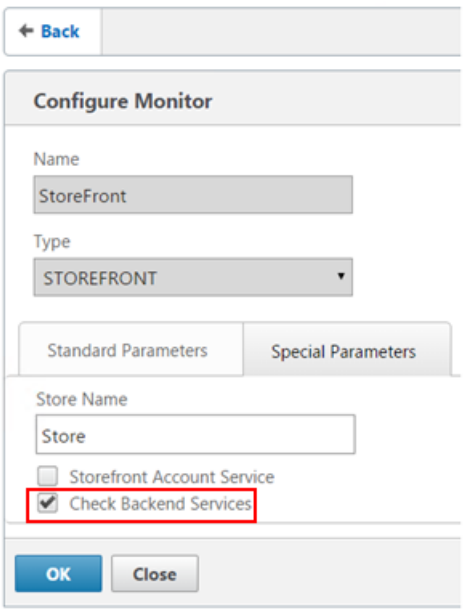
1. Melden Sie sich bei der Citrix ADC-Verwaltungskonsole an.
2. Wählen Sie **Traffic Management > Load Balancing > Monitors > Add** und fügen Sie einen neuen Monitor unter dem Namen *StoreFront* hinzu. Akzeptieren Sie alle Standardeinstellungen.
3. Wählen Sie im Dropdownmenü **Type** die Option **StoreFront**.

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 auf der Registerkarte **Special Parameters** den **Namen des Stores ein**.
6. Wählen Sie auf der Registerkarte **Special Parameters** die Option **Check Backend Services**. 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 der folgenden Dienste zurückgibt:
   - W3SVC (IIS)
   - WAS (Aktivierungsdienst für Windows-Prozesse)
   - CitrixCredentialWallet
   - CitrixDefaultDomainService

Standard Parameters Tab



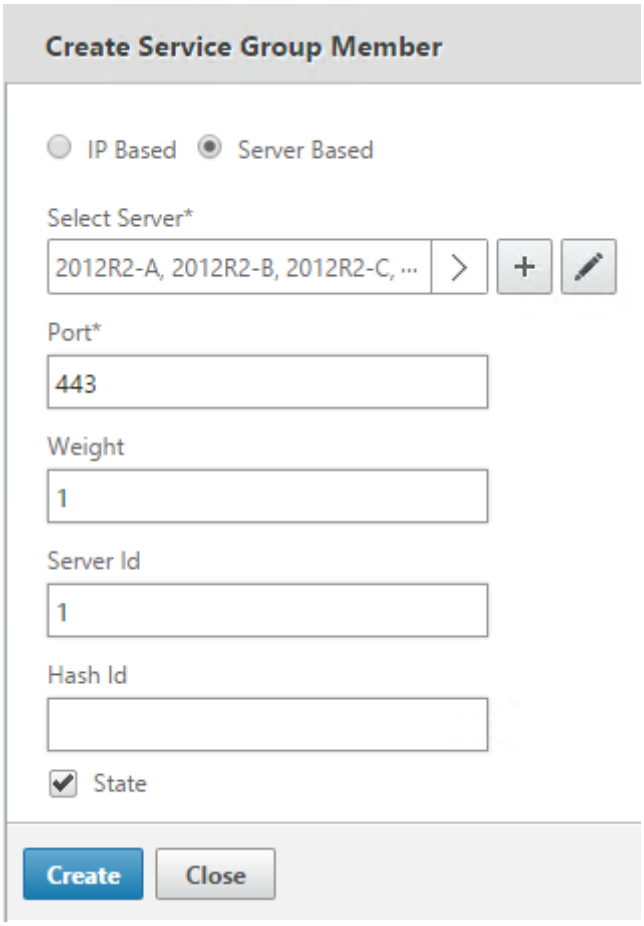
Special Parameters Tab



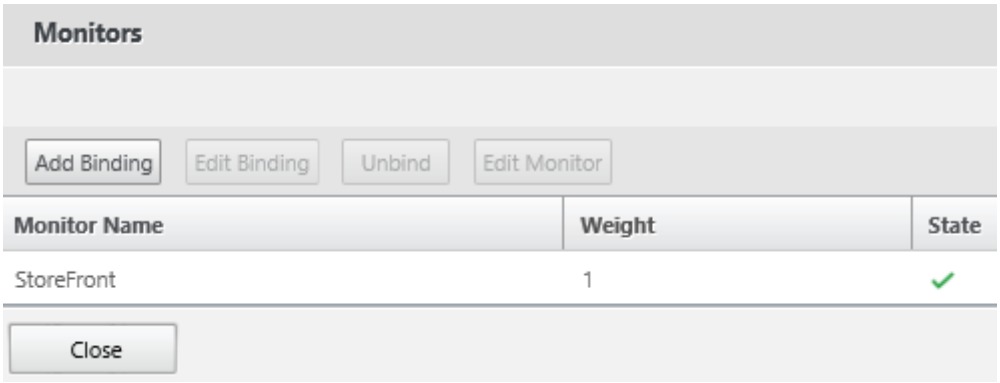
Erstellen einer HTTPS 443-Dienstgruppe für alle StoreFront-Server

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 TLS-Port fest und geben Sie für jeden Knoten beim Hinzufügen eine eindeutige

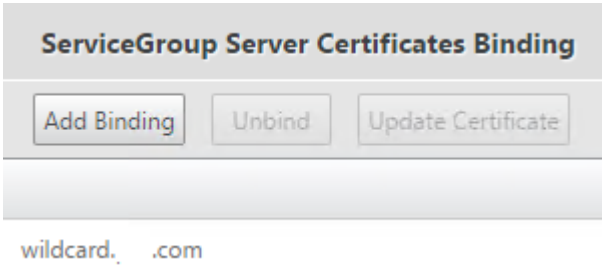
Server-ID an.



3. Wählen Sie auf der Registerkarte **Monitors** den zuvor erstellten StoreFront-Monitor aus.

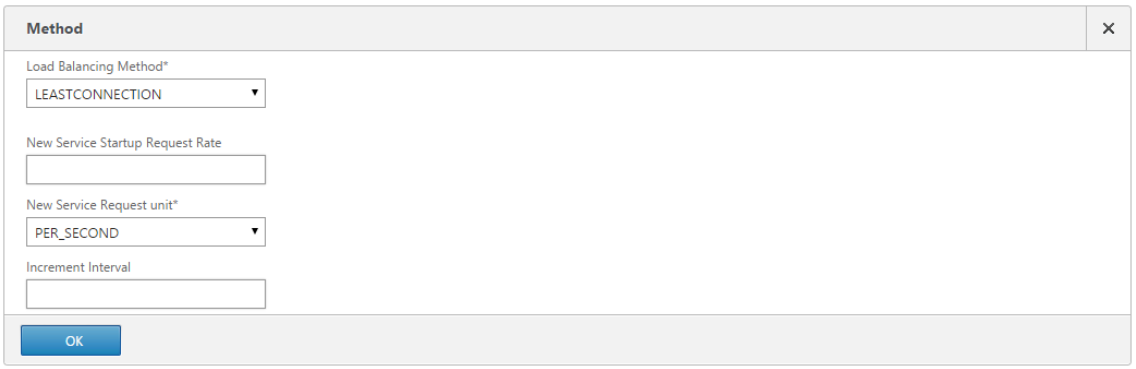


4. Binden Sie auf der Registerkarte **Certificates** das zuvor importierte Serverzertifikat.
5. Binden Sie das Zertifizierungsstellenzertifikat, das zum Signieren des zuvor importierten Serverzertifikats verwendet wurde, sowie jegliche Zertifizierungsstellen, die Teil der PKI-Vertrauenskette sind.

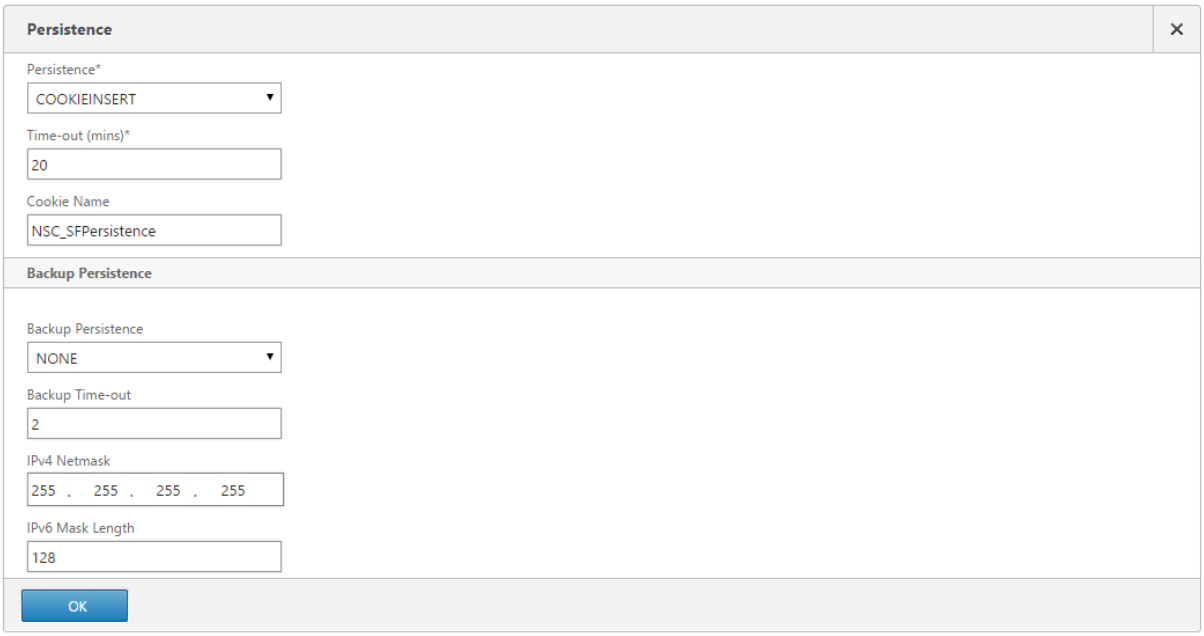


Erstellen eines virtuellen Lastausgleichservers für den Benutzerdatenverkehr

1. Melden Sie sich bei der Verwaltungs-GUI des Citrix ADC-Geräts 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 die zuvor erstellte **Dienstgruppe** an den virtuellen Lastenausgleichserver.
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. Beispielsweise, **NSC_SFPersistence**, da dies das Identifizieren von Fiddler-Spuren während des Debuggens erleichtert.
8. Legen Sie für “Backup persistence” **NONE** fest.



Szenario 2: HTTPS-Beendigung – HTTPS 443-Kommunikation zwischen Client und Citrix ADC-Load Balancer und HTTP 80-Verbindungen zwischen Load Balancer und den StoreFront 3.x-Servern dahinter

Bei diesem Szenario wird der Standard-StoreFront-Monitor unter Einsatz von Port 8000 verwendet.

Hinzufügen einzelner StoreFront-Server zum Citrix ADC-Load Balancer

1. Melden Sie sich bei der Citrix ADC-Verwaltungskonsole an.
2. Wählen Sie **Traffic Management > Load Balancing > Servers > Add** und fügen Sie die vier StoreFront-Server für den Lastausgleich hinzu. Beispiel = 4 x 2012R2 Storefront-Server namens 2012R2-A bis -D. 3.
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 Citrix ADC-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 in der Liste **Type** die Option **StoreFront** aus.

5. Geben Sie auf der Registerkarte **Special Parameters** den **Namen des Stores ein**.
6. Geben Sie für **Destination Port** “8000” ein. Dies stimmt mit der Standardmonitorinstanz überein, die auf jedem StoreFront-Server erstellt wird.
7. Wählen Sie auf der Registerkarte **Special Parameters** die Option **Check Backend Services**. 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 die zuvor erstellte Dienstgruppe an den virtuellen Lastenausgleichserver.
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 rechts **Persistence** aus und legen Sie als Persistenzmethode **COOKIEINSERT** fest.
6. Benennen Sie das Cookie. Beispielsweise, **NSC_SFPersistence**, da dies das Identifizieren von Fiddler-Spuren
   während des Debuggens erleichtert.
7. Legen Sie für “Backup persistence” **NONE** fest.

Erstellen eines virtuellen Lastausgleichsservers für die Abonnementsynchronisierung zwischen Servergruppen

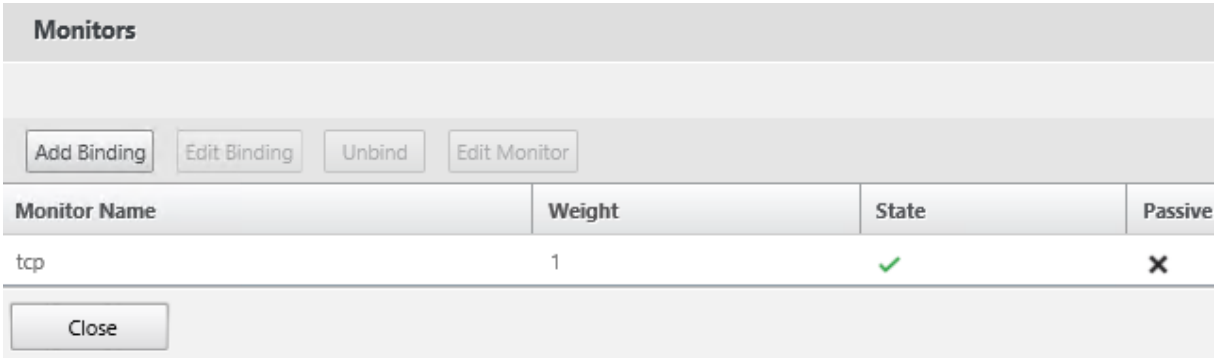
Beim Erstellen eines virtuellen Lastenausgleichsservers sind folgende Optionen in Erwägung zu ziehen:

- **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 Citrix ADC-Gerät 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.

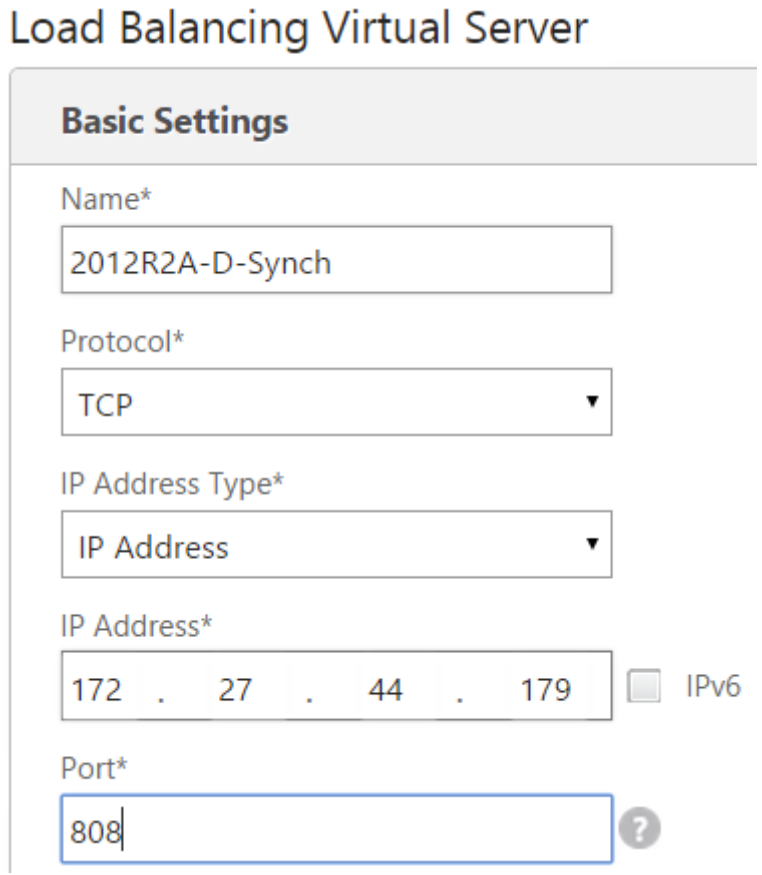
Konfigurieren einer Dienstgruppe für die Synchronisierung von Abonnements

1. Melden Sie sich bei der Verwaltungs-GUI des Citrix ADC-Geräts 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.



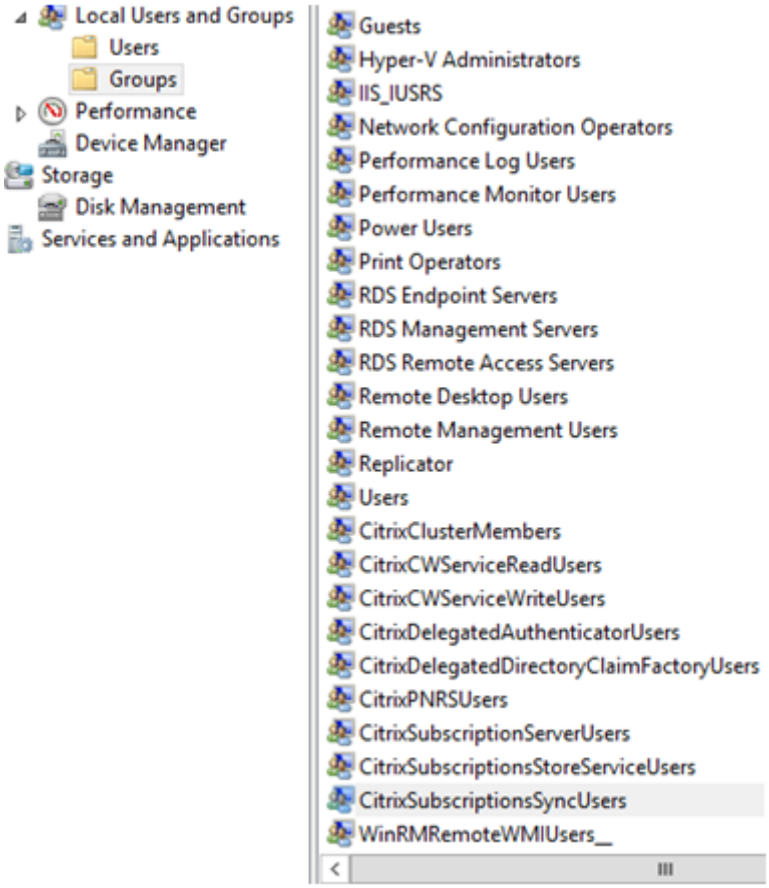
Erstellen eines virtuellen Lastausgleichsservers für die Abonnementsynchronisierung zwischen Servergruppen

1. Melden Sie sich bei der Verwaltungs-GUI des Citrix ADC-Geräts an.
2. Wählen Sie **Traffic Management > Service Groups > Add** aus und fügen Sie eine neue Dienstgruppe hinzu.
3. Setzen Sie die Lastausgleichsmethode auf **Roundrobin**.
4. Ändern Sie das Protokoll in **TCP**.
5. Geben Sie als Portnummer **808** (NICHT **443**) ein.



Mitgliedschaft in CitrixSubscriptionsSyncUsers

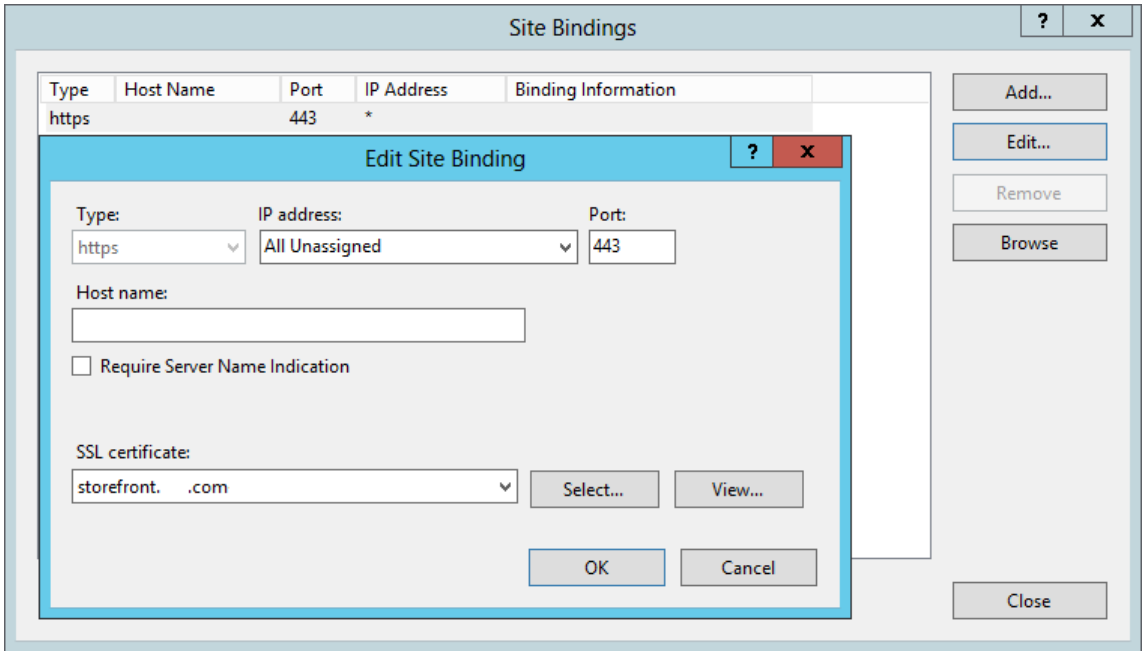
Damit **StoreFront-Server A** am **Standort A** Abonnementdaten von **Server B** an einem anderen Standort anfordern und abrufen kann, muss Server A Mitglied der lokalen Sicherheitsgruppe **CitrixSubscriptionsSyncUsers** auf Server B sein. Die lokale Gruppe **CitrixSubscriptionsSyncUsers** enthält eine 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.



Szenario 1: Konfigurieren der StoreFront-Servergruppe mit HTTPS zwischen Citrix ADC und StoreFront

1. Importieren Sie auf allen StoreFront-Knoten in der Servergruppe das Zertifikat und den privaten Schlüssel, das bzw. den Sie auf dem virtuellen Citrix ADC-Lastausgleichsserver bereitgestellt haben.
2. Erstellen Sie eine HTTPS-Bindung in IIS auf allen StoreFront-Knoten und binden Sie das zuvor

importierte Zertifikat.

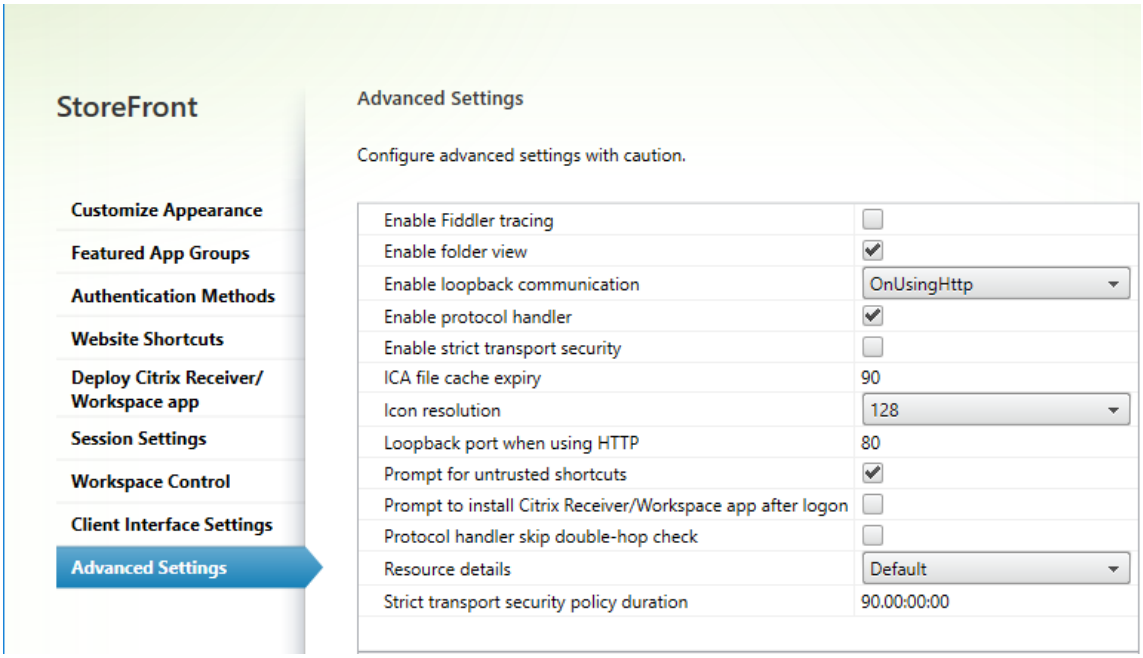


3. Wenn Sie HTTPS zwischen Citrix ADC-Load Balancer und StoreFront verwenden, müssen Sie ein Zertifikat verwenden, das den FQDN mit Lastausgleich als allgemeinen Namen (CN) oder als alternativen Antragstellernamen (Subject Alternative Name, SAN) enthält.

   Siehe Erstellen eines SSL-Zertifikats für den Citrix ADC-Load Balancer und StoreFront-Server.

Szenario 2: Konfigurieren der StoreFront-Servergruppe mit HTTP zwischen Citrix ADC und StoreFront

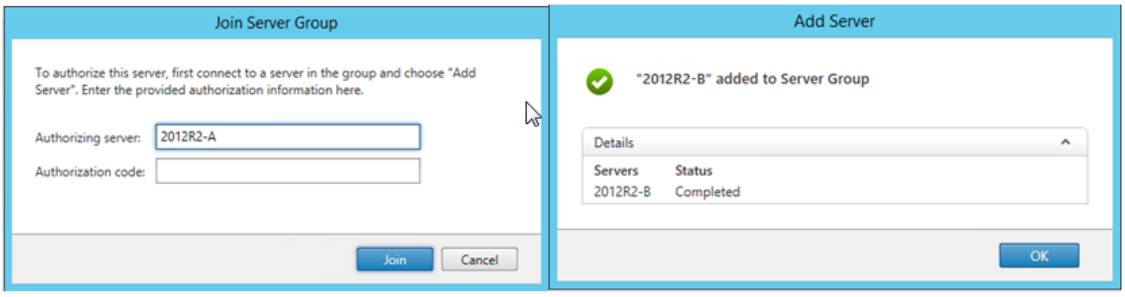
1. Entfernen Sie die HTTPS-Bindung aus IIS von jedem StoreFront-Knoten, sofern bereits vorhanden.
2. Stellen Sie sicher, dass die HTTP-Bindung in IIS vorhanden und auf Port 80 festgelegt ist.
3. Konfigurieren Sie die Loopback-Einstellungen in Receiver für Web mit **OnUsingHTTP** und Port **80** . Dieser Schritt ist wichtig, um sicherzustellen, dass die Clienterkennung zwischen der nativen Citrix Workspace-App und Receiver für Web funktioniert.



Identische Schritte in Szenario 1 und 2

1. Installieren Sie StoreFront auf jedem Knoten in der Servergruppe.
2. 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. Dies muss in beiden Szenarios `https://storefrontlb.domain.com` sein und mit dem FQDN des virtuellen Citrix ADC-Lastausgleichservers übereinstimmen.

   Siehe Erstellen eines SSL-Zertifikats für den Citrix ADC-Load Balancer und StoreFront-Server.
3. Fügen Sie nach der Erstkonfiguration von StoreFront die einzelnen Knoten nacheinander unter Verwendung des primären Knotens der Servergruppe hinzu.
4. Wählen Sie für beitretende Server **Server Group > Add Server > Copy the Authorization Code** aus.



5. Verteilen Sie die Konfiguration vom primären Knoten auf alle anderen Knoten in der Servergruppe.

6. Testen Sie die Servergruppe mit Lastausgleich mit einem Client, der den freigegebenen FQDN des Load Balancers kontaktieren und auflösen kann.

Citrix Service Monitor

Um die externe Überwachung des Ausführenstatus von Windows-Diensten zu aktivieren, 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 Citrix ADC-Geräten, 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 PowerShell-Cmdlets zum Anzeigen bzw. Konfigurieren der Dienst-URL des StoreFront-Monitors.

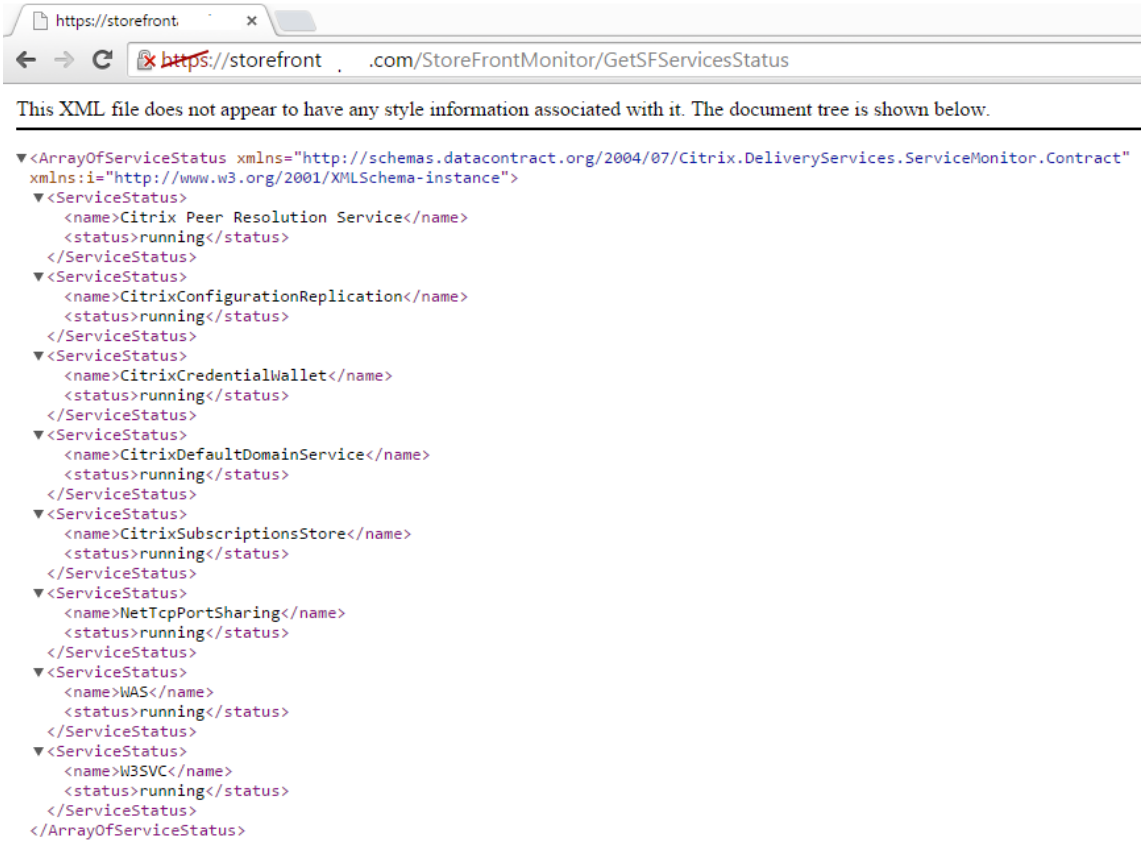
Ersetzen des Standarddienstmonitors durch einen Monitor, der HTTPS und Port 443 verwendet

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://<loadbalancingFQDN>:443/StoreFrontMonitor/GetSFServicesStatus
```

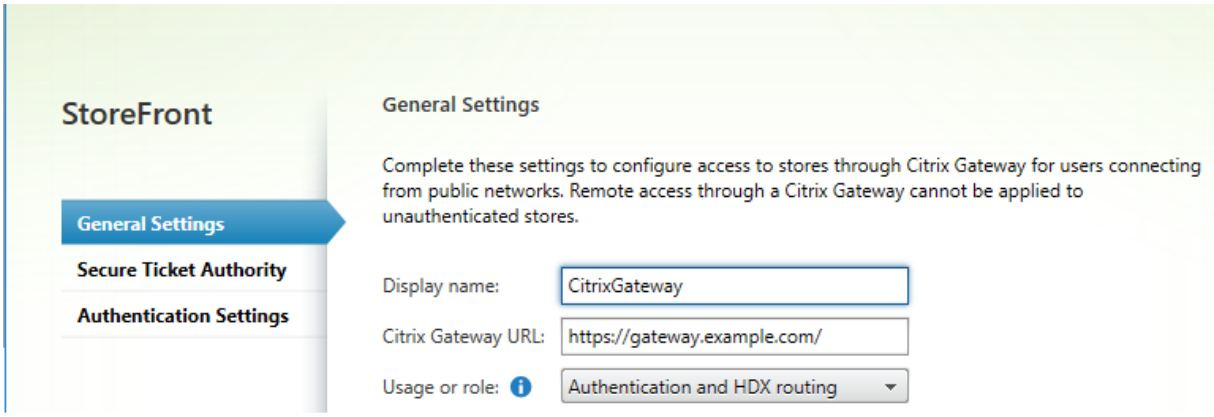



Citrix Gateway und virtuelle Lastausgleichsserver auf demselben Citrix ADC-Gerät

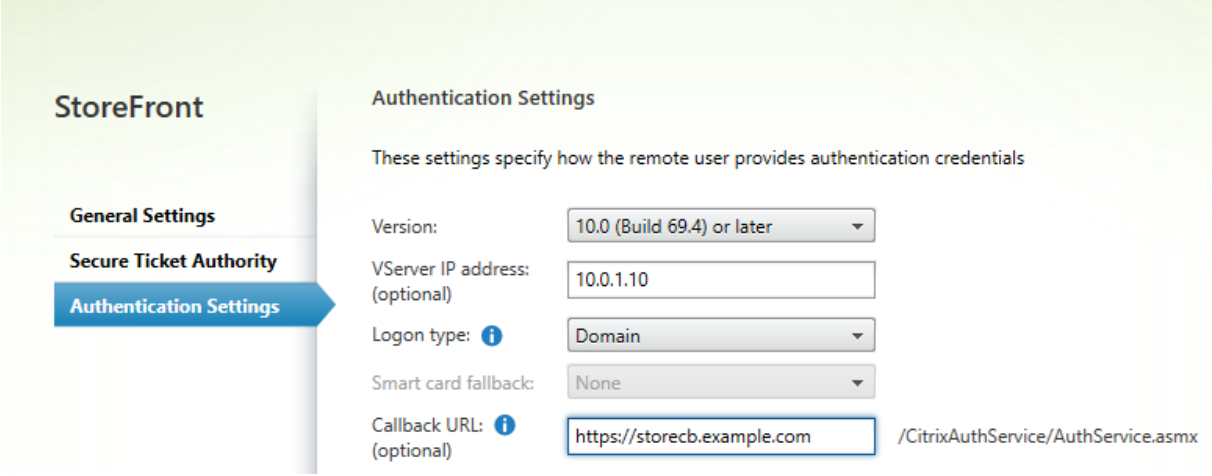
Wenn Sie den virtuellen Citrix Gateway-Server und den virtuellen Lastausgleichsserver auf demselben Citrix ADC-Gerät konfiguriert haben, treten beim Zugriff interner Domänenbenutzer auf die Host-Basis-URL von StoreFront mit Lastausgleich möglicherweise Probleme auf, wenn der Zugriff direkt und nicht über den virtuellen Citrix Gateway-Server erfolgt.

In diesem Szenario geht StoreFront davon aus, dass der Endbenutzer sich bereits bei Citrix Gateway authentifiziert hat, da StoreFront die Quell-IP-Adresse des Benutzers mit der Subnetz-IP-Adresse (SNIP) von Citrix Gateway korreliert. Dadurch wird ein Versuch von StoreFront ausgelöst, den Benutzer unter Verwendung des AGBasic-Protokolls ohne Benutzereingriff bei Citrix 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 oder geben Sie eine VIP ein, sodass die Authentifizierung mit Benutzernamen und Kennwort anstelle des AGBasic-Anmeldeprotokolls verwendet wird.

Konfigurieren von Citrix Gateway in der StoreFront-Servergruppe



Geben Sie die Citrix Gateway-VIP im Feld “vServer-IP-Adresse” ein. Verwenden Sie NICHT die Subnetz-IP für das Citrix Gateway, wenn der virtuelle Lastausgleichserver auf demselben Citrix ADC-Gerät residiert.



Loopback-Optionen beim Lastausgleich für eine StoreFront-Servergruppe mit einem Citrix ADC-Gerät

Sie können Loopback-Optionen mit PowerShell festlegen.

Beispiel einer web.config-Datei für Receiver für Web

```
1 <communication attempts="2" timeout="00:01:00" loopback="On"
     loopbackPortUsingHttp="80">
```


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 TLS-Begrenzung wird.
OnUsingHttp — Ändert den Host in 127.0.0.1 und das Schema in HTTP und ändert den Port in den für **loopbackPortUsingHttp** konfigurierten Wert.	Verwenden Sie dies nur, wenn Sie einen Load Balancer mit TLS-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 Citrix Gateway

April 1, 2020

In StoreFront können Sie über **Citrix Gateways verwalten > Hinzufügen** oder **Bearbeiten** in der StoreFront-Verwaltungskonsole eine einzelne Citrix Gateway-URL hinzufügen. Es ist auch möglich, eine öffentliche Citrix Gateway-URL und eine GSLB-URL (Global Server Load Balancing) über **Citrix 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 Citrix Gateway-Verwaltung in StoreFront in folgenden Anwendungsfällen:

1. **GSLB und mehrere Citrix Gateways**. Verwenden von GSLB und mehrerer Citrix Gateways für den Lastausgleich bei Remoteverbindungen mit veröffentlichten Ressourcen an mehreren Orten innerhalb einer großen, globalen Citrix Bereitstellung.
2. **Ein Citrix Gateway mit öffentlicher oder privater URL**. Verwenden desselben Citrix 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 (und Thema). Wenn Sie mit StoreFront-Gateway und Global Server Load Balancing (GSLB) noch nicht vertraut sind, konsultieren Sie die Informationslinks am Ende dieses Artikels.

Das Feature bietet die folgenden Vorteile:

- Unterstützung zweier URLs für dasselbe Gatewayobjekt.
- Die Benutzer können beim Zugriff auf Citrix Gateway zwischen zwei URLs wechseln, ohne dass der Administrator das StoreFront-Gatewayobjekt auf die gewünschte Gateway-URL umkonfigurieren muss.
- Weniger Zeitaufwand für Einrichtung und Tests der StoreFront-Gatewaykonfiguration bei Verwendung mehrerer GSLB-Gateways.
- Verwendung desselben Citrix Gateway-Objekts in StoreFront innerhalb der DMZ für den externen und internen Zugriff.
- Unterstützung für beide URLs für das optimale Gatewayrouting. Weitere Hinweise zum optimalen Gatewayrouting finden Sie unter Einrichten hoch verfügbarer Stores mit mehreren Sites.

Überlegungen zur Bereitstellung bei Verwendung zweier Gateway-URLs

- Der GatewayURL-FQDN wird für jedes Gateway in der StoreFront-Verwaltungskonsole angezeigt. Die Eigenschaft “GSLBURL” jedes Gateways kann nur unter Verwendung von PowerShell-Cmdlets angezeigt werden.
- Die GatewayURL wird von den nativen Citrix Receiver-Bereitstellungen und der Citrix Workspace-App zur Authentifizierung verwendet.
- Die GatewayURL ist im location-Tag der Bereitstellungsdatei (receiver.cr) enthalten, die zum Konfigurieren von Citrix Receiver und der Citrix Workspace-App mit Store- und Gateway-Informationen verwendet wird.
- Verwenden Sie die bereitgestellte PowerShell zum Ändern von web.config-Dateien für Stores und Roaming. Tun Sie dies nicht manuell.

> **Wichtig:**
>
> Bevor Sie eine zweite Gateway-URL mit dem Parameter “-gslburl” konfigurieren, prüfen Sie,

> welche Serverzertifikate installiert sind und wie die DNS-Auflösung in Ihrem Unternehmen erfolgt. Alle URLs, die Sie in der Citrix Gateway- und StoreFront-Bereitstellung verwenden möchten, müssen in den Serverzertifikaten aufgelistet sein. Weitere Informationen zu Serverzertifikaten 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. `example.com` und `example.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 Hostbasis-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 ein Citrix 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

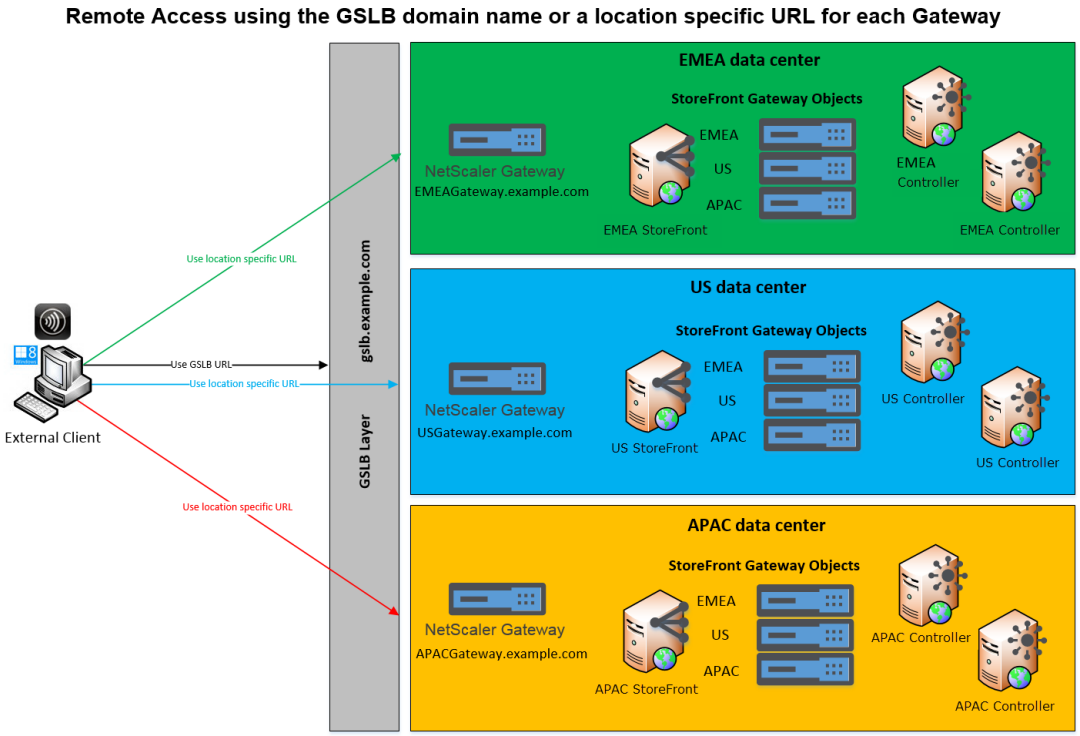
Ein öffentlich signiertes SAN-Serverzertifikat für den externen Zugriff über GSLB muss folgende FQDNs enthalten:

```
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: Receiver für Web: GSLB und mehrere Citrix Gateways

Der Administrator verwendet GSLB und mehrere Citrix 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 auf den Citrix ADC-Geräten 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 Citrix Gateway-Server der GSLB-Schicht enthalten. Die Citrix Gateways für GSLB 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 Citrix Virtual Apps and Desktops-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 1: Receiver für Web und Citrix Receiver oder Citrix Workspace-App: GSLB und mehrere Citrix Gateways

Gateway-Attribute

Zur Verwendung von GSLB mit nativen Citrix Receiver- oder Citrix Workspace-App-Bereitstellungen, verwenden Sie **Add-STFRoamingGateway** (zum Erstellen) oder **Set-STFRoamingGateway** (zum Ändern), um folgende Attribute anzugeben:

-GatewayUrl: der von allen GSLB-Gateways gemeinsam verwendete FQDN

-GSLBurl: der eindeutige FQDN für jedes Gateway

> Hinweis:
>
> Dies mag unlogisch erscheinen, hat aber keinen Einfluss auf diesen Web-Anwendungsfall. Es gewährleistet, dass native Citrix Receiver- oder Citrix Workspace-App-Bereitstellungen den von GSLB verwendeten, gemeinsam genutzten FQDN im Discoverydokument erhalten, das beim Zugriff auf den Endpunkt `https://storefront.domain.com/citrix/<storename>/discovery` gefunden wird. Außerdem wird sichergestellt, dass die mit dem StoreFront-Befehl **Provisioningdatei exportieren** exportierte Bereitstellungsdatei (receiver.cr) den gemeinsam genutzten GSLB-FQDN enthält.

Beispiele für Provisioningdateien

Beispieldatei 1 mit `-GatewayUrl https://gslb.domain.com`. Damit kann Citrix Receiver bzw. die Citrix Workspace-App GSLB verwenden, um eine Verbindung mit Gateways herzustellen.


```
<?xml version="1.0" encoding="utf-8"?>
<Services version="1.0"
    xmlns="http://www.citrix.com/ServiceRecord">
    <Service type="store">
        <SRID>167659780</SRID>
        <Name>Store</Name>
        <Address>https://storefront.domain.com/Citrix/Store/discovery</Address>
        <Gateways>
            <Gateway Name="EMEAGateway" Default="true" Edition="Enterprise" Auth="Domain" RewriteMode="NONE">
                <Location>https://gslb.domain.com/</Location>
            </Gateway>
            <Gateway Name="USGateway" Edition="Enterprise" Auth="Domain" RewriteMode="NONE">
                <Location>https://gslb.domain.com/</Location>
            </Gateway>
            <Gateway Name="APACGateway" Edition="Enterprise" Auth="Domain" RewriteMode="NONE">
                <Location>https://gslb.domain.com/</Location>
            </Gateway>
        </Gateways>
        <Beacons>
            <Internal>
                <Beacon>https://storefront.domain.com/</Beacon>
            </Internal>
            <External>
                <Beacon>https://emeagateway.domain.com</Beacon>
                <Beacon>https://usgateway.domain.com</Beacon>
                <Beacon>https://apacgateway.domain.com</Beacon>
                <Beacon>http://gslb.domain.com</Beacon>
            </External>
        </Beacons>
    </Service>
</Services>
```

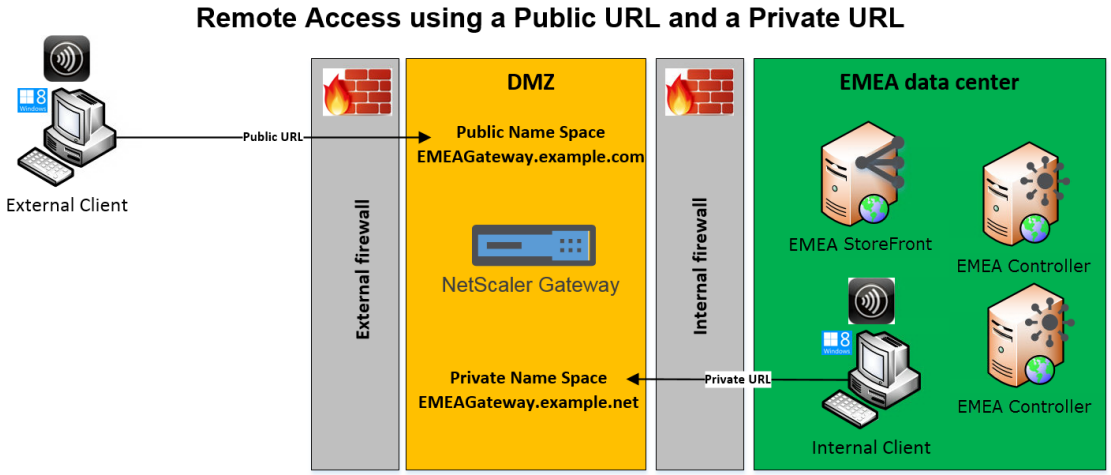
Beispieldatei 2 mit `-GatewayUrl https://emeagateway.domain.com, https://usgateway.domain.com and https://apacgateway.domain.com`. Damit kann Citrix Receiver bzw. die Citrix Workspace-App die eindeutigen URLs verwenden, um eine Verbindung mit Gateways herzustellen.

```
<?xml version="1.0" encoding="utf-8"?>
<Services version="1.0"
    xmlns="http://www.citrix.com/ServiceRecord">
    <Service type="store">
        <SRID>167659780</SRID>
        <Name>Store</Name>
        <Address>https://storefront.domain.com/Citrix/Store/discovery</Address>
        <Gateways>
            <Gateway Name="EMEAGateway" Default="true" Edition="Enterprise" Auth="Domain" RewriteMode="NONE">
                <Location>https://emeagateway.domain.com/</Location>
            </Gateway>
            <Gateway Name="USGateway" Edition="Enterprise" Auth="Domain" RewriteMode="NONE">
                <Location>https://ftlgateway.domain.com/</Location>
            </Gateway>
            <Gateway Name="APACGateway" Edition="Enterprise" Auth="Domain" RewriteMode="NONE">
                <Location>https://bglgateway.domain.com/</Location>
            </Gateway>
        </Gateways>
        <Beacons>
            <Internal>
                <Beacon>https://storefront.domain.com/</Beacon>
            </Internal>
            <External>
                <Beacon>https://emeagateway.domain.com</Beacon>
                <Beacon>https://usgateway.domain.com</Beacon>
                <Beacon>https://apacgateway.domain.com</Beacon>
                <Beacon>http://gslb.domain.com</Beacon>
            </External>
        </Beacons>
    </Service>
</Services>
```

Der gemeinsam genutzte FQDN wird von den nativen Citrix Receiver- und Citrix Workspace-App-Bereitstellungen verwendet.

Anwendungsfall 2: ein Citrix Gateway mit öffentlicher oder privater URL

Der Administrator verwendet dasselbe Citrix 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 Citrix Gateway läuft, selbst wenn der Client intern ist.
- Das Citrix Gateway befindet sich in einer DMZ.
- Es gibt zwei Netzwerkrouten zum Citrix 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", um das Attribut **GslbLocation** für das StoreFront-Gatewayobjekt festzulegen. Beispiel:

```
1 Add-STFRoamingGateway -Name "EMEAGateway" -GatewayUrl "https://
    emeagateway.example.com" -GSLBurl "https://gslb.example.com" -
    SubnetIPAddress "10.0.0.1" -CallbackUrl "https://emeagateway.example
    .com" -LogonType "DomainAndRSA" -SmartCardFallbackLogonType "None" -
    Version "Version10_0_69_4" -SecureTicketAuthorityUrls "https://emea-
    controller.example.com/scripts/ctxsta.dll,https://us-controller.
    example.com/scripts/ctxsta.dll,https://apac-controller.example.com/
    scripts/ctxsta.dll"
2 Set-STFRoamingGateway -Name "EMEAGateway" -GatewayUrl "https://
    emeagateway.example.com" -GSLBurl "https://gslb.example.com"
```



```
3 Get-STFRoamingGateway -Name "EMEAGateway" (returns just the EMEA
    gateway object)
4 Or
5 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.

```
1 $EMEAGateway = Get-STFRoamingGateway
2 $EMEAGateway.GslbLocation = $Null
3 Set-STFRoamingGateway -Gateway $EMEAGateway
```

Im Anwendungsfall 1 werden durch **Get-STFRoamingGateway** die folgenden Gateways zurückgegeben:

```
1 Name: EMEAGateway
2 Location: https://emeagateway.example.com/ (Unique URL for the EMEA
    Gateway)
3 GslbLocation: https://gslb.example.com/ (GSLB URL for all three
    gateways)
4
5 Name: USGateway
6 Location: https://USgateway.example.com/ (Unique URL for the US Gateway
    )
7 GslbLocation: https://gslb.example.com/ (GSLB URL for all three
    gateways)
8
9 Name: APACGateway
10 Location: https://APACgateway.example.com/ (Unique URL for the APAC
    Gateway)
11 GslbLocation:  https://gslb.example.com/ (GSLB URL for all three
    gateways)
```

Im Anwendungsfall 2 werden durch **Get-STFRoamingGateway** die folgenden Gateways zurückgegeben:

```
1 Name: EMEAGateway
2 Location: https://emeagateway.example.com/ (Public URL for the Gateway)
3 GslbLocation: https://emeagateway.example.net/ (Private URL for the
    Gateway)
```


Im Anwendungsfall 1 wird durch **Get STFStoreRegisteredOptimalLaunchGateway** “Optimal Gateway Routing” zurückgegeben:

```
$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-URL oder die 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.

Im Anwendungsfall 1 in der web.config-Roamingdatei

```
<gateway id="cca13269-18c1-10fd-a0df-7931b3897aa8" name="EMEAGateway" default="false" edition="Enterprise" version="Version10_0_69_1" auth="DomainAndRSA" smartcardfallback="None" ipaddress="10.0.0.1" rwmode="NONE" deployment="Appliance" callbackurl=https://emeagateway.example.com/CitrixAuthService/AuthService.asmx sessionreliability="true" requesttickettwosta="false" stasUseLoadBalancing="false" stasBypassDuration="01:00:00">
<location path="https://emeagateway.example.com/" /><gslbLocation path="https://gslb.example.com/" /><clusternodes>
<clear />
</clusternodes>
<silentauthenticationurls>
<clear />
</silentauthenticationurls>
<secureticketauthorityurls>
```



```
<clear />
<location path="https://emea-controller.example.com/scripts/ctxsta.dll" />
<location path="https://us-controller.example.com/scripts/ctxsta.dll" />
<location path="https://apac-controller.example.com/scripts/ctxsta.dll" />
</secureticketauthorityurls>
</gateway>

<gateway id="b8ec720c-d85e-1889-8188-1cf08a2cf762" name="USGateway" default="false" edition="Enterprise" version="Version10_0_69_1" auth="DomainAndRSA" smartcardfallback="None" ipaddress="10.0.0.2" rwmode="NONE" deployment="Appliance" callbackurl="https://usgateway.example.com/CitrixAuthService/AuthService.asmx" sessionreliability="true" requesttickettwosta="false" stasUseLoadBalancing="false" stasBypassDuration="01:00:00"><location path="https://usgateway.example.com/" /><gslbLocation path="https://gslb.example.com/" /><clusternodes>
<clear />
</clusternodes>
<silentauthenticationurls>
<clear />
</silentauthenticationurls>
<secureticketauthorityurls>
<clear />
<location path="https://emea-controller.example.com/scripts/ctxsta.dll" />
<location path="https://us-controller.example.com/scripts/ctxsta.dll" />
<location path="https://apac-controller.example.com/scripts/ctxsta.dll" />
</secureticketauthorityurls>
</gateway>

<gateway id="c57117b5-e111-1eed-9117-a1ffa1c8100e" name="APACGateway" default="false" edition="Enterprise" version="Version10_0_69_1" auth="DomainAndRSA" smartcardfallback="None" ipaddress="10.0.0.3" rwmode="NONE" deployment="Appliance" callbackurl="https://apacgateway.example.com/CitrixAuthService/AuthService.asmx" sessionreliability="true" requesttickettwosta="false" stasUseLoadBalancing="false" stasBypassDuration="01:00:00"><location path="https://apacGateway.example.com/" /><gslbLocation path="https://gslb.example.com/" /><clusternodes>
<clear />
```



```
</clusternodes>
<silentauthenticationurls>
<clear />
</silentauthenticationurls>
<secureticketauthorityurls>
<clear />
<location path="https://emea-controller.example.com/scripts/ctxsta.dll" />
<location path="https://us-controller.example.com/scripts/ctxsta.dll" />
<location path="https://apac-controller.example.com/scripts/ctxsta.dll" />
</secureticketauthorityurls>
</gateway>
```

Im Anwendungsfall 2 in der web.config-Roamingdatei

```
<gateway id="cca13269-18c1-10fd-a0df-7931b3897aa8" name="EMEAGateway" default="false" edition="Enterprise" version="Version10_0_69_1" auth="Domain" smartcardfallback="None" ipaddress="10.0.0.1" rwmode="NONE" deployment="Appliance" callbackurl="https://emeagateway.example.com/CitrixAuthService/AuthService.asmx" sessionreliability="true" requesttickettwosta="false" stasUseLoadBalancing="false" stasBypassDuration="01:00:00">
<location path="https://emeagateway.example.com/" />
<gslbLocation path=" https://emeagateway.example.net/" />
<clusternodes>
<clear />
</clusternodes>
<silentauthenticationurls>
<clear />
</silentauthenticationurls>
<secureticketauthorityurls>
<clear />
<location path="https://emea-controller.example.net/scripts/ctxsta.dll" />
</secureticketauthorityurls>
</gateway>
```

Verwandte Informationen

Siehe Citrix StoreFront SDK PowerShell Modules in der Dokumentation für Entwickler.

Konfigurieren von Citrix ADC und StoreFront für die delegierte Formularauthentifizierung (DFA)

July 9, 2019

Die erweiterbare Authentifizierung (extensible authentication) bietet einen einzelnen Anpassungspunkt zur Erweiterung der formularbasierten Authentifizierung des Citrix ADC-Geräts und von StoreFront. Zum Erstellen einer Authentifizierungslösung mit dem Extensible Authentication-SDK müssen Sie die delegierte Formularauthentifizierung (DFA) zwischen dem Citrix ADC-Gerät 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: Citrix Gateway delegiert seine Authentifizierung an StoreFront und StoreFront interagiert dann mit einem Drittanbieter-Authentifizierungsserver oder -dienst.

Das Konfigurieren der delegierten Formularauthentifizierung in Citrix Gateway wird in unter CTX200383 beschrieben.

Installationsempfehlungen

- Zum Schützen der Kommunikation zwischen dem Citrix ADC-Gerät 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 auf dem Citrix ADC-Gerät 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, 860
                                      e9401-39c8-4f2c-928d-34251102
                                      b840] }

ParameterData                   : {
 [FeatureClassId, e1eb3668-9c1c-4ad8-bbae-c08b2682c1bc], [
```



```
       ParentInstanceId, 8dd182c7-f
24                                970-466c-ad4c-27a5980f716c], [
                                      TenantId, 860e9401-39c8-4f2c
                                      -928d-34251102b840] }
25
26 AdditionalInstanceDependencies : {
27  b1e48ef0-b9e5-4697-af9b-0910062aa2a3 }
28
29 IsDeployed                     : True
30 FeatureClass                   : Citrix.DeliveryServices.Framework
      .Feature.FeatureClass
```

2. Fügen Sie Citrix Trusted Client hinzu. Konfigurieren Sie den gemeinsamen geheimen Schlüssel (Passphrase) zwischen StoreFront und dem Citrix ADC-Gerät. Passphrase und Client-ID müssen mit denen auf dem Citrix ADC-Gerät identisch sein.

```
1 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. Sie finden ConversationFactory unter C:\inetpub\wwwroot\Citrix\Authentication\web.config. Dies ist ein Beispiel für das, was Sie sehen.

```
1  <example connectorURL="http://Example.connector.url:8080/adapters-
      sf-aaconnector-webapp">
2        <routeTable order="1000">
3          <routes>
4            <route name="StartExampleAuthentication" url="Example-
                Bridge-Forms/Start">
5              <defaults>
6                <add param="controller" value="
                    ExplicitFormsAuthentication" />
7                <add param="action" value="AuthenticateStart" />
8                <add param="postbackAction" value="Authenticate" />
9                <add param="cancelAction" value="CancelAuthenticate"
                     />
10               <add param="conversationFactory" value="
                    ExampleBridgeAuthentication" />
11               <add param="changePasswordAction" value="
                    StartChangePassword" />
12               <add param="changePasswordController" value="
                    ChangePassword" />
```

```
13                <add param="protocol" value="CustomForms" />
14              </defaults>
15            </route>
```

4. Legen Sie die Formularkonversationsfactory für die delegierte Formularauthentifizierung in PowerShell fest. In diesem Beispiel auf ExampleBridgeAuthentication.

```
1 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 Sie 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

December 23, 2019

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 Citrix 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 Citrix 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 oder die Citrix Workspace-App unterstützt.

Einrichten einer Testumgebung

In diesem Beispiel werden die Produktionsdomäne “production.com” und die Testdomäne “development.com” verwendet.

`production.com`-Domäne

Die Domäne `production.com` ist im Beispiel wie folgt eingerichtet:

- Citrix Gateway mit konfigurierter LDAP-Authentifizierungsrichtlinie für `production.com`.
- Die Authentifizierung über das Gateway erfolgt mit einem Konto vom Typ production\testuser1 plus Kennwort.

`development.com`-Domäne

Die Domäne `development.com` ist im Beispiel wie folgt eingerichtet:

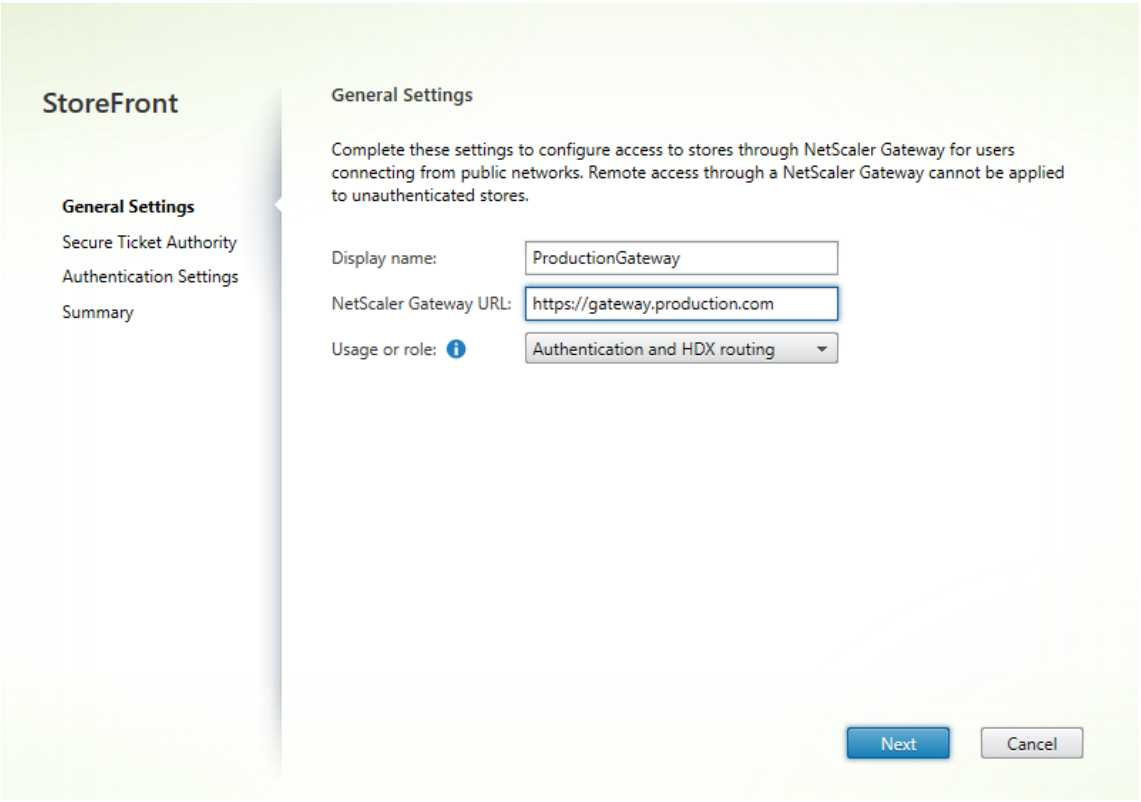
- StoreFront, Citrix Virtual Apps and Desktops und VDAs befinden sich alle in der`development.com` Domäne.
- Die Authentifizierung bei der Citrix Receiver für Web-Site erfolgt mit einem Konto vom Typ development\testuser1 plus Kennwort.
- Es besteht keine Vertrauensstellung zwischen den beiden Domänen.

Konfigurieren eines Citrix Gateways für den Store

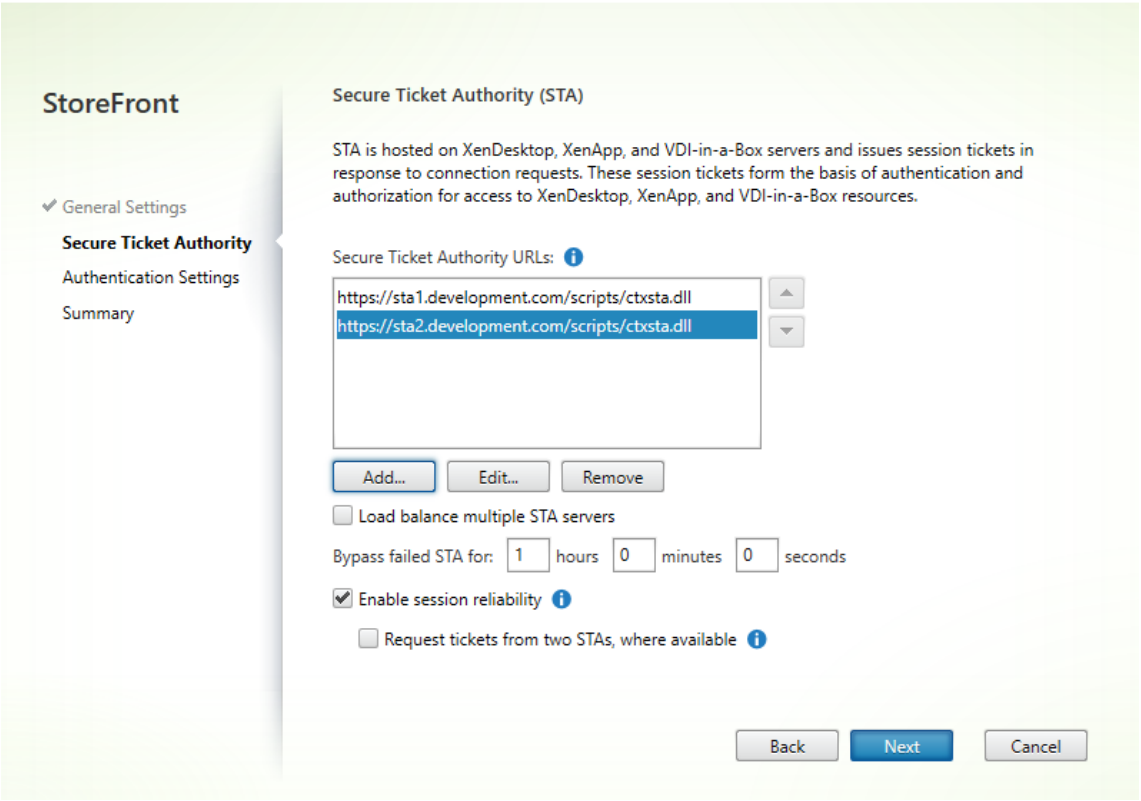
Gehen Sie zum Konfigurieren eines Citrix Gateways für den Store folgendermaßen vor:

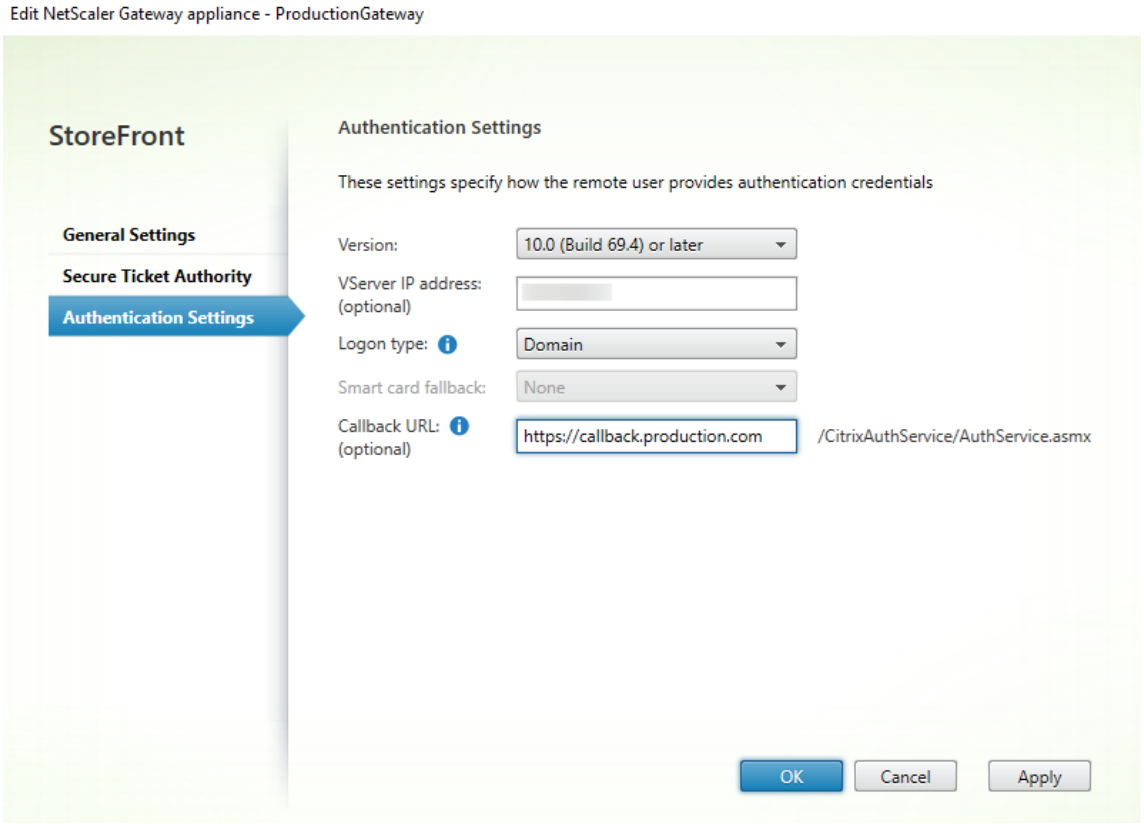
1. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole **Stores** und klicken Sie im Bereich **Aktionen** auf **Citrix Gateways verwalten**.
2. Klicken Sie auf dem Bildschirm “Citrix Gateways verwalten” auf die Schaltfläche **Hinzufügen**.
3. Legen Sie die Einstellungen für “Allgemeine Einstellungen”, “Secure Ticket Authority” und “Authentifizierung” fest.

Add NetScaler Gateway Appliance



Add NetScaler Gateway Appliance

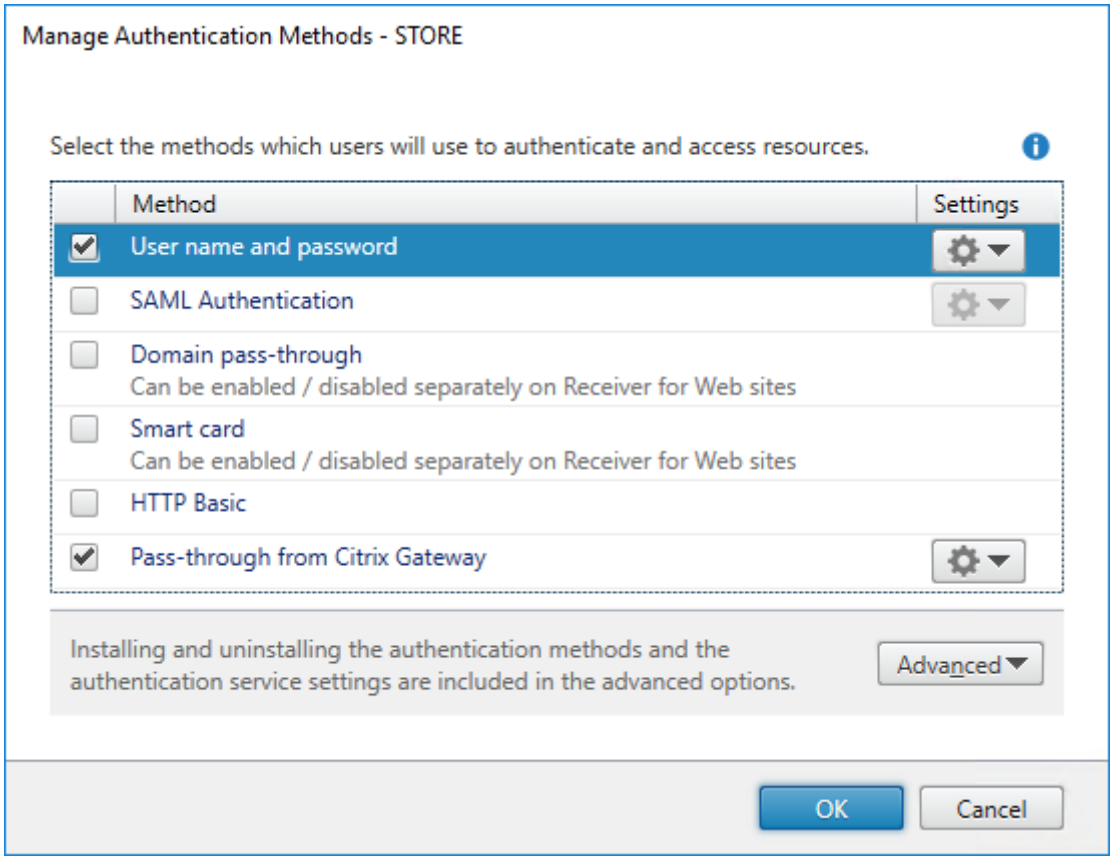




> **Hinweis:**
>
> Bedingte DNS-Weiterleitungen müssen ggf. hinzugefügt werden, damit DNS-Server in beiden Domänen FQDNs in der anderen Domäne auflösen können. Das Citrix ADC-Gerät muss die FQDNs des STA-Servers in der Domäne `development.com` auflösen können, indem es den DNS-Server von `production.com` 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 Citrix Gateway-Servers aufgelöst wird.

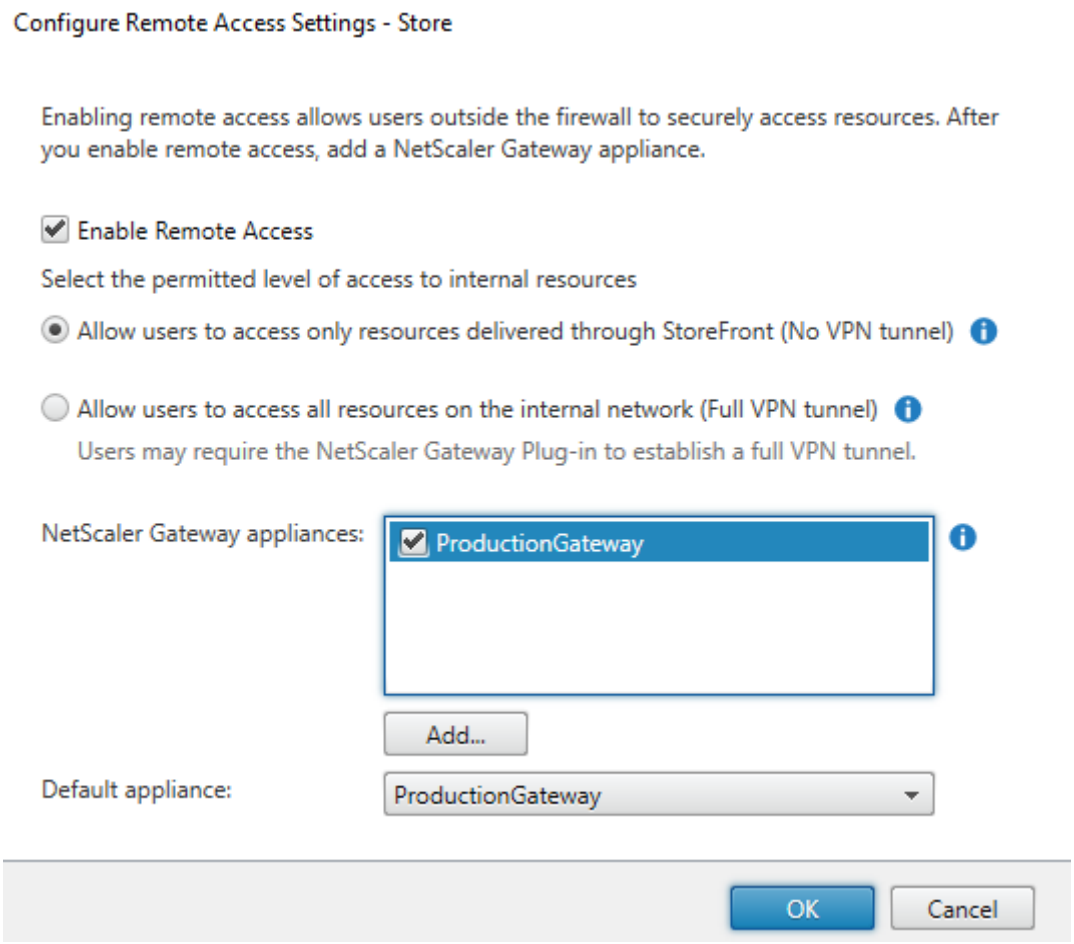
Aktivieren von Passthrough von Citrix Gateway

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 Citrix Gateway**.
3. Klicken Sie auf **OK**.



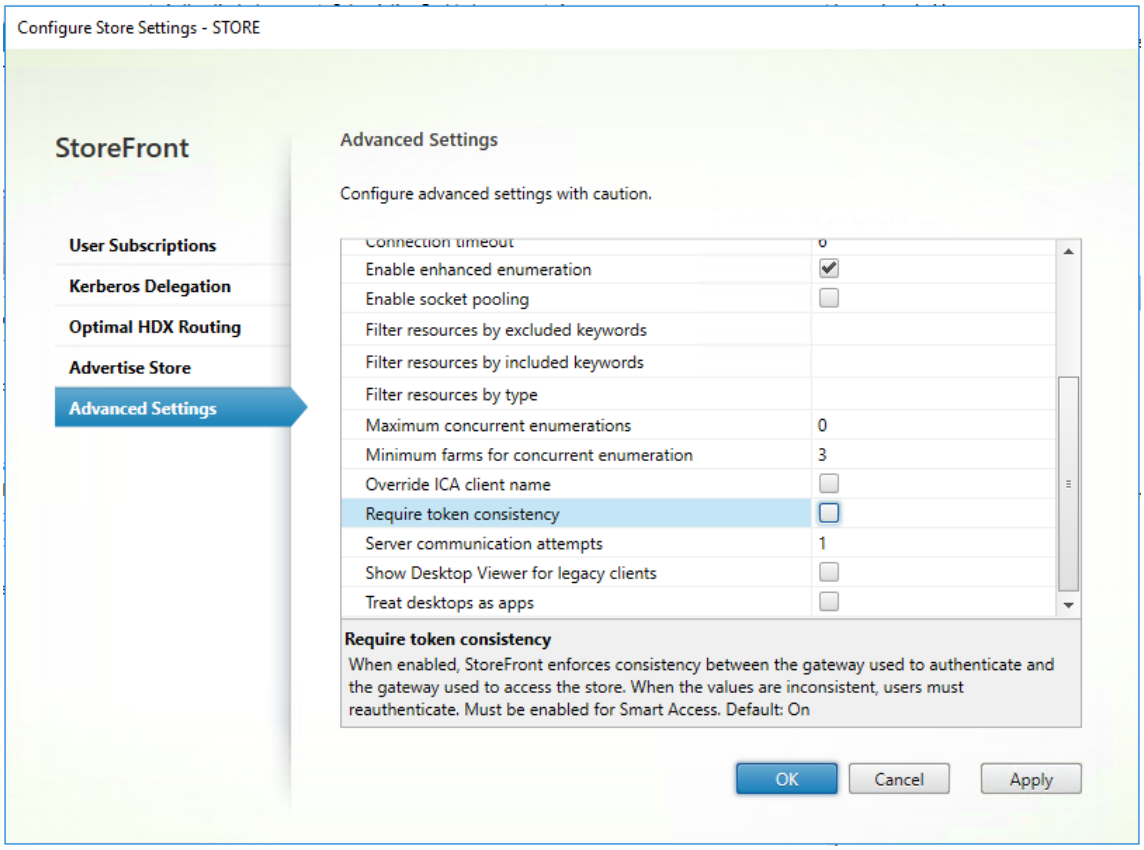
Konfigurieren des Stores für einen Remotezugriff über Gateway

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 Citrix Gateway beim Store registriert haben. Wenn Citrix 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**.



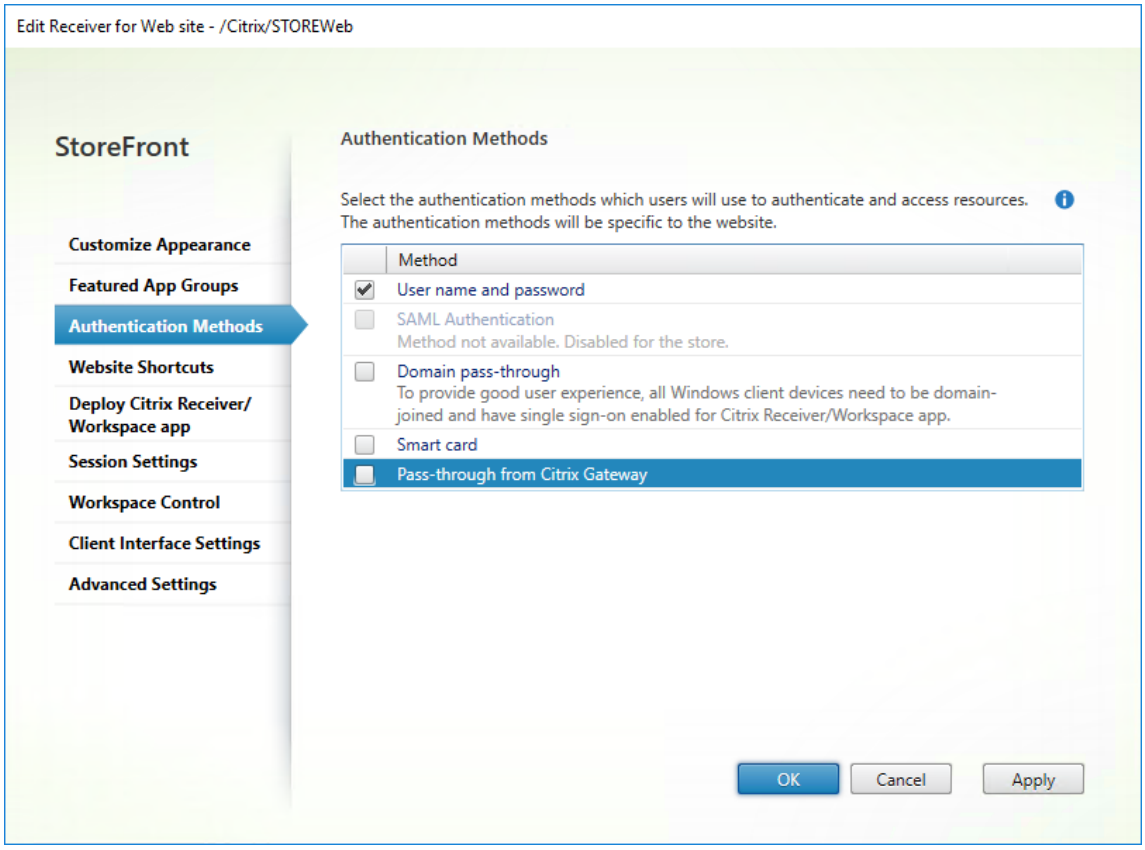
> Hinweis:
>
> Die Einstellung “Tokenkonsistenz erforderlich” ist standardmäßig aktiviert. Wenn Sie diese Einstellung deaktivieren, funktionieren SmartAccess-Features für die Citrix ADC-Endpunktanalyse (EPA) nicht mehr. Weitere Informationen zu SmartAccess finden Sie unter CTX138110.

Deaktivieren der Passthrough-Authentifizierung von Citrix Gateway für die Receiver für Web-Site

> **Wichtig:**
>
> Durch Deaktivieren der Passthrough-Authentifizierung von Citrix Gateway wird verhindert, dass Receiver für Web die falschen Anmeldeinformationen der Domäne `production.com` verwendet, die vom Citrix ADC-Gerät weitergegeben werden. Bei deaktivierter Passthrough-Authentifizierung von Citrix Gateway wird der Benutzer von Receiver für Web zur Eingabe der Anmeldeinformationen aufgefordert. Diese Anmeldeinformationen unterscheiden sich von den Anmeldeinformationen, die zur Anmeldung über Citrix Gateway verwendet werden.

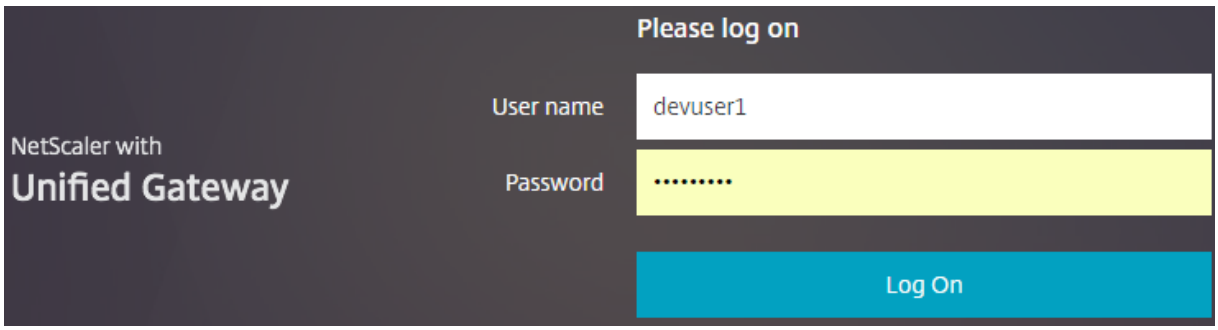
1. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores**.
2. Wählen Sie den **Store** aus, den Sie ändern möchten.
3. Klicken Sie im Bereich **Aktionen** auf **Receiver für Web-Sites verwalten**.

4. Deaktivieren Sie unter “Authentifizierungsmethoden” **Passthrough-Authentifizierung von Citrix Gateway**.
5. Klicken Sie auf **OK**.

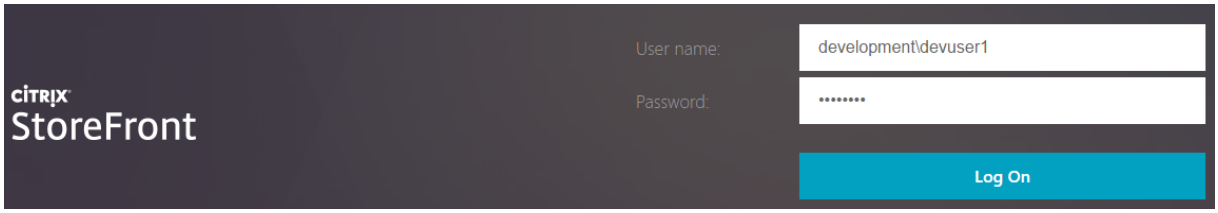


Melden Sie sich beim Gateway mit einem Benutzerkonto und Anmeldeinformationen von `production.com` an

Zum Testen melden Sie sich beim Gateway mit einem Benutzerkonto und Anmeldeinformationen von `production.com` an.



Nach der Anmeldung wird der Benutzer aufgefordert, die Anmeldeinformationen von `development.com` einzugeben.

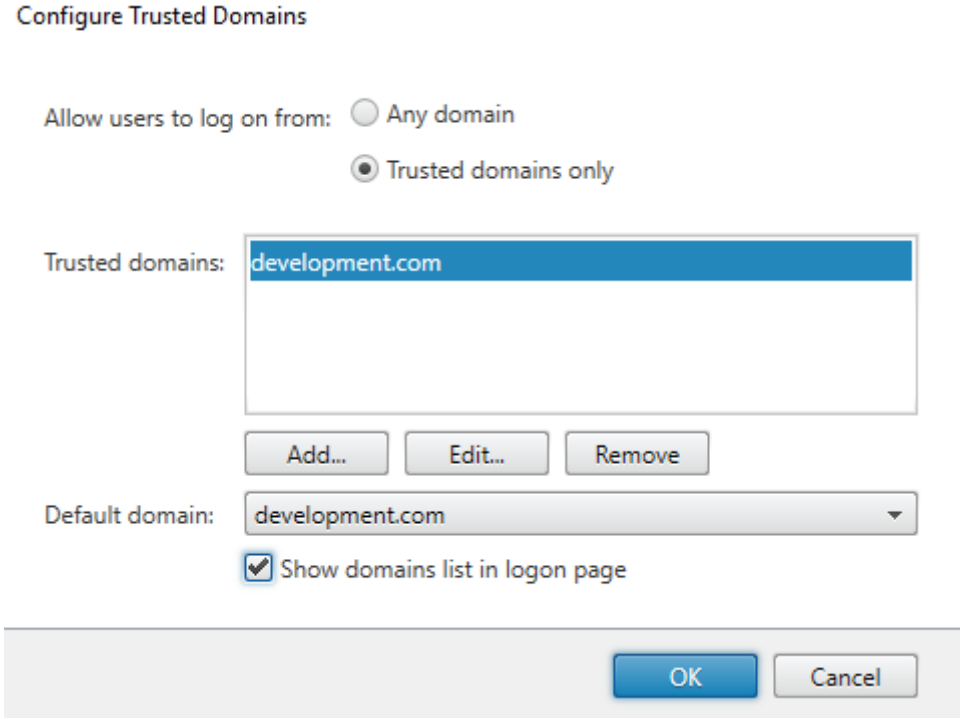


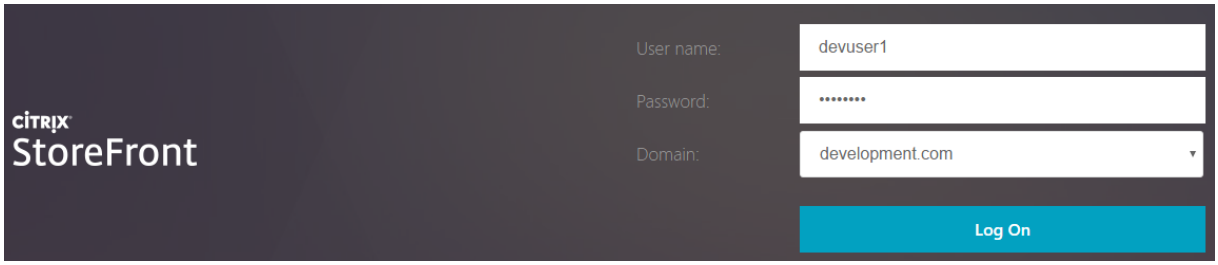
Hinzufügen einer Dropdownliste vertrauenswürdiger Domänen in StoreFront (optional)

Mit dieser optionalen Einstellung kann verhindert werden, dass Benutzer versehentlich die falsche Domäne zur Authentifizierung über Citrix Gateway eingeben.

Wenn der Benutzername für beide Domänen gleich ist, ist die Eingabe der falschen Domäne wahrscheinlicher. Neue Benutzer sind außerdem evtl. gewohnt, bei der Anmeldung über Citrix Gateway keine Domäne 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**.

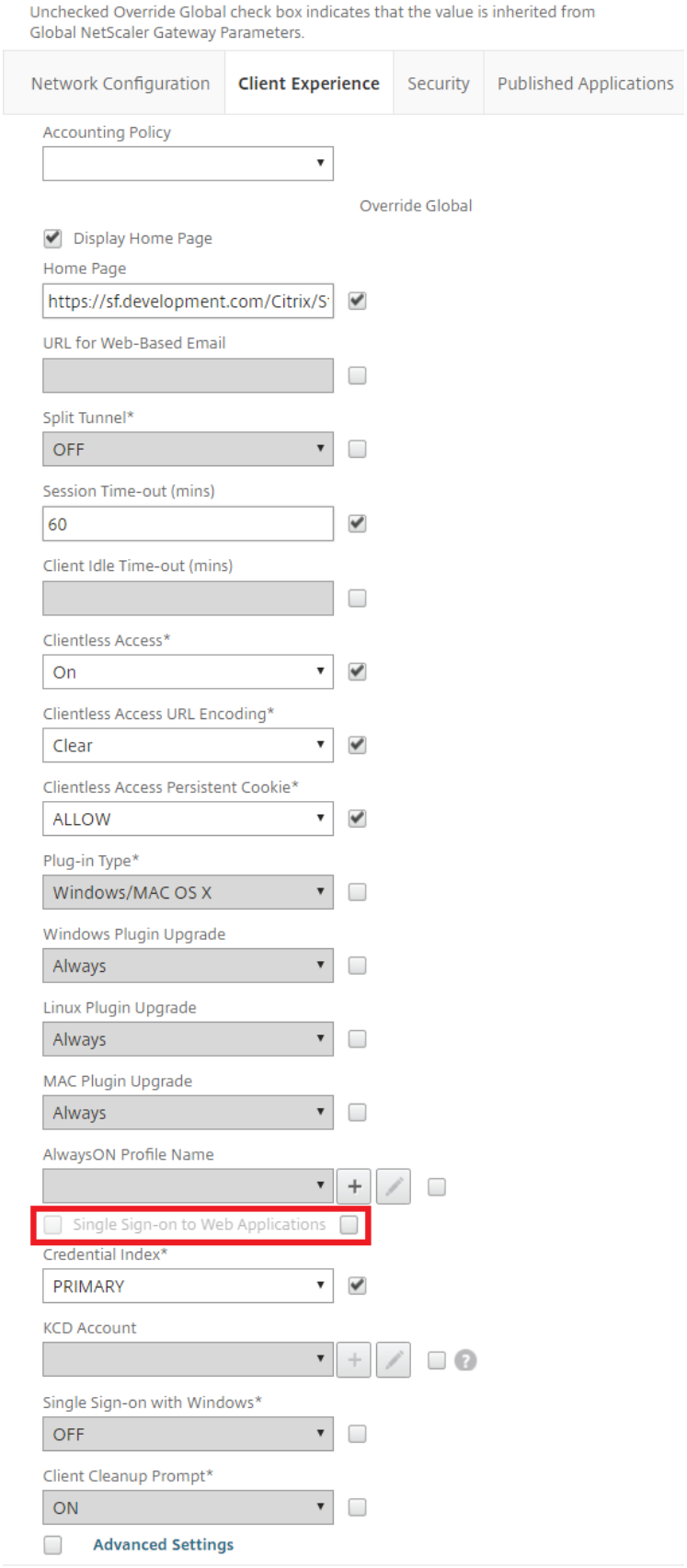


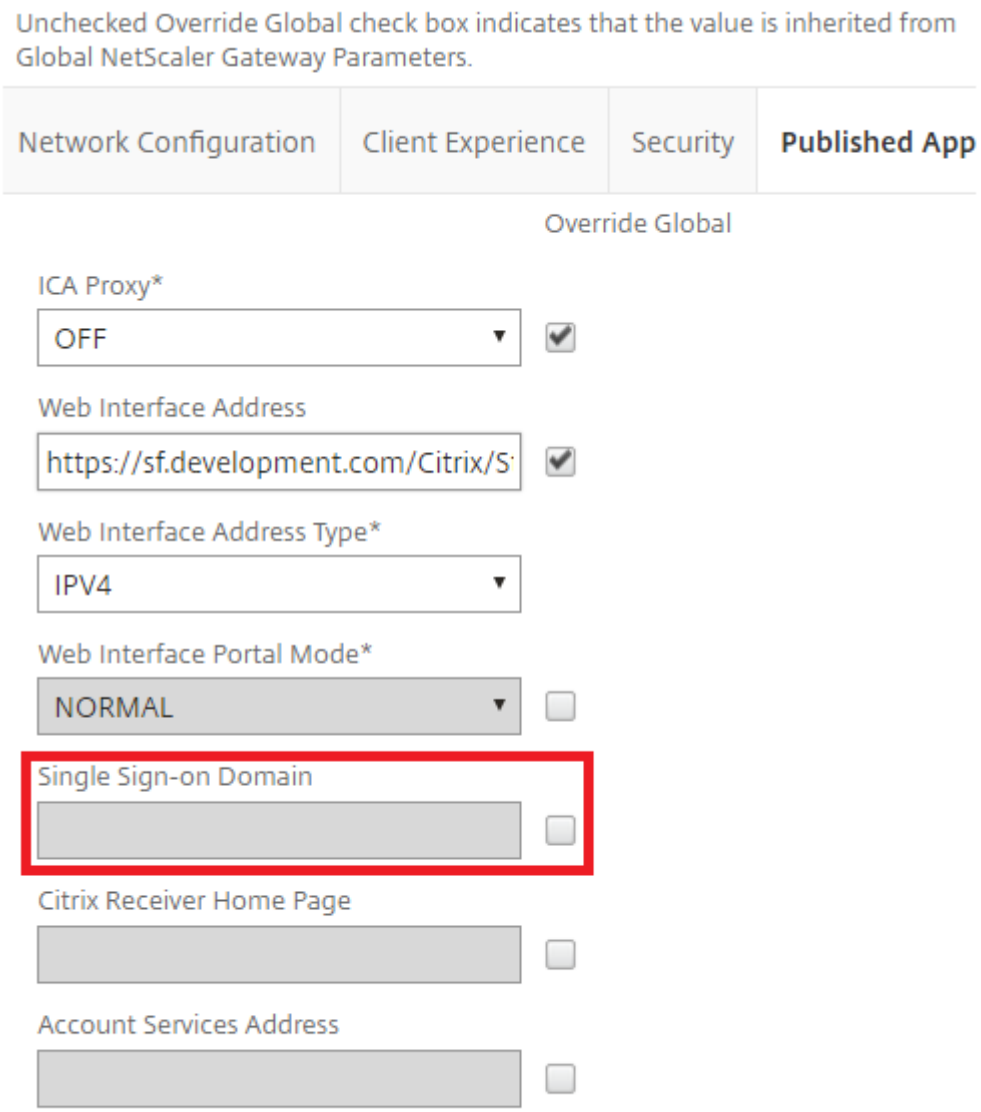


> **Hinweis:**
>
> Die Kennwortzwischenspeicherung im Browser wird für dieses Authentifizierungsszenario nicht empfohlen. Wenn Benutzer unterschiedliche Kennwörter für die beiden Domänenkonten verwenden, kann die Kennwortzwischenspeicherung zu Fehlern führen.

Aktionsrichtlinie für Citrix Gateway-Sitzungen mit clientlosem VPN (CVPN)

- Wenn Single Sign-On für Webanwendungen in der Citrix Gateway-Sitzungsrichtlinie aktiviert ist, ignoriert Receiver für Web falsche Anmeldeinformationen, die vom Citrix ADC-Gerät gesendet wurden, da die Authentifizierungsmethode **Passthrough-Authentifizierung von Citrix 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” auf dem Citrix ADC-Gerät ändert nicht das in diesem Artikel beschriebene Verhalten.





Konfigurieren von Beacons

January 30, 2020

Verwenden Sie die Aufgabe “Beacons verwalten”, um URLs innerhalb und außerhalb des internen Netzwerks anzugeben, die als Beacons verwendet werden sollen. Die Citrix Workspace-App 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 die Citrix Workspace-App zurückgegeben werden können. Dadurch wird sichergestellt, dass die Benutzer nicht aufgefordert werden, sich neu anzumelden, 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 die Citrix Workspace-App 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 sich der Benutzer über Citrix Gateway mit Desktops und Anwendungen verbinden. Wenn ein Benutzer auf einen Desktop oder eine Anwendung zugreift, wird der Server mit der Ressource benachrichtigt, um Details zum Citrix 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 Citrix Gateway-Bereitstellung werden standardmäßig als externe Beacons verwendet.

Wenn Sie Beacons ändern, müssen Sie sicherstellen, dass die Benutzer die Citrix Workspace-App mit den geänderten Beaconinformationen aktualisieren. Bei der Konfiguration einer Receiver für Web-Site für einen Store können die Benutzer eine aktualisierte Citrix Workspace-App-Provisioningdatei von der Site beziehen. Andernfalls können Sie eine Provisioningdatei 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. Navigieren Sie auf der Windows-Startseite oder auf der Apps-Seite zur 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 an, die als interner Beacon verwendet werden soll.
    - 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 die Citrix Workspace-App 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.

Erstellen eines einzelnen vollqualifizierten Domänennamens (FQDN) für den internen und externen Zugriff auf einen Store

April 1, 2020

Sie können Zugriff auf Ressourcen aus dem Unternehmensnetzwerk und aus dem Internet durch ein Citrix 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 die Citrix Workspace-App

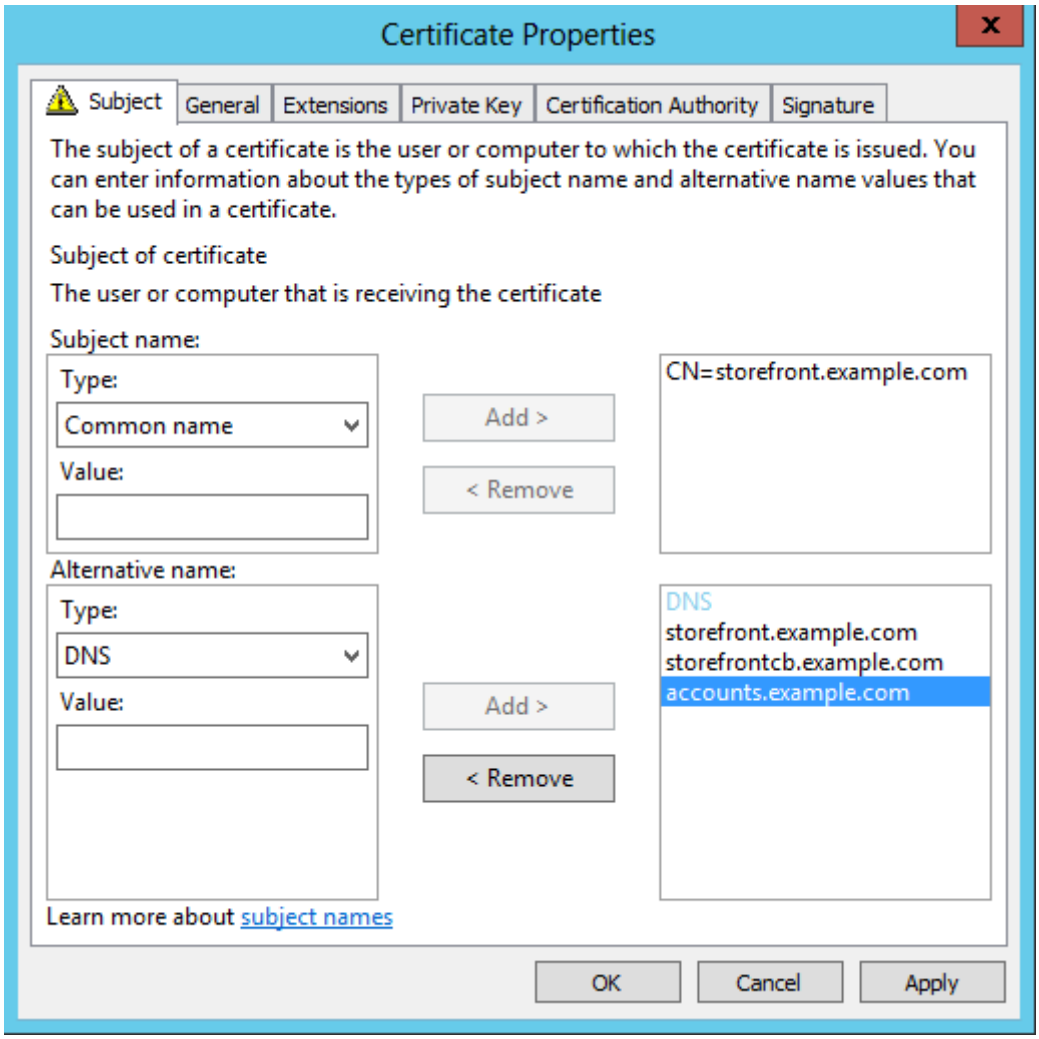
Die Citrix Workspace-App versucht eine Kontaktaufnahme mit den Beacons und ermittelt anhand der Antworten, ob Benutzer mit lokalen oder öffentlichen Netzwerken verbunden sind. Wenn ein Benutzer auf einen Desktop oder eine Anwendung zugreift, werden die Standortinformationen an den Server mit der Ressource weitergegeben, sodass die entsprechenden Verbindungsinformationen an die Citrix Workspace-App zurückgegeben werden können. Dadurch wird sichergestellt, dass die Benutzer nicht aufgefordert werden, sich neu anzumelden, wenn sie auf einen Desktop oder eine Anwendung zugreifen. Weitere Informationen zur Konfiguration von Beacons finden Sie unter Konfigurieren von Beacons.

> Hinweis:
>
> In diesem Artikel gelten die Erläuterungen zur Citrix Workspace-App, sofern nicht anders angegeben, auch für die unterstützten Versionen von Citrix Receiver.

Konfigurieren des virtuellen Citrix 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 Citrix 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. Wenn Sie eine Stammzertifizierungsstelle von Drittanbietern wie Verisign anstelle einer Unternehmenszertifizierungsstelle zum Signieren des Gatewayzertifikats verwenden, vertraut jeder externe Client automatisch dem an den Gateway vServer gebundenen Zertifikat. Wenn Sie eine Stammzertifizierungsstelle eines Drittanbieters wie Verisign verwenden, müssen keine zusätzlichen Stammzertifizierungsstellenzertifikate auf externen Clients importiert werden.

Überlegen Sie beim Bereitstellen eines einzelnen Zertifikats mit dem Common Name des gemeinsamen FQDN für Citrix Gateway und den StoreFront-Server, ob Sie Remoteerkennung unterstützen möchten. Falls ja, muss das Zertifikat der Spezifikation für alternative Antragstellernamen entsprechen.



Beispielzertifikat eines virtuellen Citrix Gateway-Servers: `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 Citrix Gateway importiert werden können.
3. Stellen Sie sicher, dass "Default Authorization" auf "Allow" festgelegt ist.
4. Unterzeichnen Sie das Zertifikat mit einer Drittanbieterzertifizierungsstelle, z. B. Verisign, oder einer Unternehmensstammzertifizierungsstelle für Ihre Organisation.

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 Citrix Gateway-Servers durch eine Zertifizierungsstelle

Je nach Anforderungen haben Sie für den Typ des von einer Zertifizierungsstelle signierten Zertifikats zwei Möglichkeiten zur Auswahl.

- 1. Von einer Drittanbieter-Zertifizierungsstelle signiertes Zertifikat: Wenn das an den virtuellen Citrix 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 Citrix 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. Wenn Sie tragbare Geräte mit nativem Receiver wie z. B. iPhones und iPads verwenden, erstellen Sie auf diesen Geräten ein Sicherheitsprofil.

Importieren des Stammzertifikats auf mobilen Geräten

- iOS-Geräte können .CER x.509-Zertifikatsdateien über E-Mail-Anhänge importieren. Der Zugriff auf den lokalen Speicher von iOS-Geräten ist anders normalerweise nicht möglich.
- Android-Geräte benötigen dasselbe .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 Citrix 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 Citrix Gateway

WinSCP ist ein nützliches und kostenloses Drittanbietertool zum Verschieben von Dateien von einer Windows-Maschine in ein Citrix Gateway-Dateisystem. Kopieren Sie Zertifikate für den Import in den Ordner /nsconfig/ssl/ im Citrix Gateway-Dateisystem. Sie können OpenSSL-Tools auf dem Citrix Gateway-Gerät verwenden, um das Zertifikat und den Schlüssel aus einer PKCS12/PFX-Datei zu extrahieren, um zwei separate CER- und KEY X.509-Dateien im PEM-Format zu erstellen, die Citrix Gateway verwenden kann.

1. Kopieren Sie die PFX-Datei in den Ordner /nsconfig/ssl auf dem Citrix Gateway-Gerät in VPX.
2. Öffnen Sie die Citrix Gateway-Befehlszeilenschnittstelle.
3. Zum Wechseln in die FreeBSD-Shell geben Sie **Shell** ein, um die Citrix Gateway-Befehlszeilenschnittstelle zu verlassen.
4. Verwenden Sie `cd /nsconfig/ssl`, um das Verzeichnis zu wechseln.
5. Führen Sie `openssl pkcs12 -in <imported cert file>.pfx -nokeys -out <certfilename>.cer` aus und geben Sie auf Aufforderung das PFX-Kennwort ein.
6. Führen Sie `openssl pkcs12 -in <imported cert file>.pfx -nocerts -out <keyfilename>.key`

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. Um sicherzustellen, dass die CER- und die KEY-Datei erfolgreich erstellt wurden, führen Sie in /nsconfig/ssl/ den Befehl ls `ls -al` aus.
9. Geben Sie Exit ein, um zur Citrix Gateway-Befehlszeilenschnittstelle zurückzukehren.

Citrix Gateway-Sitzungsrichtlinie für Citrix Receiver für Windows oder Citrix Receiver für Mac

REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver && REQ.HTTP.HEADER X-Citrix-Gateway EXISTS

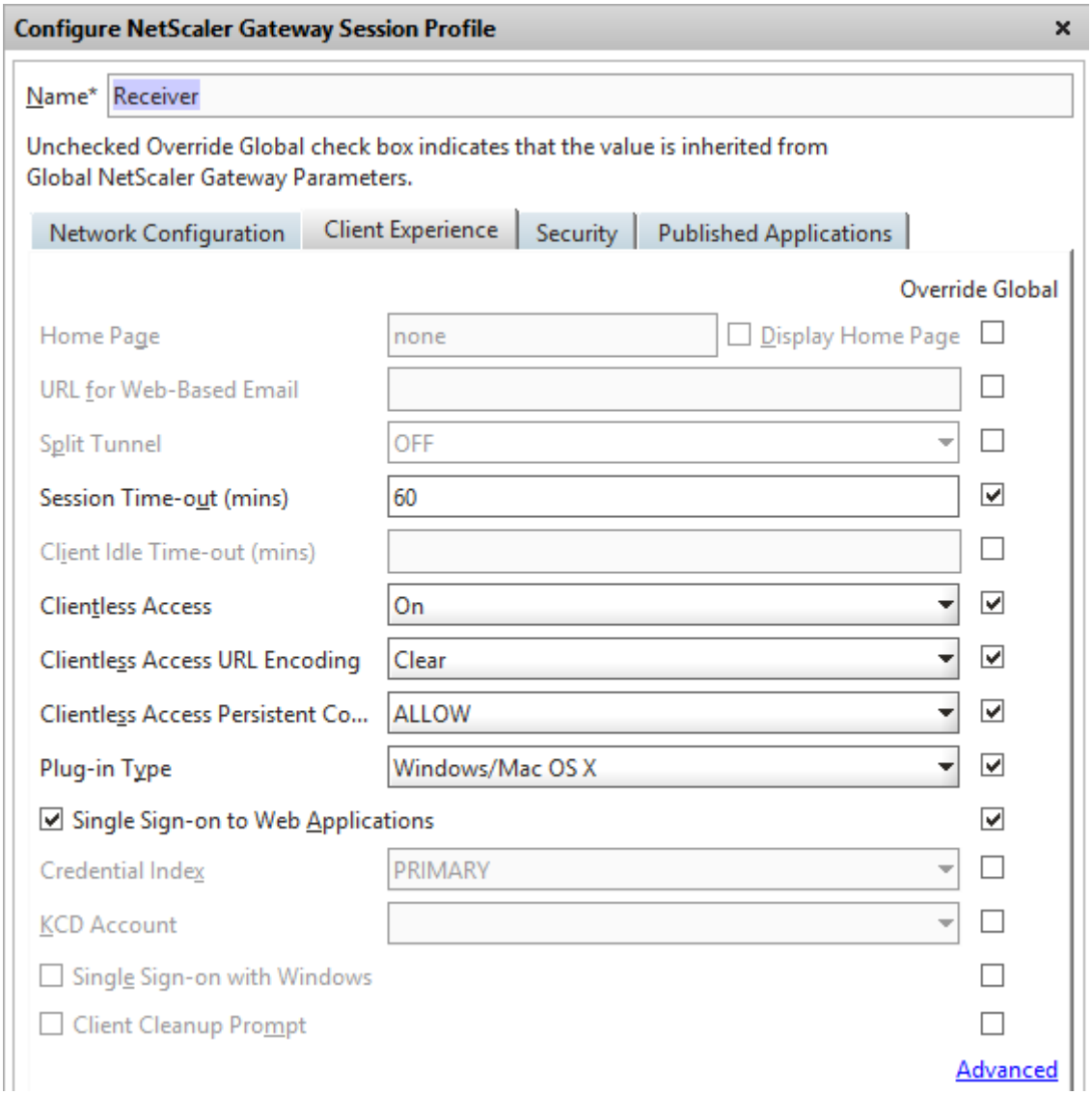
Sitzungsrichtlinie für Receiver für Web

REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver && REQ.HTTP.HEADER Referer EXISTS

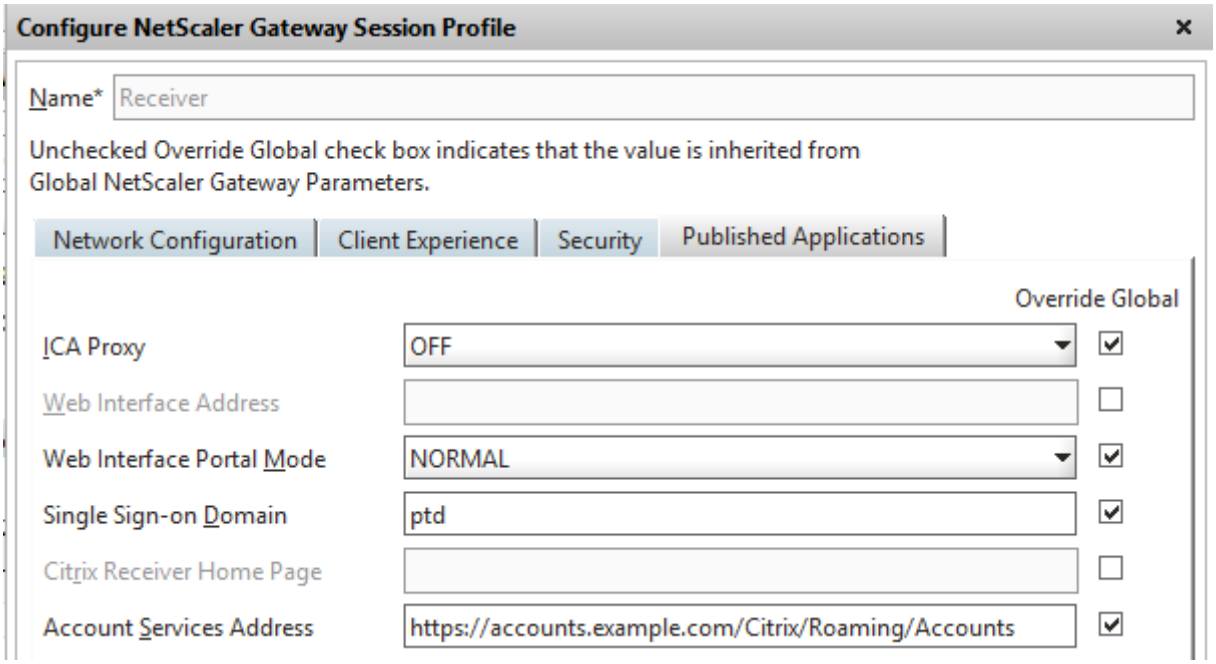
CVPN- und SmartAccess-Einstellungen

Wenn Sie SmartAccess verwenden, aktivieren Sie den SmartAccess-Modus auf der Eigenschaftenseite des virtuellen Citrix Gateway-Servers. Für jeden gleichzeitigen Benutzer, der auf Remoteressourcen zugreift, ist eine universelle Lizenz erforderlich.

Receiver-Profil

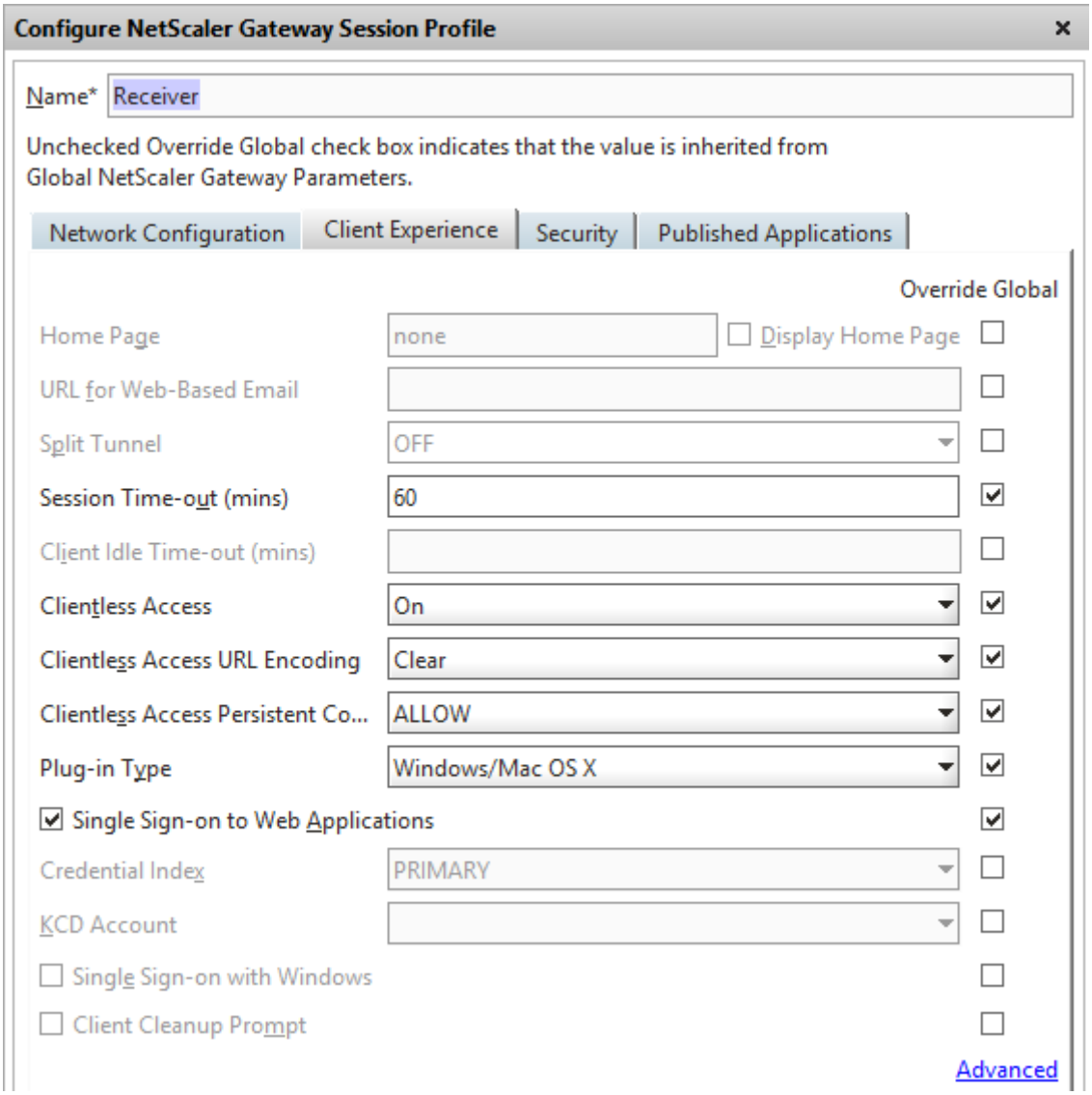


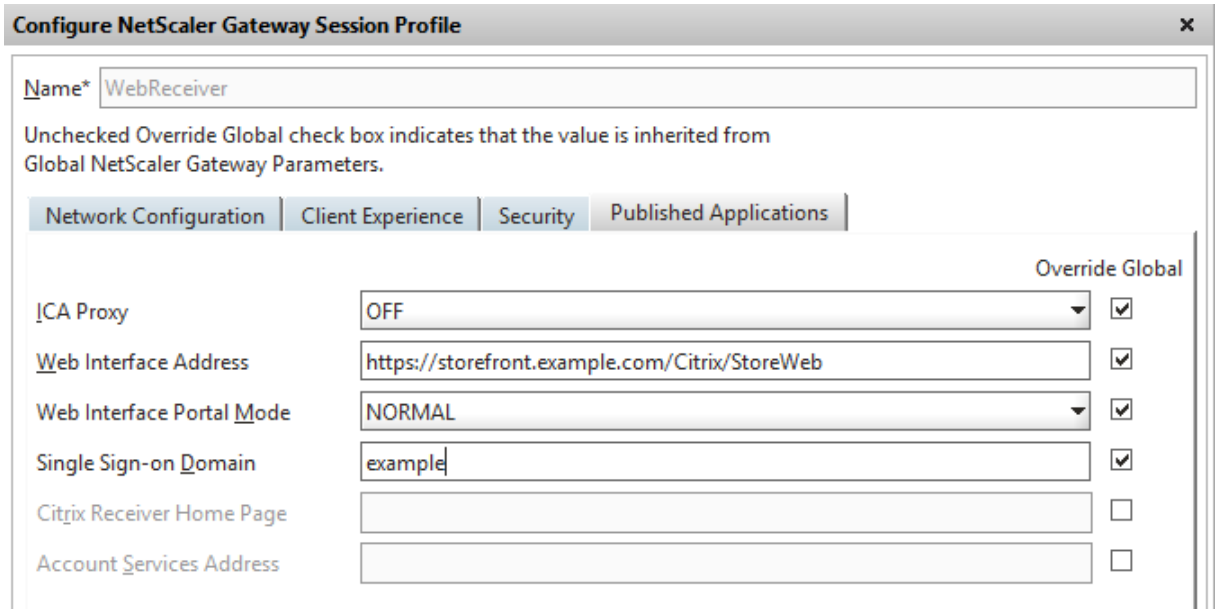
Konfigurieren Sie die Kontodienst-URL für das Sitzungsprofil so, dass sie `https://accounts.example.com/Citrix/Roaming/Accounts` lautet und NICHT `https://storefront.example.com/Citrix/Roaming/Accounts`.



Fügen Sie diese URL zusätzlich auch 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

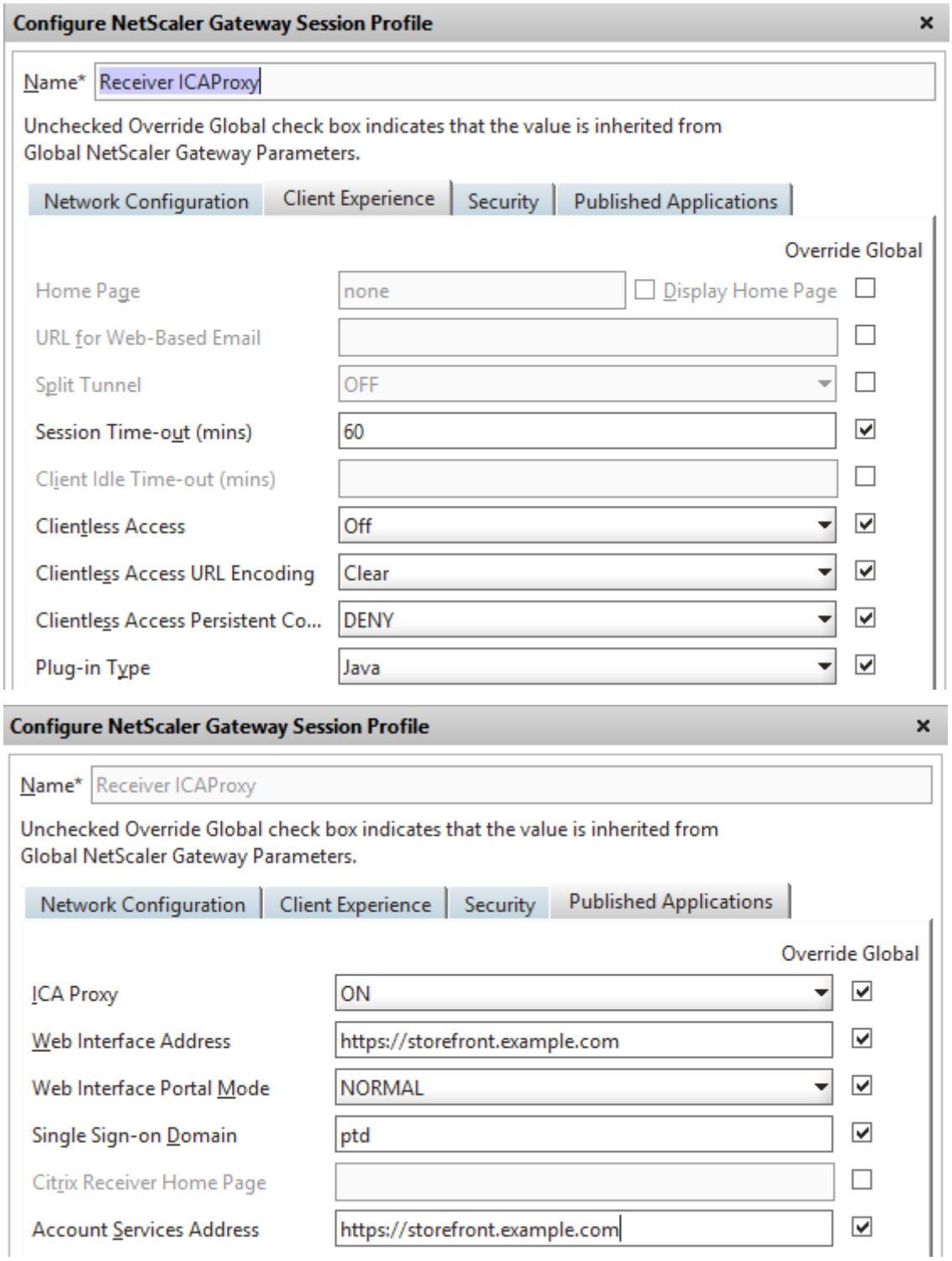




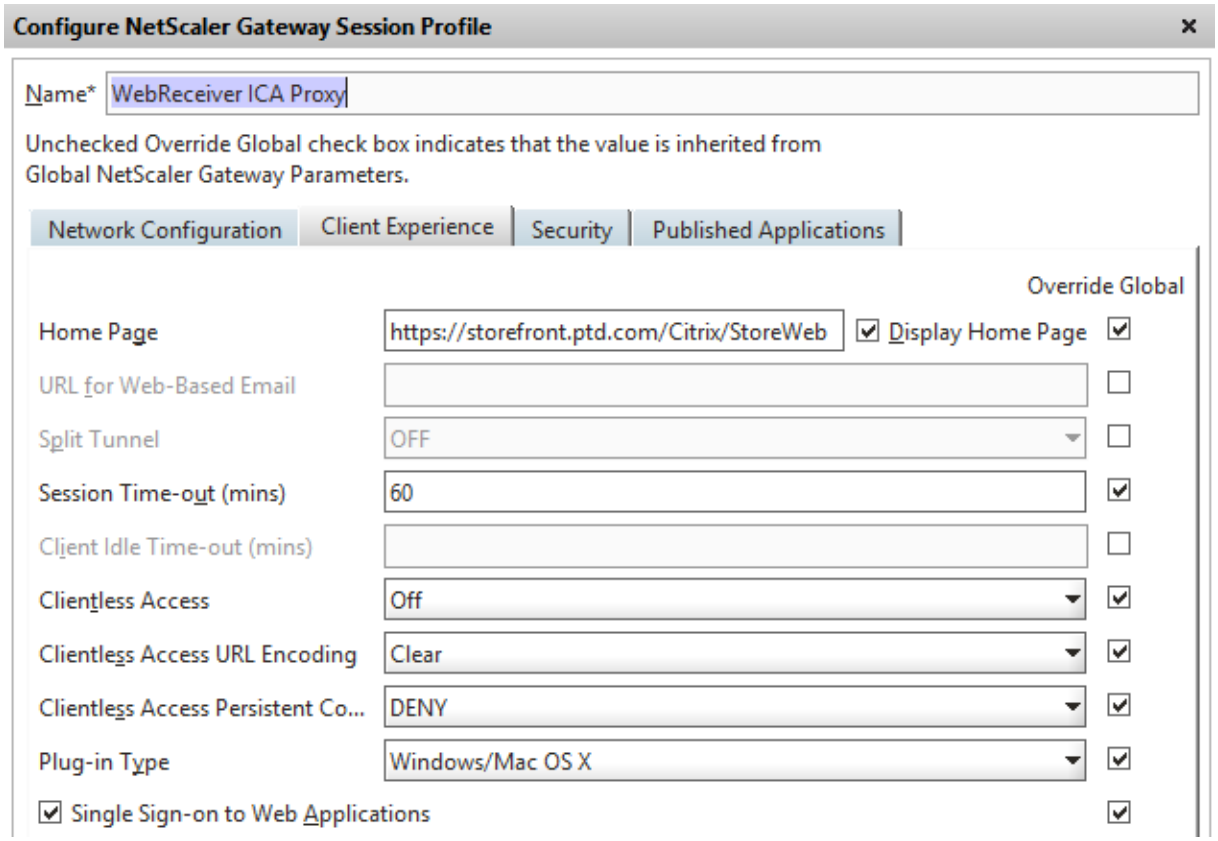
ICA-Proxy-Einstellung und Moduseinstellung “Basic”

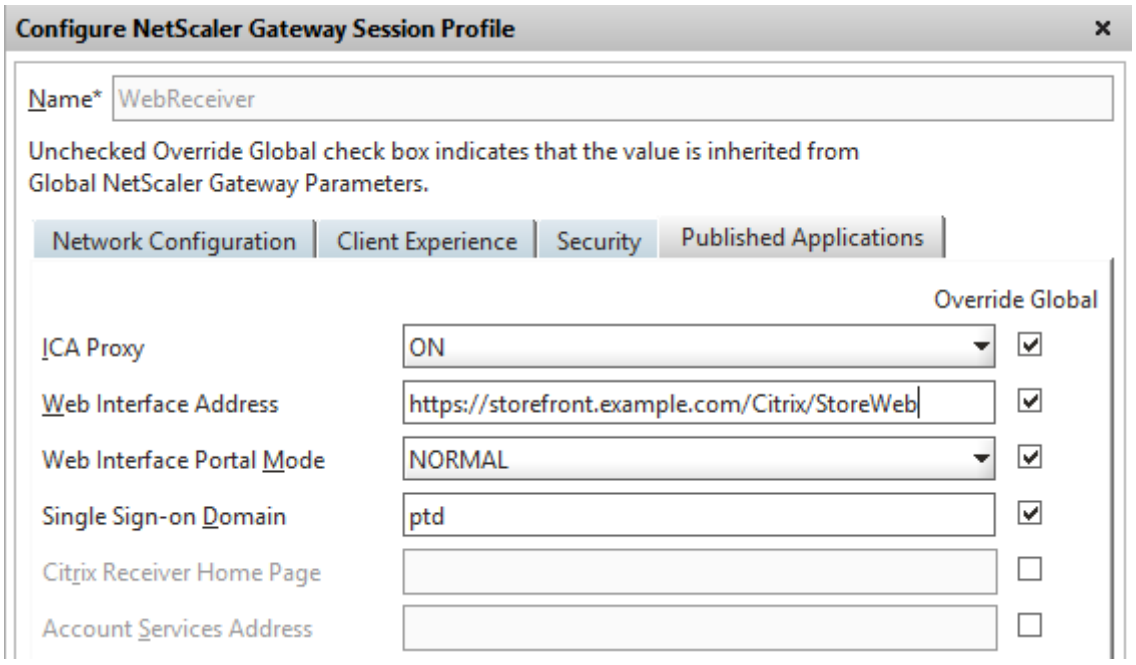
Wenn Sie den ICA-Proxy verwenden, aktivieren Sie den Modus “Basic” auf der Eigenschaftenseite des virtuellen Citrix Gateway-Servers. Es ist nur eine Citrix ADC-Plattformlizenz erforderlich.

Receiver-Profil



Receiver für Web-Profil





Konfigurieren der Hostbasis-URL des StoreFront-Servers, des Gateways und des SSL-Zertifikats

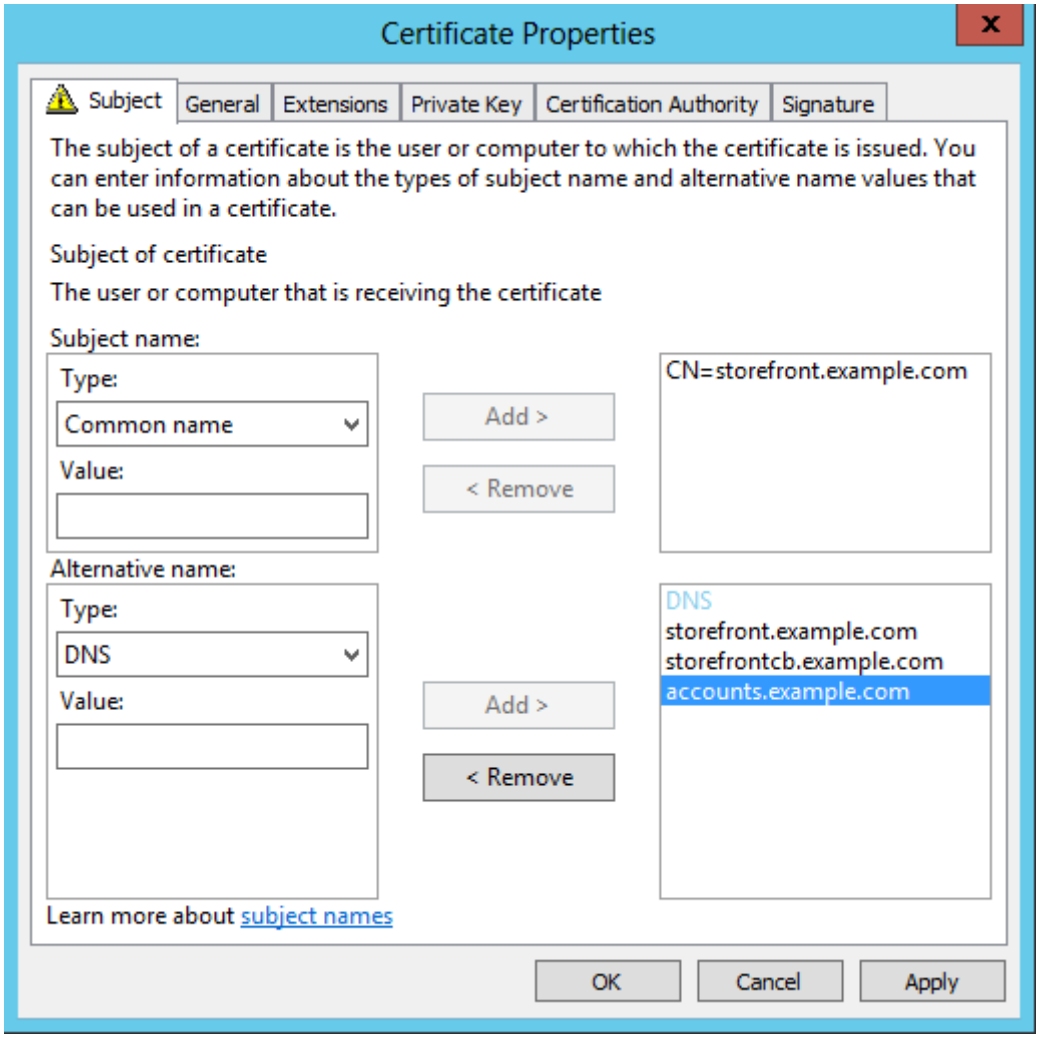
Wenn ein StoreFront-Cluster oder eine einzelne StoreFront-IP zum Hosten des Stores erstellt wurde, muss der gemeinsame FQDN, der in den virtuellen Citrix Gateway-Server aufgelöst wird, auch direkt in den StoreFront-Load Balancer aufgelöst werden.

Internes DNS: Erstellen Sie drei DNS Alias-Datensätze

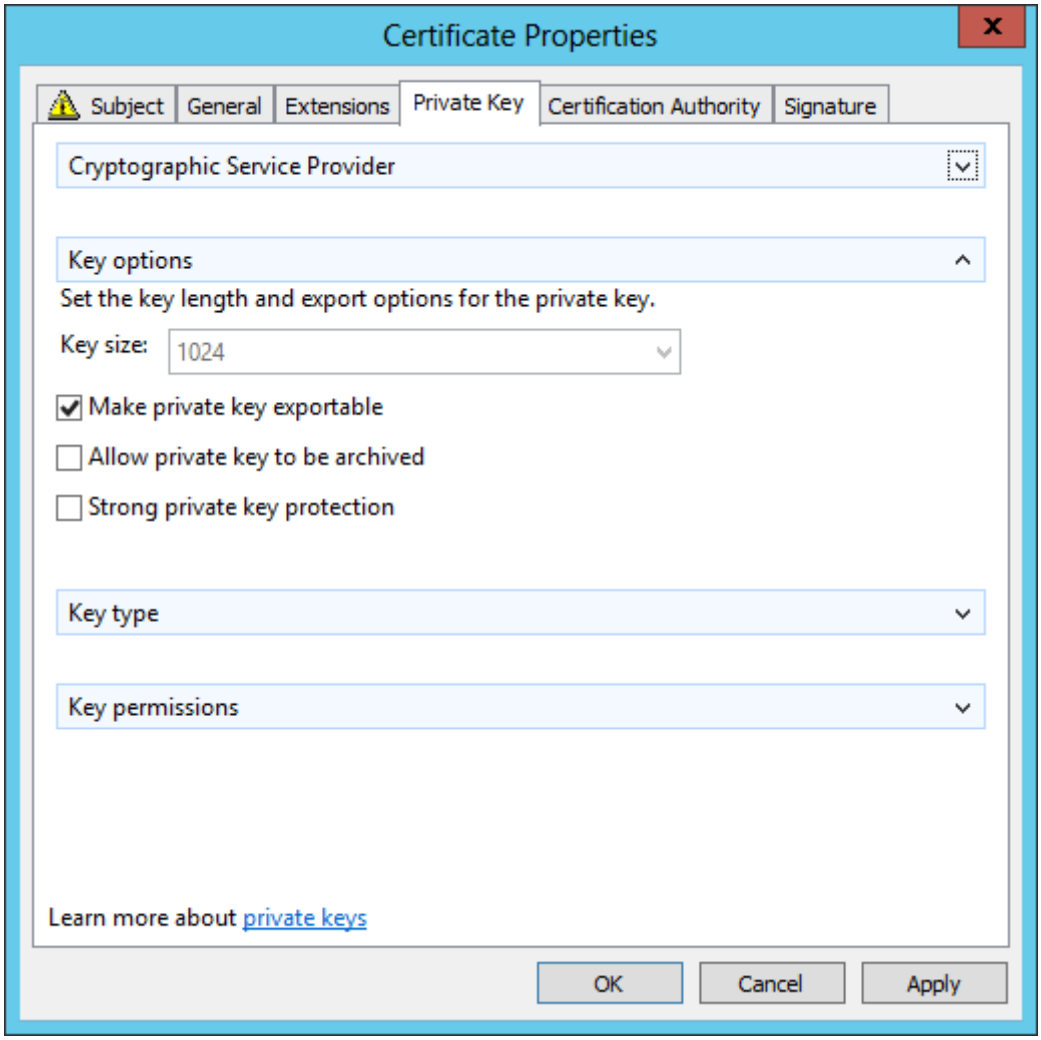
- storefront.example.com muss in den StoreFront-Load Balancer bzw. die IP des einzelnen StoreFront-Servers aufgelöst werden.
- storefrontcb.example.com muss in die virtuelle IP-Adresse des virtuellen Gatewayservers aufgelöst werden. Treffen Sie daher entsprechende Vorkehrungen, wenn zwischen DMZ und 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

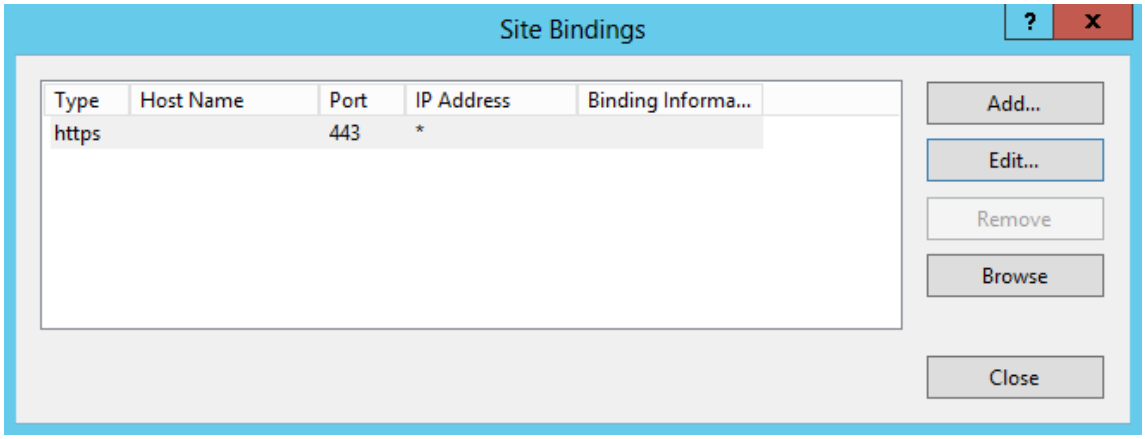
1. Erstellen Sie ein geeignetes Zertifikat für den StoreFront-Server bzw. die StoreFront-Servergruppe, bevor Sie StoreFront installieren.
2. Tragen Sie den gemeinsamen FQDN in die Felder “Common Name” und “DNS” ein. Dieser muss mit dem FQDN in dem zuvor erstellten, an den virtuellen Citrix Gateway-Server gebundenen SSL-Zertifikat übereinstimmen oder verwenden Sie das gleiche an den virtuellen Citrix Gateway-Server gebundene Zertifikat.
3. Fügen Sie das Alias des Kontos (`accounts.example.com`) als weiteres SAN dem Zertifikat hinzu. Beachten Sie, dass das im SAN verwendete Kontenalias das Alias ist, das im Citrix Gateway-Sitzungsprofil in den früheren Anweisungen verwendet wird - **Native Receiver-Gatewaysitzungsrichtlinie und -profil**.



4. Stellen Sie sicher, dass der private Schlüssel exportierbar ist, damit das Zertifikat auf einen anderen Server oder auf StoreFront-Servergruppenknoten übertragen werden kann.

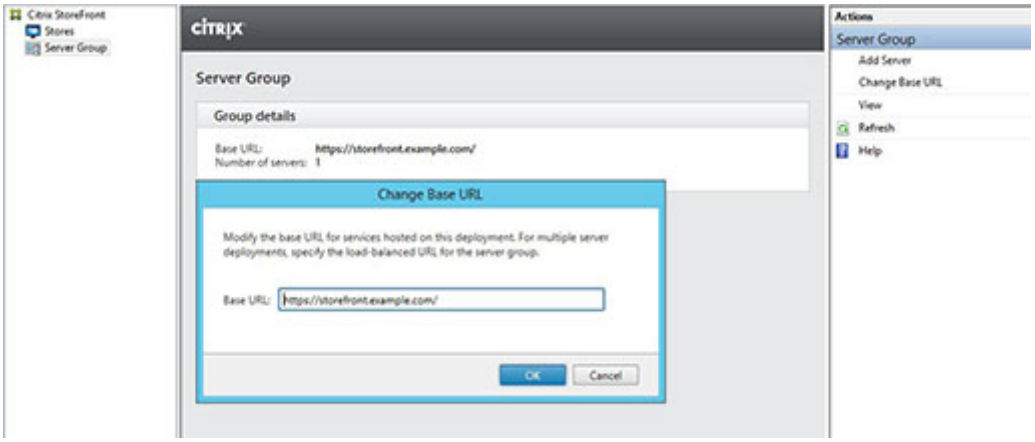


5. Unterzeichnen Sie das Zertifikat mit einer Drittanbieterzertifizierungsstelle, z. B. Verisign, dem Unternehmensstammzertifizierungsstelle für Ihre Organisation oder einer Zwischenzertifizierungsstelle.
6. Exportieren Sie das Zertifikat im PFX-Format einschließlich des privaten Schlüssels.
7. Importieren 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 Lastausgleichserver von Citrix ADC, 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, er ist im Zertifikat als SAN eingetragen. Beispiel: `https://storefront.example.com`.



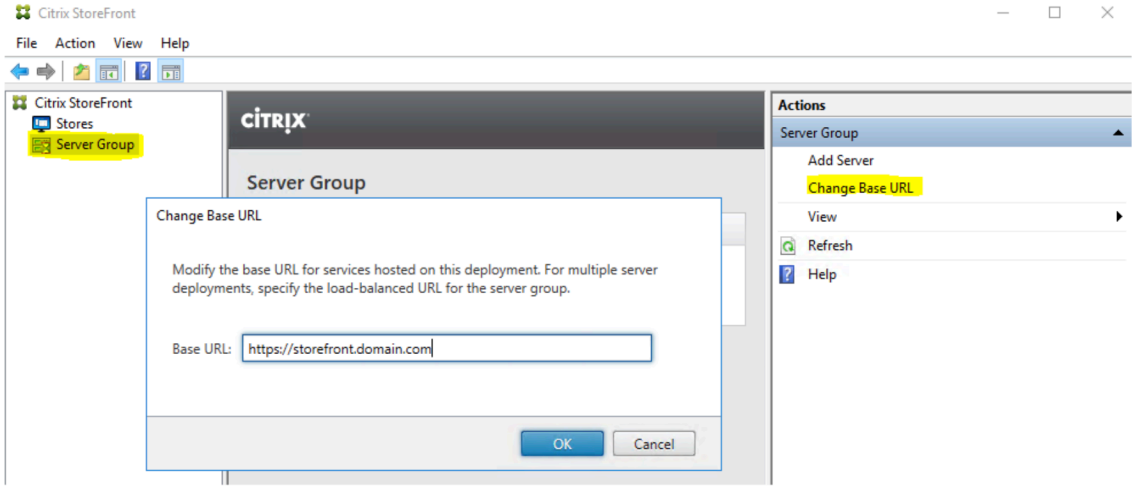
Ändern der Basis-URL des Servers von HTTP in HTTPS

Die Host-Basis-URL kann in Citrix StoreFront für Bereitstellungen mit einem Einzelserver oder mit einer Servergruppe festgelegt werden. Die Option steht Kunden zur Verfügung, die Citrix StoreFront ohne Serverzertifikat installiert und konfiguriert haben. Stellen Sie nach der Zertifikatsinstallation sicher, dass StoreFront und die zugehörigen Dienste eine sichere Verbindung verwenden.

> Hinweis:
>
> Vor dem Ausführen des Verfahrens muss vom IT-Administrator ein Serverzertifikat auf dem Citrix StoreFront-Server erstellt und installiert werden. Darüber hinaus muss eine IIS-Bindung über HTTPS (443) erstellt werden, um jede neue Verbindung zu sichern.

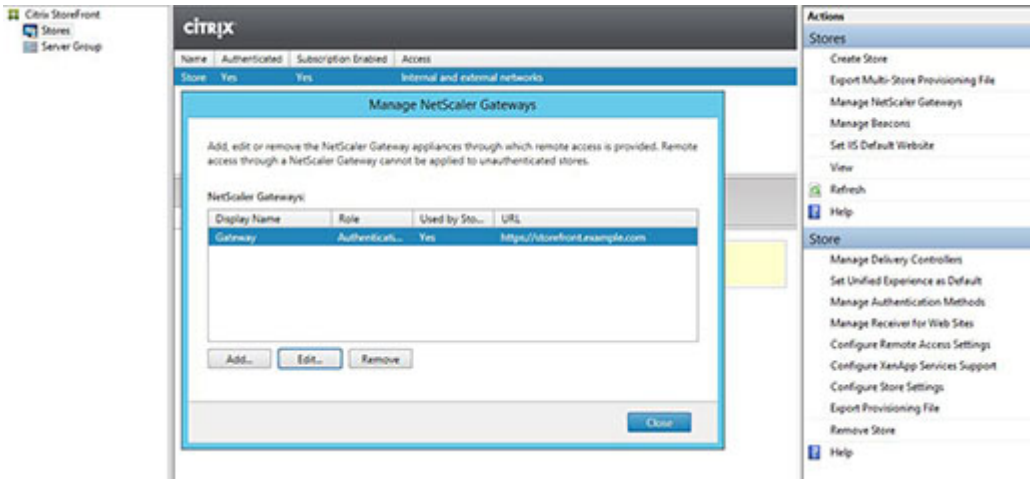
Führen Sie die folgenden Schritte aus, um die Basis-URL in StoreFront 3.x zu ändern:

1. Klicken Sie in StoreFront im linken Bereich auf **Servergruppe**.
2. Klicken Sie im rechten Bereich auf **Basis-URL ändern**.
3. Geben Sie die Basis-URL ein und klicken Sie auf **OK**.

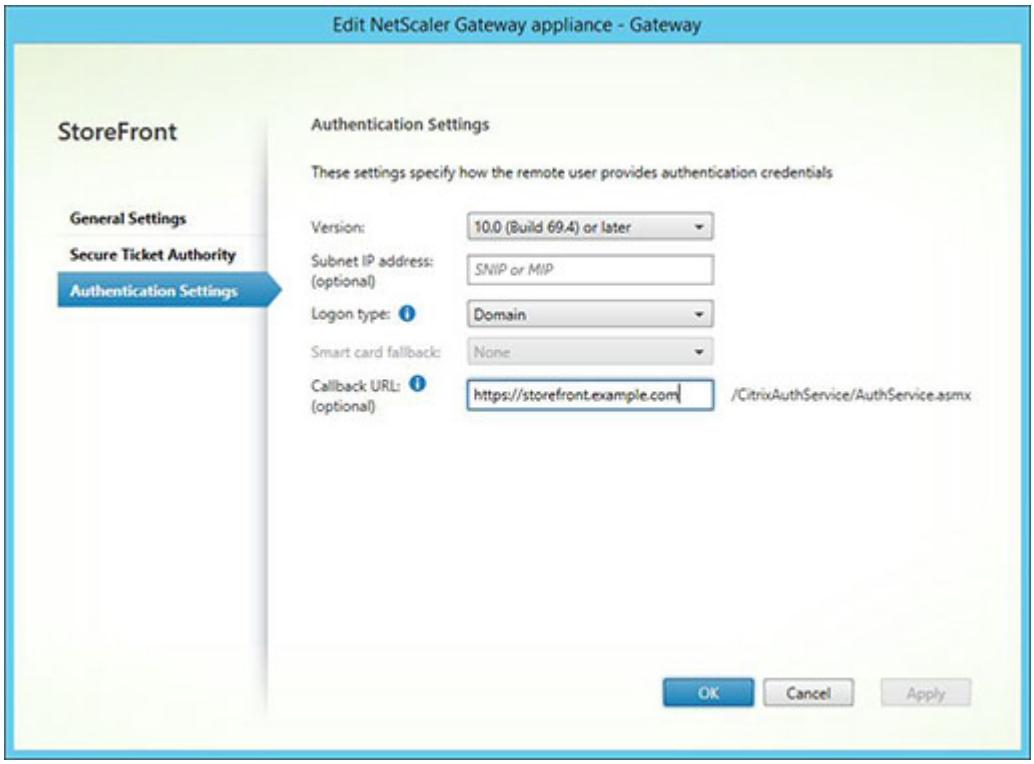


Konfigurieren Sie das Gateway auf dem StoreFront-Server: storefront.example.com

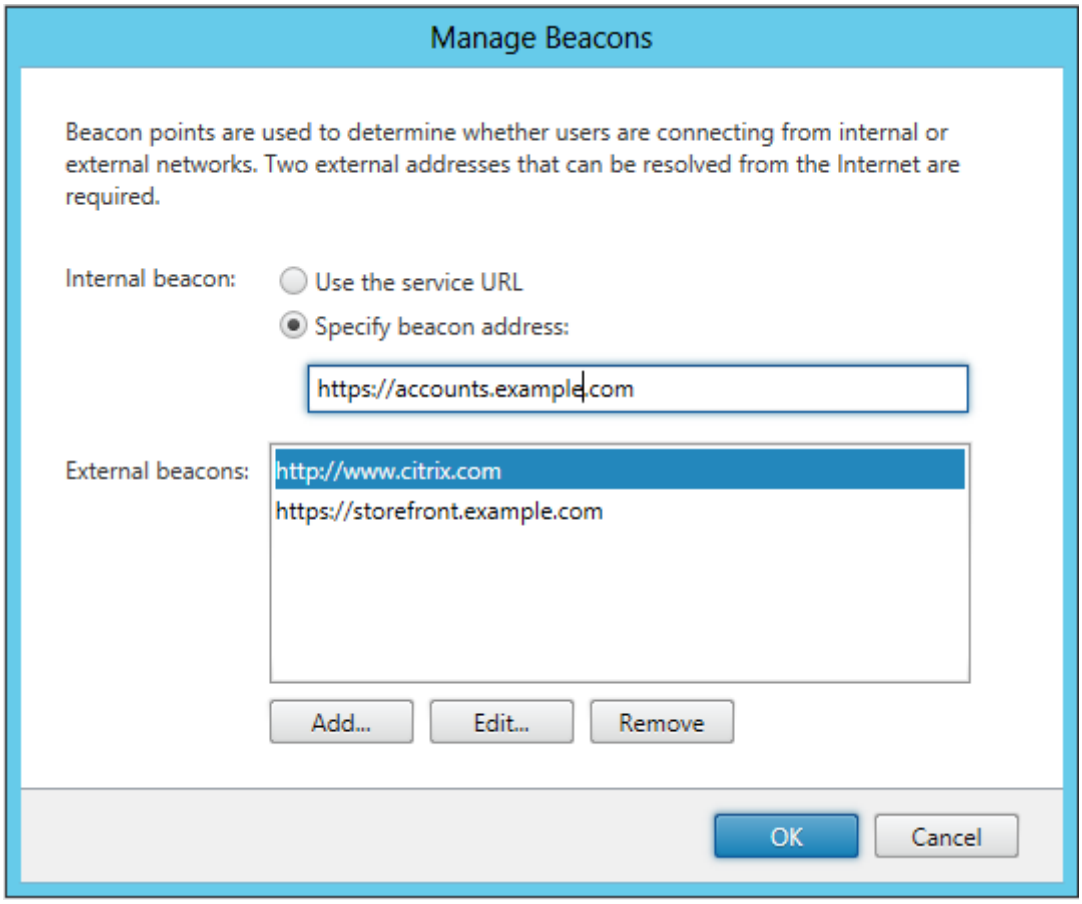
1. Klicken Sie im Knoten **Stores** im Bereich **Aktionen** auf **Citrix Gateways verwalten**.
2. Wählen Sie das **Gateway** aus der Liste aus und klicken Sie auf **Weiter**.



3. Geben Sie auf der Seite **Allgemeine Einstellungen** den gemeinsamen FQDN in das Feld **Citrix 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 Citrix 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.



Unterstützen der Erkennung per FQDN

Zum Unterstützen der Erkennung per FQDN führen Sie die nachfolgenden Schritte aus. Wenn die 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 <allowedAudiences>-Eintrag ein. Es gibt zwei <allowedAudiences>-Einträge in dieser Datei. Nur der erste "Authentication Token Producer"-Eintrag in der Datei erfordert einen zusätzlichen <allowedAudience>-Eintrag.

1. Suchen Sie im Abschnitt <service id> die Zeichenfolge <allowedAudiences>. Fügen Sie eine Zeile für audience="https://accounts.example.com/" ein (siehe Abbildung). Speichern und schließen Sie die Datei web.config.

```
<service id="abd6f54b-7d1c-4a1b-a8d7-14804e6c8c64" displayName="
    Authentication Token Producer">
...
<allowedAudiences>
<add name="https-storefront.example.com" audience="https://
    storefront.example.com/" />
```

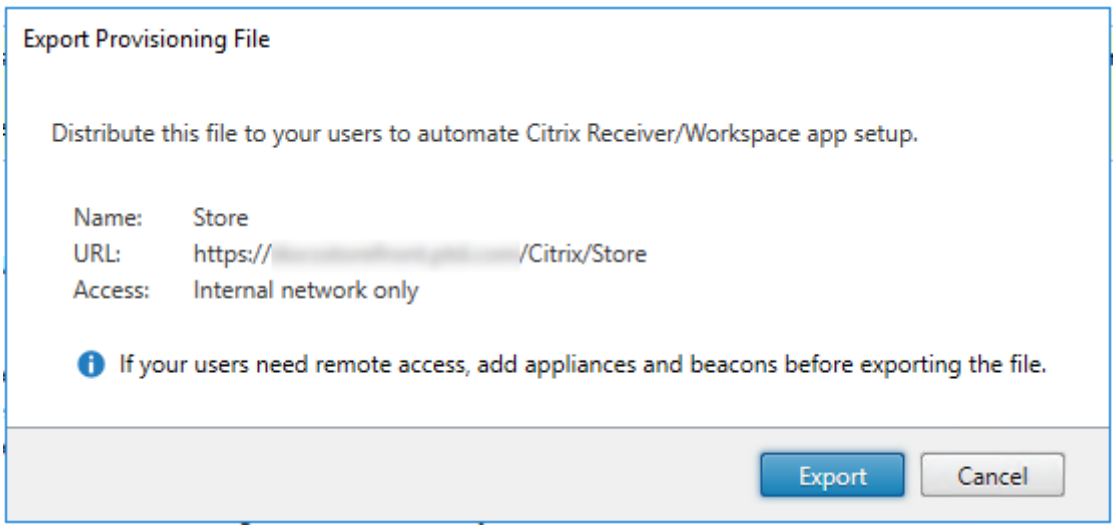


```
<add name="https-accounts.example.com" audience="https://accounts.
    example.com/" />
</allowedAudiences>
```

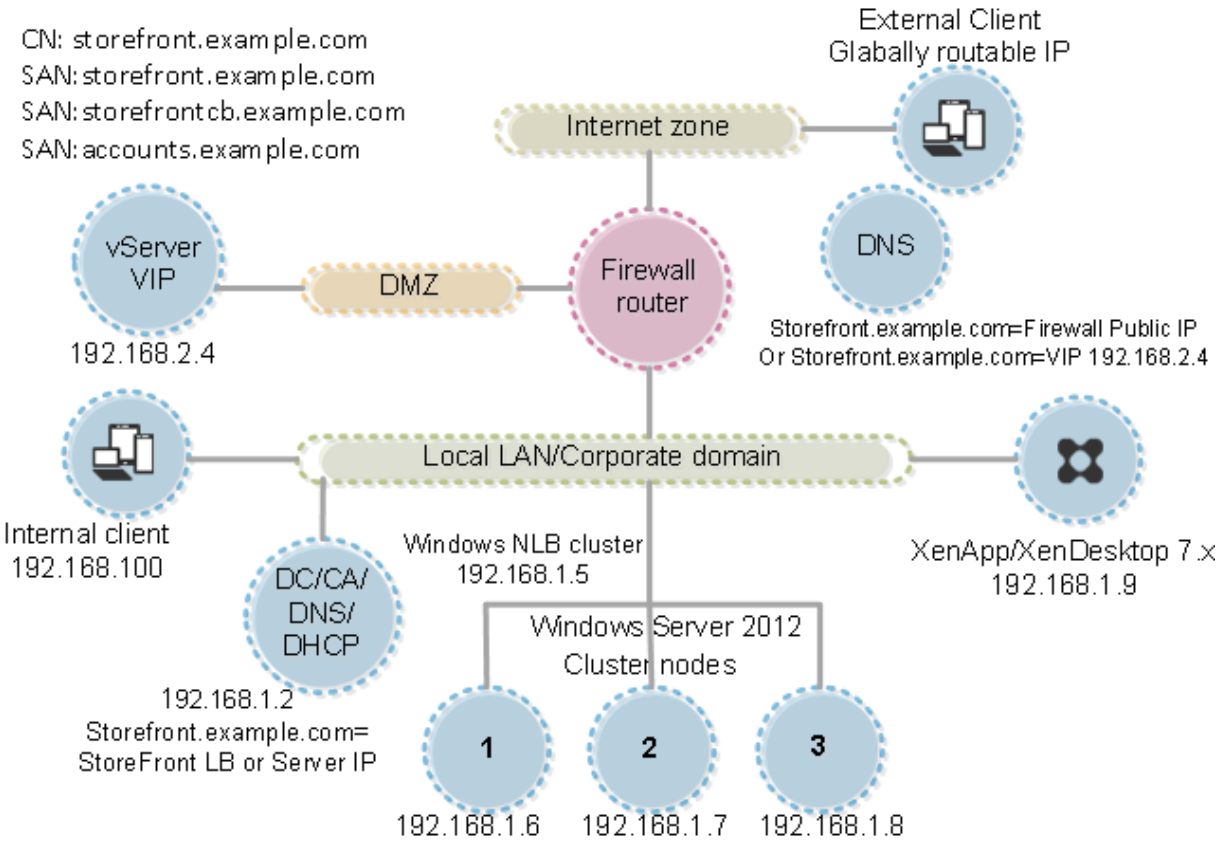
2. Suchen Sie in *C:\inetpub\wwwroot\Citrix\Roaming\web.config* den Abschnitt "<tokenManager>" und fügen Sie eine Zeile für `audience="https://accounts.example.com/"` ein (siehe Abbildung). Speichern und schließen Sie die Datei web.config.

```
<tokenManager>
<services>
<clear />
...
</trustedIssuers>
<allowedAudiences>
<add name="https-storefront.example.com" audience="https://
    storefront.example.com/" />
<add name='https-accounts.example.com" audience="https://accounts.
    example.com/" />
</allowedAudiences>
</service>
</services>
</tokenManager>
```

Alternativ können Sie die native Empfänger.CR-Bereitstellungsdatei für den Speicher exportieren. Dadurch wird die Erstverwendungs-Konfiguration der Citrix Workspace-App überflüssig. Verteilen Sie diese Datei an alle Windows- und MAC-Clients der Citrix Workspace-App.



Wenn die Citrix Workspace-App auf einem Client installiert wird, wird der CR-Dateityp erkannt und der Import der Provisioningdatei durch einen Doppelklick gestartet.



Erweiterte Konfigurationen

January 6, 2020

Sie können die folgende erweiterte Option über die StoreFront-Konsole, PowerShell, Zertifikateigenschaften oder Konfigurationsdateien konfigurieren.

Aufgabe	Detail
Konfigurieren der Ressourcenfilterung	Filtern von Enumerationsressourcen nach Ressourcentyp und Schlüsselwörtern.

Konfigurieren der Ressourcenfilterung

September 10, 2019

In diesem Abschnitt wird erläutert, wie Enumerationsressourcen nach Ressourcentyp und Schlüsselwörtern gefiltert werden können. Sie können diese Art des Filterns mit 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 siehe Citrix StoreFront SDK PowerShell Modules.

> 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:

```
1 $dsInstallProp = Get-ItemProperty ‘
2  -Path HKLM:\SOFTWARE\Citrix\DeliveryServicesManagement -Name
      InstallDir
3 $dsInstallDir = $dsInstallProp.InstallDir
4 & $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 Citrix Virtual Apps and Desktops 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
- Mandatory

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:

```
1 Set-DSResourceFilterKeyword -SiteId 1 -VirtualPath "/Citrix/Store" -
    ExcludeKeywords @("WFS")
```

Mit diesem Beispiel werden als zulässigen Ressourcentypen ausschließlich Anwendungen festgelegt:

```
1 Set-DSResourceFilterType -SiteId 1 -VirtualPath "/Citrix/Store" -
    IncludeTypes @("Applications")
```

Konfigurieren mit Konfigurationsdateien

January 6, 2020

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 Anmeldedialogfelds der Citrix Workspace-App
- Deaktivieren der Zwischenspeicherung von Kennwörtern und Benutzernamen in der Citrix Workspace-App 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

April 1, 2020

In diesem Artikel werden zusätzliche Konfigurationsaufgaben beschrieben, die nicht mit der Citrix StoreFront-Verwaltungskonsole ausgeführt werden 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.

Aktivieren der ICA-Dateisignierung

StoreFront bietet die Option, ICA-Dateien digital zu signieren, damit die Versionen der Citrix Workspace-App, 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 der Schlüssel für die digitalen Signaturen verwendet werden. 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. Informationen zum Aktivieren der ICA-Dateisignierung in der Citrix Workspace-App 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.

1. Stellen Sie sicher, dass das Zertifikat, das Sie zum Signieren von ICA-Dateien verwenden möchten, im Citrix Delivery Services-Zertifikatspeicher auf dem StoreFront-Server verfügbar ist und nicht im Zertifikatspeicher des aktuellen Benutzers.
2. Öffnen Sie die Datei web.config für den Store mit einem Texteditor. 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.

```
<certificateManager>
    <certificates>
        <clear />
        <add ... />
        ...
    </certificates>
</certificateManager>
```

4. Fügen Sie die Details des Zertifikats hinzu, das zum Signieren verwendet werden soll.

```
<certificateManager>
    <certificates>
```



```
3          <clear />
4          <add id="certificateid" thumb="certificatethumbprint" />
5          <add ... />
6      ...
7      </certificates>
8  </certificateManager>
```

Wobei **certificateid** ein Wert ist, mit dem Sie das Zertifikat in der Storekonfigurationsdatei identifizieren können, und **certificatethumbprint**die Übersicht (oder der Fingerabdruck) der vom Hashalgorithmus erzeugten Zertifikatdaten.

5. Suchen Sie das folgende Element in der Datei.

```
1 <icaFileSigning enabled="False" certificateId="" hashAlgorithm="
     sha1" />
```

6. Ändern Sie den Wert des aktivierten Attributs in "True", um die ICA-Dateisignierung für den Store zu aktivieren. Legen Sie als Wert des Attributs **certificateId** die ID fest, mit der Sie das Zertifikat identifizieren möchten, d. h. **certificateid** in Schritt 4.
7. Wenn Sie einen anderen Hashalgorithmus als SHA-1 verwenden möchten, setzen Sie den Wert des Attributs "hashAgorithm" nach Bedarf auf sha256, sha384 oder sha512.
8. Starten Sie Windows PowerShell von einem Konto mit lokalen Administratorrechten und geben Sie an der Eingabeaufforderung die folgenden Befehle ein, damit der Store auf den privaten Schlüssel zugreifen kann.

```
1 Add-PSSnapin Citrix.DeliveryServices.Framework.Commands
2   $certificate = Get-DSCertificate "certificatethumbprint"
3 Add-DSCertificateKeyReadAccess -certificate $certificates[0] -
     accountName "IIS APPPOOL\Citrix Delivery Services Resources"
```

Dabei ist "certificatethumbprint" der 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.

1. Öffnen Sie die Datei web.config für den Store mit einem Texteditor. 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.

```
<farmset ... enableFileTypeAssociation="on" ... >
```

3. Ändern Sie den Wert des Attributs "enableFileTypeAssociation" in "off", um die Dateitypzuordnung für den Store zu deaktivieren.

Anpassen des Anmeldedialogfelds der Citrix Workspace-App

Wenn sich Benutzer der Citrix Workspace-App 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. Um den Titeltext im Citrix Workspace-App-Anmeldedialogfeld anzuzeigen und anzupassen, bearbeiten Sie die Dateien für den Authentifizierungsdienst.

1. Öffnen Sie die Datei UsernamePassword.tfrm für den Authentifizierungsdienst mit einem Texteditor. Die Datei ist normalerweise im Verzeichnis C:\inetpub\wwwroot\Citrix\Authentication\App_Data\Temp
2. Suchen Sie die folgenden Zeilen in der Datei.

```
@* @Heading("ExplicitAuth:AuthenticateHeadingText") *@
```

3. Heben Sie die Auskommentierung auf für die Anweisung auf, indem Sie an Anfang und Ende **\@*** entfernen und am Ende ***@**.

```
@Heading("ExplicitAuth:AuthenticateHeadingText")
```

   Citrix Workspace-App-Benutzern 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 Texteditor die Datei *ExplicitFormsCommon.xx.resx* für den Authentifizierungsdienst (normalerweise im Verzeichnis C:\inetpub\wwwroot\Citrix\Aut
5. Suchen Sie die folgenden Elemente in der Datei. Bearbeiten Sie den vom <value>-Element umschlossenen Text, um den Titeltext zu ändern, der Benutzern im Citrix Workspace-App-Anmeldedialogfeld angezeigt wird, wenn sie auf Stores zugreifen, die diesen Authentifizierungsdienst verwenden.

```
<data name="AuthenticateHeadingText" xml:space="preserve">
    <value>My Company Name</value>
</data>
```


Um den Titeltext des 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 der Citrix Workspace-App für Windows

Standardmäßig speichert die Citrix Workspace-App für Windows die Kennwörter von Benutzern, wenn sie sich bei StoreFront-Stores anmelden. Sie können verhindern, dass die Citrix Workspace-App bzw. Citrix Receiver für Windows (jedoch nicht Citrix Receiver für Windows Enterprise) die Kennwörter von Benutzern zwischenspeichert, indem Sie die Dateien für den Authentifizierungsdienst ändern.

1. Verwenden Sie einen Texteditor, um die Dateiinetpub\wwwroot\Citrix\Authentication\App_Data\Templates\ zu öffnen.
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 gezeigt.

```
<!-- @SaveCredential(id: @GetTextValue(”saveCredentialsId”),
    labelKey: ”ExplicitFormsCommon:SaveCredentialsLabel”,
    initiallyChecked: ControlValue(”SaveCredentials”)) -->
```

Die Benutzer 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. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

Standardmäßig verwendete Citrix Receiver für Windows automatisch den zuletzt eingegebenen Benutzernamen. Um das Einfügen des Benutzernamen 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

September 10, 2019

In diesem Artikel werden zusätzliche Konfigurationsaufgaben für Citrix Receiver für Web-Sites beschrieben, die nicht mit der Citrix StoreFront-Verwaltungskonsole ausgeführt werden 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.

Konfigurieren der Anzeige von Ressourcen für Benutzer

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 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.

1. Öffnen Sie die Datei web.config für die Citrix Receiver für Web-Site in einem Texteditor. 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.

```
1 <uiViews showDesktopsView=”true” showAppsView=”true” defaultView=”
    desktops” />
```

3. Ändern Sie den Wert der Attribute **showDesktopsView** und **showAppsView** zu “false”, um zu verhindern, dass Desktops bzw. Anwendungen den Benutzern angezeigt werden, selbst wenn sie von der 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.

```
<userInterface ... autoLaunchDesktop="true">
```

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"

1. Öffnen Sie die Datei web.config für die Citrix Receiver für Web-Site in einem Texteditor. 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.

```
<userInterface enableAppsFolderView="true">
```

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

January 6, 2020

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 folgenden Dateinamenerweiterungen beim Filtern der Anforderungen:

- . (leere Erweiterung)
- .appcache
- .aspx
- .cr
- .css
- .dtd
- .png
- .htm
- .html
- .ica
- .ico
- .jpg
- .js
- .png
- .svg
- .txt
- .xml

Ist Download oder Upgrade der Citrix Workspace-App für Citrix Receiver für Web aktiviert, sind für StoreFront außerdem diese Dateinamenerweiterung erforderlich:

- .dmg
- .exe

Ist die Citrix Workspace-App 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

> **Wichtig:**
>
> - 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

> Hinweis:
>
> Microsoft IIS wird im Rahmen der StoreFront-Installation aktiviert. Microsoft IIS gewährt die Anmeldeberechtigung **Als Batchauftrag anmelden** und das Privileg **Annehmen der Clientidentität nach Authentifizierung** für die integrierte Gruppe "IIS_IUSRS". Dies ist normales Microsoft IIS-Installationsverhalten. Ändern Sie diese Benutzerrechte nicht. Weitere Informationen finden Sie in der Microsoft-Dokumentation.

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. Die Anwendungspools sind Citrix Configuration API, Citrix Delivery Services-Ressourcen, Citrix Delivery Services-Authentifizierung und Citrix Receiver für Web.

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 normalerweise 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". Ändern Sie diese Konfiguration nicht. Der Citrix StoreFront-Protokollübergangsdienst meldet sich als "SYSTEM" an. Ändern Sie diese Konfiguration nicht.

Konfigurieren der Gruppenmitgliedschaften

Wenn Sie eine StoreFront-Servergruppe konfigurieren, werden der Sicherheitsgruppe “Administratoren” die folgenden Dienste hinzugefügt:

- Citrix Konfigurationsreplikationsdienst (NT SERVICE\CitrixConfigurationReplication)
- Citrix Cluster Join (NT SERVICE\CitrixClusterService) . Dieser Dienst wird nur auf Servern angezeigt, die Teil einer Gruppe sind, und wird nur während des Beitritts ausgeführt.

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 die Citrix Workspace-App 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 mit dem Eintrag **discoverReceiver.domain** für Antragsteller oder Alternativer Antragstellername, wobei "domain" die Microsoft Active Directory-Domäne ist, die die E-Mail-Konten der 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 zwischen Citrix Workspace-App und 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 die Benutzer ihre Konten statt über die e-mail-basierte Kontenermittlung selbst durch Eingeben der Store-URLs in der Citrix Workspace-App konfigurieren, darf das Zertifikat auf dem StoreFront-Server nur für diesen Server gültig sein und muss 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 <*Installationsverzeichnis*>\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 **Eingeschränkt** wird nicht unterstützt, da sie das Ausführen von PowerShell-Skripts verhindert.) 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 Citrix Virtual Apps-Servern zu schützen. SSL-Relay ist eine Standardkomponente von Citrix Virtual Apps, die die Hostauthentifizierung und Datenverschlüsselung übernimmt.

Citrix empfiehlt, die TLS 1.0- und 1.1-Unterstützung auf dem Webserver zu deaktivieren, der StoreFront hostet. Sie sollten dies über Gruppenrichtlinienobjekte erzwingen, die die erforderlichen Registrierungseinstellungen auf dem StoreFront-Server erstellen, um ältere Protokolle wie TLS 1.0 und TLS 1.1 zu deaktivieren. Siehe TLS/SSL-Einstellungen in der Microsoft-Dokumentation.

Citrix empfiehlt, die Kommunikation zwischen StoreFront und Benutzergeräten mit Citrix Gateway und HTTPS zu schützen. Damit HTTPS verwendet werden kann, erfordert StoreFront, dass die Microsoft Internet Information Services (IIS)-Instanz, auf der der Authentifizierungsdienst gehostet wird, und damit verknüpfte Stores für HTTPS konfiguriert ist. 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.

Isolierung der StoreFront-Sicherheit

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 negativ beeinflussen. Ist höhere Sicherheit erforderlich, empfiehlt Citrix die Bereitstellung von StoreFront in einer getrennten Webdomäne.

Bereitstellen von SaaS- und Web-Apps über StoreFront

Sie können Ihre SaaS- und Webapps sicher über den StoreFront-Store für Benutzer bereitstellen. Mit Citrix Cloud und dem Hilfsprogramm Access Control Sync for StoreFront können Sie erweiterte Sicherheits- und Webfilterrichtlinien für diese Apps verwenden, um Benutzer und Netzwerk vor Malware und Datenlecks zu schützen. Die Benutzer greifen wie gewohnt auf den StoreFront-Store zu, um SaaS- und Web-Apps zu starten, die Sie in Citrix Cloud konfiguriert haben. Weitere Informationen finden Sie unter Zugriffssteuerung für SaaS- und Web-Apps in StoreFront.

ICA-Dateisignierung

In StoreFront können ICA-Dateien digital mit einem auf dem Server angegebenen Zertifikat signiert werden, damit Citrix Workspace-App-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.

Ändern der Basis-URL des StoreFront-Servers von HTTP in HTTPS

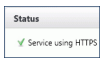
Wenn Sie die Kommunikation zwischen StoreFront und Benutzergeräten mit HTTPS sichern möchten, müssen Sie Microsoft Internetinformationsdienste (IIS) für HTTPS konfigurieren. Wenn Sie Citrix StoreFront installieren und konfigurieren, ohne zuvor ein SSL-Zertifikat zu installieren und zu konfigurieren, verwendet StoreFront HTTP für die Kommunikation.

Wenn Sie später ein SSL-Zertifikat installieren und konfigurieren, verwenden Sie das folgende Verfahren, um sicherzustellen, dass StoreFront und StoreFront-Dienste HTTPS-Verbindungen verwenden.

Beispiel:

Vor dem Ändern der Basis-URL in HTTPS:

Nach dem Ändern der Basis-URL in HTTPS:



1. Konfigurieren von Microsoft Internetinformationsdienste (IIS) für HTTPS auf dem StoreFront-Server:
   a) Importieren Sie mit der IIS-Verwaltungskonsole ein SSL-Serverzertifikat, das von der Microsoft Active Directory-Domänenzertifizierungsstelle signiert wurde.
   b) Fügen Sie der Standardwebsite eine IIS-Bindung über HTTPS (443) hinzu.

   Ausführliche Anweisungen finden Sie unter CTX200292.
2. Klicken Sie in der Citrix StoreFront-Verwaltungskonsole links auf **Servergruppe**.
3. Klicken Sie im Aktionsbereich auf **Basis-URL ändern**.
4. Geben Sie die Basis-URL ein und klicken Sie auf **OK**.

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.

Weitere Sicherheitsinformationen

> **Hinweis:**
>
> Diese Informationen können jederzeit und ohne vorherige Ankündigung geändert werden.

Sicherheitsprüfungen an StoreFront können zur Erfüllung gesetzlicher oder anderer Auflagen erforderlich sein. Die o. g. Konfigurationsoptionen können zu dazu beitragen, dass einige Sicherheitsprobleme vermieden werden.

Gibt es ein Gateway zwischen der Sicherheitsprüfung und StoreFront, können sich bestimmte Befunde im Prüfbericht auf das Gateway anstelle von StoreFront beziehen. Sicherheitsprüfberichte unterscheiden hier normalerweise nicht (Beispiel: TLS-Konfiguration). Aus diesem Grund können technische Beschreibungen in Sicherheitsprüfberichten irreführend sein.

Beachten Sie beim Lesen von Sicherheitsprüfberichten Folgendes:

- HTML-Seiten in StoreFront sind ggf. nicht gegen Clickjacking geschützt (durch die Inhaltssicherheitsrichtlinie oder “X-Frame-Options”-Header). Diese HTML-Seiten bestehen jedoch nur aus statischem Inhalt und sind nicht Clickjacking-anfällig.
- Die Version von Microsoft IIS und die Verwendung von ASP.NET sind in HTTP-Headern sichtbar. Diese Informationen gehen jedoch bereits aus dem Vorhandensein von StoreFront hervor, da es auf dieser Technologien basiert.
- Beim Starten von Anwendungen und Desktops verwendet StoreFront ein Token zum Schutz vor websiteübergreifender Anforderungsfälschung (CSRF). Das Token wird als Cookie in einer Antwort ohne Secure- oder HTTPOnly-Markierung gesendet. Wenn das Token später in einer Anforderung gesendet wird, ist es in der Abfragezeichenfolge einer URL enthalten. In StoreFront wird diese Art der Authentifizierung von HTTP-Anforderungen jedoch nicht verwendet.
- StoreFront verwendet die Open Source-Komponente jQuery. Eine verwendete Version ist jQuery 1.3.2. Laut Open Source-Projekt jQuery wurde in jQuery 1.12.0 eine Änderung vorgenommen, um potenzielle Schwachstellen in einer bestimmten Form domänenübergreifender Anfragen zu beseitigen. Die Änderung zielt nicht auf eine Schwachstelle in jQuery selbst, sondern auf einen potenziellen Missbrauch durch Anwendungslogik ab. Die relevante Citrix Anwendungslogik in dem Receiver für Web-Feature, das von NetScaler und StoreFront genutzt

wird, verwendet diese Art domänenübergreifende Anforderung nicht und ist nicht von der Schwachstelle betroffen. Für sie ist die Änderung nicht relevant.

Diese Änderung wurde aus Kompatibilitätsgründen in jQuery 1.12.3 entfernt. Da sie nicht für die Citrix Anwendungslogik relevant war, hat ihre Entfernung keine Auswirkungen auf die Versionen von NetScaler und StoreFront, die jQuery 1.12.4 verwenden.

Exportieren und Importieren der StoreFront-Konfiguration

March 3, 2020

> Hinweis:
>
> Sie können nur StoreFront-Konfigurationen von StoreFront-Versionen importieren, welche mit der der Zielinstallation identisch sind.

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.

Szenarios, in denen Konfigurationsexport und -import verwendet werden kann

- Führen Sie nur ein Backup von StoreFront-Bereitstellungen in einem funktionierenden und vertrauenswürdigen Zustand aus. Bei jeder Änderung an der Konfiguration ist ein neues Backup erforderlich, welches das alte ersetzt. Sie können vorhandene Backups nicht ändern, da ein Datei-Hash der Datei backup.zip Änderungen verhindert.
- Führen Sie zum Zweck der Notfallwiederherstellung ein Backup VOR dem Upgrade von StoreFront aus.
- Klonen bestehender StoreFront-Testbereitstellungen für die Produktion
- Erstellen von Benutzerakzeptanzumgebungen durch Klonen von Produktionsbereitstellungen in eine Testumgebung
- Verschieben von StoreFront während einer Betriebssystemmigration, z. B. beim Upgrade des Hostbetriebssystems von 2008R2 auf 2019
- Aufbau zusätzlicher Servergruppen in Bereitstellungen mit mehreren Standorten, z. B. in großen Unternehmen mit mehreren Datencentern

Punkte, die beim Exportieren und Importieren einer StoreFront-Konfiguration zu berücksichtigen sind

- 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-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

Parameter	Beschreibung
-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.

> **Wichtig:**
>
> Der Parameter **-SiteID** aus StoreFront 3.5 ist seit 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** 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`

Parameter	Beschreibung
-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://<importingserver>.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 (Zeichenfolge)	Der vollständige Pfad für das verschlüsselte Backuparchiv, das Sie entschlüsseln möchten. Sie müssen die Dateierweiterung CTXZIP angeben. 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\`

Parameter	Beschreibung
-Force (Boolean)	Dieser Parameter überschreibt automatisch Backuparchive mit demselben Dateinamen, die bereits im angegebenen Speicherort vorhanden sind.

Beispiele für Konfigurationsexporte und -importe

Importieren der StoreFront-Cmdlets in die aktuelle PowerShell-Sitzung

Öffnen Sie PowerShell Integrated Scripting Environment (ISE) auf dem StoreFront-Server und führen Sie Folgendes aus:

```
1 $env:PSModulePath = [Environment]::GetEnvironmentVariable('PSModulePath
    ','Machine')
2 $SDKModules = 'C:\Program Files\Citrix\Receiver StoreFront\
    PowerShellSDK\Modules\Citrix.StoreFront'
3 Import-Module "$SDKModules\Citrix.StoreFront.psd1" -verbose
4 Import-Module "$SDKModules.Authentication\Citrix.StoreFront.
    Authentication.psd1" -verbose
5 Import-Module "$SDKModules.Roaming\Citrix.StoreFront.Roaming.psd1" -
    verbose
6 Import-Module "$SDKModules.Stores\Citrix.StoreFront.Stores.psd1" -
    verbose
7 Import-Module "$SDKModules.WebReceiver\Citrix.StoreFront.WebReceiver.
    psd1" -verbose
```

Einzelserverszenarios

Erstellen Sie ein unverschlüsseltes Backup einer vorhandenen Konfiguration auf Server A und stellen Sie es auf derselben Bereitstellung wieder her

Exportieren Sie die Konfiguration des Servers, den Sie sichern möchten.

```
1 Export-STFConfiguration -targetFolder "$env:userprofile\desktop\" -
    zipFileName "backup" -NoEncryption
```

Kopieren Sie die Datei backup.zip an einen sicheren Speicherort. Sie können das Backup im Rahmen einer Notfallwiederherstellung dazu verwenden, den Server im vorherigen Zustand wiederherzustellen.


```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\
    backup.zip" -HostBaseURL "https://storefront.example.com"
```

Serverklonerstellung durch Sichern der Konfiguration auf Server A und Wiederherstellen auf Server B

Exportieren Sie die Konfiguration des Servers, den Sie sichern möchten.

```
Export-STFConfiguration -targetFolder "$env:userprofile\desktop\" -
    zipFileName "backup" -NoEncryption
```

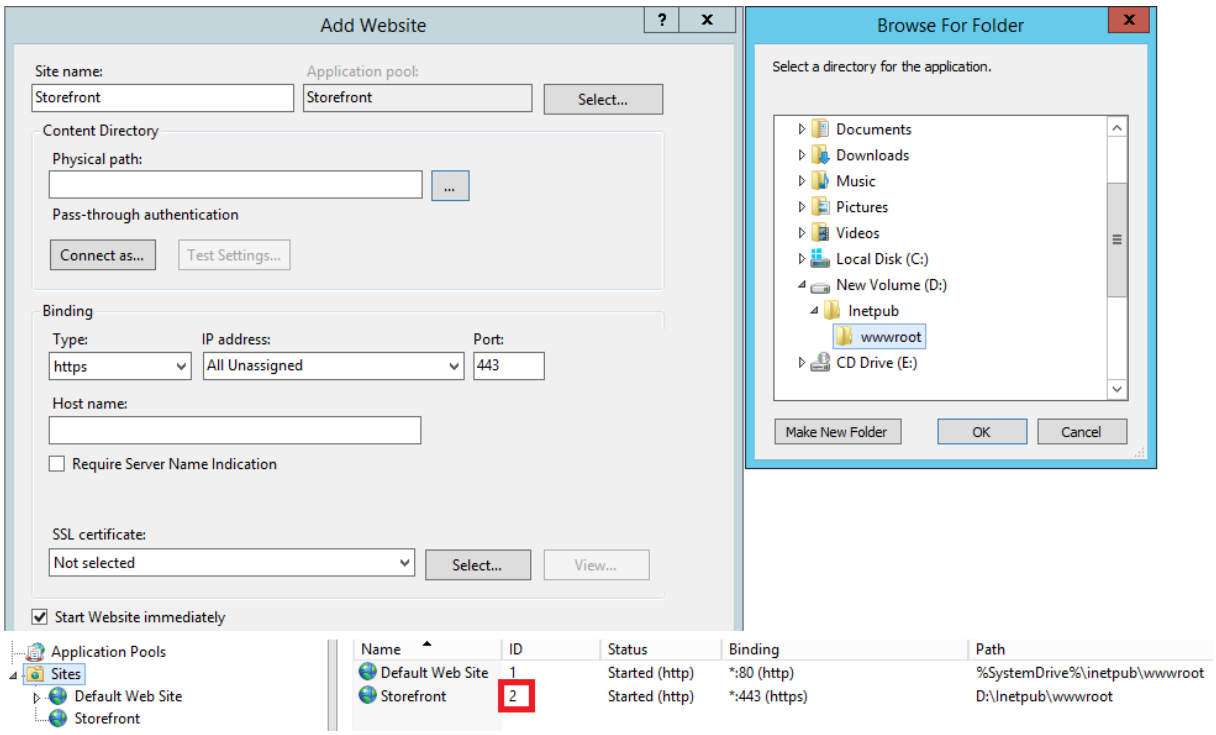
Kopieren Sie die Datei backup.zip auf den Desktop des Servers B.

```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\
    backup.zip" -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.

Eine neue Website mit dem Namen “StoreFront” wurde in IIS konfiguriert, die **SiteID = 2** verwendet. StoreFront wurde bereits auf der benutzerdefinierten Website in IIS bereitgestellt und der physische Pfad auf dem Laufwerk ist `d:\inetpub\wwwrooot`.



1. Exportieren Sie eine Kopie der Konfiguration von Server-A.
2. Konfigurieren Sie IIS auf Server B mit einer neuen Website namens **StoreFront**, die auch **SiteID 2** verwendet.
3. Importieren Sie die Server A-Konfiguration auf Server B. Die Site-ID im Backup wird verwendet und muss mit der Zielwebsite übereinstimmen, in die Sie die StoreFront-Konfiguration importieren.

   ```
   Import-STFConfiguration -configurationZip "$env:userprofile\desktop\
   backup.ctxzip"-HostBaseURL "https://serverB.example.com"
   ```

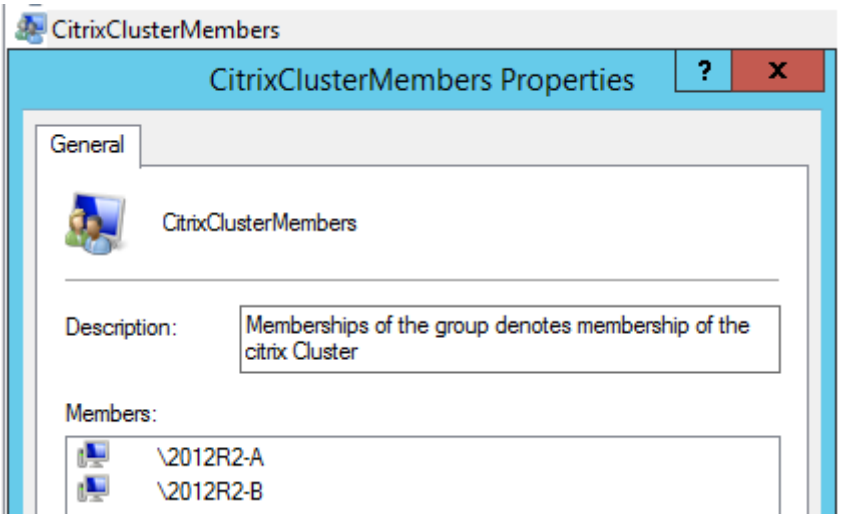
Servergruppenszenarios

Szenario 1: Erstellen Sie ein Backup einer vorhandenen Servergruppenkonfiguration und stellen Sie die Konfiguration in derselben Servergruppenbereitstellung später wieder her

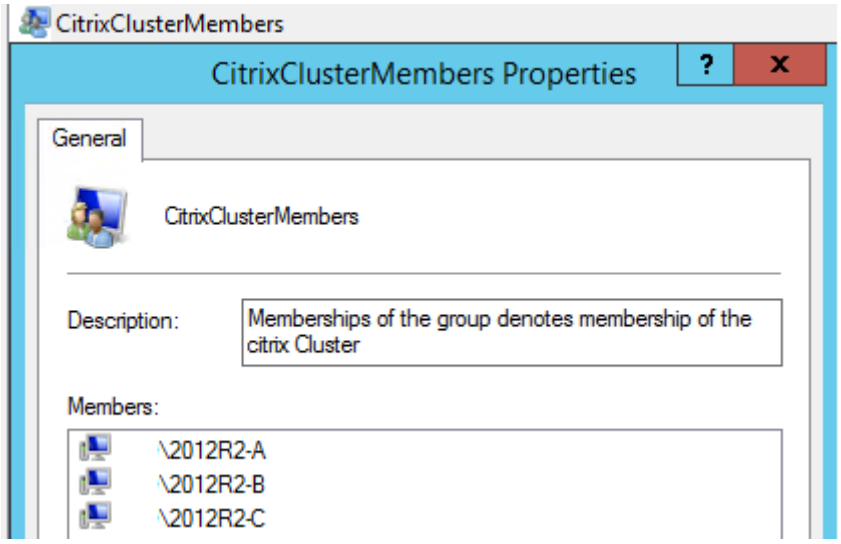
Zu einem früheren Zeitpunkt, als die Servergruppe nur zwei StoreFront-Server, 2012R2-A und 2012R2-B, enthielt, wurde ein Backup der Konfiguration erstellt. Das Backuparchiv enthält einen Datensatz der **CitrixClusterMembership**, die zur Zeit des Backups nur die beiden ursprünglichen Server 2012R2-A 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.



1. Fügen Sie der vorhandenen Servergruppe dann einen weiteren Server, 2012R2-C, hinzu.



1. Stellen Sie die Konfiguration der Servergruppe auf einen früheren funktionierenden Zustand wieder her. Während des Importvorgangs erstellt StoreFront ein Backup der aktuellen Citrix-ClusterMembership der drei Server und stellt sie nach dem Abschluss des Imports wieder her.
2. Importieren Sie die Konfiguration der Servergruppe 1 zurück auf den Knoten 2012R2-A.

```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\
```



```
backup.ctxzip”-HostBaseURL ”https://servergroup1.example.com”
```

3. 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”-HostBaseURL ”https://servergroup2.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"-NoEncryption -HostBaseURL "https://servergroup2.example.
   com"
   ```

Erstellen eines verschlüsselte Backups der Serverkonfiguration

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 der PowerShell-Sitzung 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 den zurzeit angemeldeten Windows-Benutzer.

Erstellen Sie ein PowerShell-Anmeldeinformationsobjekt in der Powershell-Sitzung auf dem exportierenden Server.

```
1 $User = [System.Security.Principal.WindowsIdentity]::GetCurrent().Name
2 $Password = "Pa55w0rd"
3 $Password = $Password | ConvertTo-SecureString -asPlainText -Force
4 $CredObject = New-Object System.Management.Automation.PSCredential(
      $User,$Password)
```

Exportieren Sie die Konfiguration in backup.ctxzip (eine verschlüsselte ZIP-Datei).

```
1 Export-STFConfiguration -targetFolder "$env:userprofile\desktop\" -
      zipFileName "backup" -Credential $CredObject
```

Erstellen Sie ein identisches PowerShell-Anmeldeinformationsobjekt in der Powershell-Sitzung auf dem importierenden Server.


```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\
    backup.ctxzip" -Credential $CredObject -HostBaseURL "https://
    storefront.example.com"
```

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
```

StoreFront SDK

April 1, 2020

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-MMC-Konsole 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 Citrix 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.

> **Wichtig:**
>
> 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 Folgendes ein, um alle Cmdlets zu importieren:

   ```
   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**, geben Sie den Cmdlet-Namen und den Parameter **-Full** an, 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
Erstellen einer einfachen Bereitstellung	Skript: erstellt eine einfache Bereitstellung mit einem StoreFront-Controller, der mit einem einzelnen XenDesktop-Server konfiguriert ist.
Erstellen einer Remotezugriffbereitstellung	Skript: erstellt eine Bereitstellung wie im vorherigen Skript plus Remotezugriff.
Erstellen einer Remotezugriffbereitstellung mit Gateway für den optimalen Start	Skript: erstellt eine Bereitstellung wie im vorherigen Skript und ermöglicht das Hinzufügen bevorzugter Gateways für den optimalen Start zur Verbesserung der Benutzererfahrung.

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 unter 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"
    )
    # Import StoreFront modules. Required for versions of
       PowerShell earlier than 3.0 that do not support
       autoloading
    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 dem angegebenen **$StoreVirtualPath**. **$StoreVirtualPath** entspricht **$StoreIIS-path**, da Virtuelle Pfade immer der Pfad in IIS sind. Daher haben sie in Powershell einen Wert wie "/Citrix/Store", "/Citrix/StoreWeb" oder "/Citrix/StoreAuth".

```
# Determine the Authentication and Receiver virtual path to use
   based of the 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.

```
# Determine if the deployment already exists
$existingDeployment = Get-STFDeployment
if(-not $existingDeployment)
{

    # Install the required StoreFront components
    Add-STFDeployment -HostBaseUrl $HostbaseUrl -SiteId $SiteId -
        Confirm:$false
 }

elseif($existingDeployment.HostbaseUrl -eq $HostbaseUrl)
{

    # The deployment exists but it is configured to the desired
        hostbase url
    Write-Output "A deployment has already been created with the
        specified hostbase url on this server and will be used."
 }

else
{

    Write-Error "A deployment has already been created on this
        server with a different host base url."
 }
```

- Erstellt, sofern noch nicht vorhanden, einen neuen Authentifizierungsdienst an dem angegebenen virtuellen Pfad. Die Standardauthentifizierungsmethode mit Benutzernamen und Kennwort ist aktiviert.

```
# Determine if the authentication service at the specified
    virtual path exists
$authentication = Get-STFAuthenticationService -VirtualPath
    $authenticationVirtualPath
if(-not $authentication)
{

```



```
6       # Add an Authentication service using the IIS path of the
            Store appended with Auth
7       $authentication = Add-STFAuthenticationService
            $authenticationVirtualPath
8    }
9
10   else
11   {
12
13      Write-Output "An Authentication service already exists at the
             specified virtual path and will be used."
14   }
```

- Erstellt einen neuen Storedienst mit einem XenDesktop-Controller und mit im Array **$XenDesktopServers** definierten Servern an dem angegebenen Pfad, sofern noch nicht vorhanden.

```
1   # Determine if the store service at the specified virtual path
        exists
2   $store = Get-STFStoreService -VirtualPath $StoreVirtualPath
3   if(-not $store)
4   {
5
6   # Add a Store that uses the new Authentication service configured
         to publish resources from the supplied servers
7   $store = Add-STFStoreService -VirtualPath $StoreVirtualPath -
        AuthenticationService $authentication -FarmName $Farmtype -
        FarmType $Farmtype -Servers $FarmServers -LoadBalance
        $LoadbalanceServers ‘
8            -Port $Port -SSLRelayPort $SSLRelayPort -TransportType
                $TransportType
9    }
10
11  else
12  {
13
14     Write-Output "A Store service already exists at the specified
            virtual path and will be used. Farm and servers will be
           appended to this store."
15     # Get the number of farms configured in the store
16     $farmCount = (Get-STFStoreFarmConfiguration $store).Farms.
           Count
17     # Append the farm to the store with a unique name
18     Add-STFStoreFarm -StoreService $store -FarmName "Controller$(
           $farmCount + 1)" -FarmType $Farmtype -Servers $FarmServers
            -LoadBalance $LoadbalanceServers -Port $Port ‘
```



```
19          -SSLRelayPort $SSLRelayPort -TransportType $TransportType
20   }
```

- Fügt einen Citrix Receiver für Web-Dienst an dem angegebenen virtuellen IIS-Pfad ein für den Zugriff auf Anwendungen, die in dem oben erstellten Store veröffentlicht wurden.

```
1  # Determine if the receiver service at the specified virtual path
       exists
2  $receiver = Get-STFWebReceiverService -VirtualPath
      $receiverVirtualPath
3  if(-not $receiver)
4  {
5
6      # Add a Receiver for Web site so users can access the
          applications and desktops in the published in the Store
7      $receiver = Add-STFWebReceiverService -VirtualPath
          $receiverVirtualPath -StoreService $store
8   }
9
10 else
11 {
12
13     Write-Output "A Web Receiver service already exists at the
          specified virtual path and will be used."
14  }
```

- Aktiviert XenApp-Dienste für den Store, damit ältere Citrix Receiver-/Citrix Workspace-App-Clients eine Verbindung mit veröffentlichten Anwendungen herstellen können.

```
1  # Determine if PNA is configured for the Store service
2  $storePnaSettings = Get-STFStorePna -StoreService $store
3  if(-not $storePnaSettings.PnaEnabled)
4  {
5
6  # Enable XenApp services on the store and make it the default for
       this server
7  Enable-STFStorePna -StoreService $store -AllowUserPasswordChange
      -DefaultPnaService
8   }
```

Beispiel: Erstellen einer Remotezugriffbereitstellung

Das folgende, auf dem vorherigen Skript aufbauende Beispiel dient zum Erstellen einer Bereitstellung mit Remotezugriff.

Bevor Sie beginnen, stellen Sie sicher, dass Sie die unter 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,
    [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

# Any failure is a terminating failure.
```



```
$ErrorActionPreference = 'Stop'
$ReportErrorShowStackTrace = $true
$ReportErrorShowInnerException = $true
# Import StoreFront modules. Required for versions of PowerShell earlier than 3.0 that do not support autoloading
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.

```
# Create a simple deployment by invoking the SimpleDeployment example
$scriptDirectory = Split-Path -Path $MyInvocation.MyCommand.Definition -Parent
$scriptPath = Join-Path $scriptDirectory "SimpleDeployment.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.

```
# Determine the Authentication and Receiver sites based on the Store
$store = Get-STFStoreService -VirtualPath $StoreVirtualPath
$authentication = Get-STFAuthenticationService -StoreService $store
$receiverForWeb = Get-STFWebReceiverService -StoreService $store
```

- Aktiviert CitrixAGBasic in dem für Remotezugriff mit Citrix Gateway erforderlichen Citrix Receiver für Web-Dienst. Ruft die Citrix Receiver für Web CitrixAGBasic- und die ExplicitForms-Authentifizierungsmethode von den unterstützten Protokollen ab.

```
# Get the Citrix Receiver for Web CitrixAGBasic and ExplicitForms authentication method from the supported protocols
# Included for demonstration purposes as the protocol name can be used directly if known
$receiverMethods = Get-STFWebReceiverAuthenticationMethodsAvailable | Where-Object {
 $_ -match "Explicit" -or $_ -match "CitrixAG"  }

```



```
# Enable CitrixAGBasic in Receiver for Web (required for remote
    access)
Set-STFWebReceiverService $receiverForWeb -AuthenticationMethods
    $receiverMethods
```

- Aktiviert CitrixAGBasic für den Authentifizierungsdienst. Dies ist für den Remotezugriff erforderlich.

```
# Get the CitrixAGBasic authentication method from the protocols
    installed.
# Included for demonstration purposes as the protocol name can be
     used directly if known
$citrixAGBasic = Get-STFAuthenticationProtocolsAvailable | Where-
    Object {
 $_ -match "CitrixAGBasic"  }

# Enable CitrixAGBasic in the Authentication service (required
    for remote access)
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.

```
# Add a new Gateway used to access the new store remotely
Add-STFRoamingGateway -Name "NetScaler10x" -LogonType Domain -
    Version Version10_0_69_4 -GatewayUrl $GatewayUrl '
-CallbackUrl $GatewayCallbackUrl -SecureTicketAuthorityUrls
    $GatewaySTAUrls
# Get the new Gateway from the configuration (Add-
    STFRoamingGateway will return the new Gateway if -PassThru is
    supplied as a parameter)
$gateway = Get-STFRoamingGateway -Name $GatewayName
# If the gateway subnet was provided then set it on the gateway
    object
if($GatewaySubnetIP)
{

    Set-STFRoamingGateway -Gateway $gateway -SubnetIPAddress
        $GatewaySubnetIP
 }

# Register the Gateway with the new Store
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 unter 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,
```



```
20      [string]$GatewaySubnetIP,
21      [Parameter(Mandatory=$true)]
22      [string]$GatewayName,
23      [Parameter(Mandatory=$true)]
24      [Uri]$OptimalGatewayUrl,
25      [Parameter(Mandatory=$true)]
26      [string[]]$OptimalGatewaySTAUrls,
27      [Parameter(Mandatory=$true)]
28      [string]$OptimalGatewayName
29  )
30  Set-StrictMode -Version 2.0
31  # Any failure is a terminating failure.
32  $ErrorActionPreference = 'Stop'
33  $ReportErrorShowStackTrace = $true
34  $ReportErrorShowInnerException = $true
35  # Import StoreFront modules. Required for versions of PowerShell
        earlier than 3.0 that do not support autoloading
36  Import-Module Citrix.StoreFront
37  Import-Module Citrix.StoreFront.Stores
38  Import-Module Citrix.StoreFront.Roaming
```

- Ruft das Skript zur Erstellung einer Remotezugriffbereitstellung zum Konfigurieren der einfachen Bereitstellung mit Remotezugriff auf.

```
1  # Create a remote access deployment
2  $scriptDirectory = Split-Path -Path $MyInvocation.MyCommand.
       Definition -Parent
3  $scriptPath = Join-Path $scriptDirectory "RemoteAccessDeployment.
       ps1"
4  & $scriptPath -HostbaseUrl $HostbaseUrl -SiteId $SiteId -
       FarmServers $FarmServers -StoreVirtualPath $StoreVirtualPath -
       Farmtype $Farmtype `
5       -LoadbalanceServers $LoadbalanceServers -Port $Port  -
           SSLRelayPort $SSLRelayPort -TransportType $TransportType `
6       -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.

```
1  # Add a new Gateway used for remote HDX access to desktops and
       apps
2  $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.

```
# Get the Store configured by SimpleDeployment.ps1
$store = Get-STFStoreService -VirtualPath $StoreVirtualPath
# Register the Gateway with the new Store for launch against all
   of the farms (currently just one)
$farmNames = @($store.FarmsConfiguration.Farms | foreach {
 $_.FarmName  }
)
Register-STFStoreOptimalLaunchGateway -Gateway $gateway -
   StoreService $store -FarmName $farmNames
```

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) oder mit den folgenden PowerShell-Cmdlets:

- 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://<storefront host>/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:


```
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/FederationMetadata.xml

# 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.xml"
```

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.

```
# 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:

```
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

April 1, 2020

Wenn StoreFront installiert oder deinstalliert wird, werden die folgenden Protokolldateien vom StoreFront-Installationsprogramm im Verzeichnis *C:\Windows\Temp\StoreFront* 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 zeichnet automatisch Ablaufverfolgungsinformationen auf. 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 gespeichert, normalerweise C:\Programme\Citrix\Receiver StoreFront. 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 Texteditor. 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.

   ```
   <logger duplicateInterval=”00:01:00”duplicateLimit=”10”>
   ```

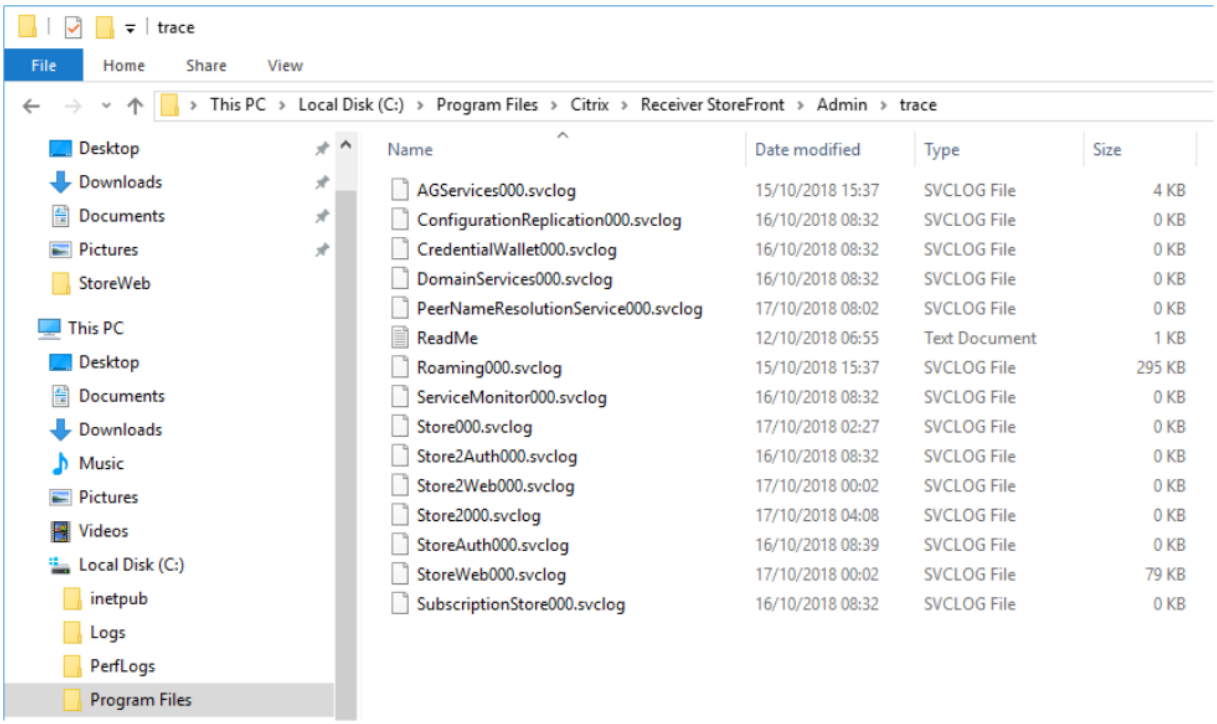
   Standardmäßig wird in der Konfiguration von StoreFront die Anzahl der doppelten Protokolleinträge auf 10 pro Minute beschränkt.
3. Ändern Sie den Wert des Attributs duplicateInterval, um den Zeitraum, in dem doppelte Protokolleinträge überwacht werden, in Stunden, Minuten und Sekunden festzulegen. Legen 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 zur Problembehandlung

> **Wichtig:**
>
> 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 der PowerShell-Konsole, bevor Sie die StoreFront-Konsole öffnen.

Die Ausgabe der Ablaufverfolgung wird an c:\Program Files\Citrix\Receiver StoreFront\admin\trace gesendet.



> **Hinweis:**
>
> Führen Sie `Get-Help Set-STFDiagnostics -detailed` aus, um die Powershell-Hilfe und Anweisungen für die Cmdlet Set-STFDiagnostics anzuzeigen.

Starten Sie mit einem Konto mit lokalen Administratorrechten Windows PowerShell und geben Sie an der Eingabeaufforderung die erforderlichen Parameter ein, um die Ablaufverfolgung zu aktivieren oder zu deaktivieren.

- **-All**. Ein Flag, das angibt, dass die Ablaufverfolgung für alle Instanzen und Dienste aktualisiert werden soll.
- **-TraceLevel**. In aufsteigender Detaildichte sind die zulässige Werte für "-TraceLevel": Off, Error, Warning, Info, Verbose. Aufgrund der großen Datenmenge, die generiert werden kann, kann die Ablaufverfolgung die Leistung von StoreFront erheblich beeinträchtigen. "Info" oder "Verbose" werden nicht empfohlen, es sei denn, sie sind speziell für die Problembehandlung erforderlich.

Optionale Parameter:

- **-FileSizeKb**. Die Größe der Ablaufverfolgungsdatei in KB.
- **-FileCount**. Die Anzahl der Ablaufverfolgungsdateien, die gleichzeitig auf dem Datenträger verwaltet werden sollen.
- **-confirm:$False**. Unterdrückt Windows-Aufforderungen, damit das Cmdlet StoreFront jedes Mal ausgeführt werden kann.

Beispiele

Aktivieren der Ablaufverfolgung mit der Stufe “Verbose” für alle Dienste für das Debugging:

```
Set-STFDiagnostics -All -TraceLevel ”Verbose” -confirm:$False
```

Deaktivieren der Ablaufverfolgung mit der Stufe “Verbose” und Zurücksetzen der Ablaufverfolgung auf den Standardwert für alle Dienste:

```
Set-STFDiagnostics -All -TraceLevel ”Error” -confirm:$False
```

Weitere Informationen zum Cmdlet Set-STFDiagnostics finden Sie in der Dokumentation zum StoreFront PowerShell SDK.

Aktivieren der Protokollierung für die Datei launch.ica

Speichern Sie die Informationen in der Datei launch.ica auf dem Clientcomputer, um verschiedene Probleme zu behandeln. Die Datei launch.ica wird von Citrix Webinterface- oder Citrix StoreFront-Servern generiert.

Führen Sie die folgenden Schritte aus, um die Protokollierung der Datei launch.ica zu aktivieren:

1. Navigieren Sie mit dem Registrierungs-Editor zum folgenden Registrierungsschlüssel:

   32-Bit-Systeme: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\Logging`

   64-Bit-Systeme: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\Logging`

2. Legen Sie die folgenden Zeichenfolgenwert fest:

   - LogFile=”Pfad zur Protokolldatei”
   - LogICAFile=true

   Beispiel:

   ```
   LogFile=C:\ica\ica.log
   LogICAFile=true
   ```

Weitere Ressourcen

> Hinweis:

> Die Verwendung einer ICA-Datei in Ihrer Umgebung für andere Zwecke als die Problembehandlung wird in CTX200126 erläutert.

Behandlung von StoreFront-Upgradeproblemen

Gehen Sie zur Behandlung von StoreFront-Upgradeproblemen folgendermaßen vor.

Vor dem Upgrade

1. Vergewissern Sie sich, dass Sie alle StoreFront-Server gesichert haben.
2. Stellen Sie sicher, dass Sie kein Upgrade von einer End-of-Life-StoreFront-Version versuchen. Weitere Informationen finden Sie unter CTX200356.
3. Stellen Sie sicher, dass Sie ausschließlich ein Upgrade von einer unterstützten StoreFront-Version auf die aktuelle Version durchführen.
4. Wenn der StoreFront-Server Teil einer StoreFront-Servergruppe ist, müssen alle Server in der Gruppe nacheinander aktualisiert werden. Das gleichzeitige Aktualisieren der Server in einer StoreFront-Servergruppe wird nicht unterstützt.
5. Löschen Sie alle *thumbs.db*-Dateien in *C:\inetpup\wwwroot\citrix* und den Unterverzeichnissen dieses Pfads. Zeigen Sie verborgene Dateien an, um diesen Schritt durchzuführen: Wählen Sie **Ordneroptionen > Ansicht** und dann die Option **Versteckte Dateien, Ordner und Laufwerke anzeigen** und deaktivieren Sie die Option **Geschützte Systemdateien ausblenden (empfohlen)**.
6. Deaktivieren Sie Antivirensoftware vor dem Upgrade.
7. Vergewissern Sie sich, dass die Server, die aktualisiert werden sollen, von jedem Load Balancer entfernt wurden und keine aktiven Benutzersitzungen haben.
8. Starten Sie die StoreFront-Server vor dem Upgrade neu.
9. Beenden Sie die folgenden Dienste manuell:
    - CitrixConfigurationReplication
    - CitrixCredentialWallet
    - CitrixDefaultDomainService
    - CitrixPeerResolutionService
    - CitrixSubscriptionsStore
10. Stellen Sie sicher, dass die StoreFront-Verwaltungskonsole geschlossen ist.

Vorgehen bei einem Upgradefehler

1. Öffnen Sie im Ordner *C:\Windows\Temp\StoreFront* das neueste *CitrixMsi*.log* und suchen Sie nach Ausnahmefehlern.

Ausnahmen mit **Thumbs.db Access**: Verursacht durch *thumbs.db*-Dateien in *C:\inetpup\wwwroot\citrix* oder Unterverzeichnissen. Löschen Sie alle gefundenen Dateien *thumbs.db*-Dateien.

Cannot get exclusive file access \in use: Stellen Sie den Snapshot/die Sicherung, falls verfügbar, wieder her oder starten Sie den Server neu und beenden Sie alle StoreFront-Dienste manuell.

Service cannot be started: Stellen Sie den Snapshot/die Sicherung, falls verfügbar, wieder her oder installieren Sie die Vollversion von .NET Framework 4.5 (nicht Client Profile).

2. Enthält *CitrixMsi*.log* keine Ausnahmen, überprüfen Sie die Ereignisanzeige des Servers unter **Delivery Services** auf die o. a. Fehlermeldungen. Folgen Sie den entsprechenden Anweisungen.
3. Enthält die Ereignisanzeige keine Ausnahmefehler, überprüfen Sie die Admin-Protokolle unter *C:\Programme\Citrix\Receiver StoreFront\logs* auf die o. a. Fehlermeldungen. Folgen Sie den entsprechenden Anweisungen.

Manuelles Entfernen von StoreFront

> Warnung:
>
> Beim manuellen Entfernen von StoreFront werden alle vorhandenen Informationen gelöscht.

Gehen Sie zum manuellen Entfernen von StoreFront folgendermaßen vor:

1. Deinstallieren Sie StoreFront.
2. Entfernen Sie die Webserverrolle.
3. Löschen Sie den Ordner *C: Programme\Citrix\Receiver StoreFront*.
4. Löschen Sie alle Unterverzeichnisse unter *C:\Programme\Citrix\StoreFront Install*.
5. Löschen Sie den Ordner *C:\Inetpub*.

Sie können jetzt StoreFront neu installieren.

